Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-10-12 8:17 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; Csversko, Christine; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted]; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 10, 2012 / le 10 février 2012

Print Media / Médias imprimés

Youths are vulnerable to Internet luring
Youths ranging in age from 12 to 15 continue to remain targets of online luring, according to figures released this week by the Canadian Centre for Child Protection. The Daily Gleaner, A4

Online Media / Médias en ligne

Analysis: In cyber era, militaries scramble for new skills
With growing worries about the threat of "cyber warfare," militaries around the world are racing to recruit the computer specialists they believe may be central to the conflicts of the 21st century. ut whilst money is plentiful for new forces of "cyber warriors," attracting often individualistic technical specialists and hackers into military hierarchies is another matter. Reuters

Inside INTERPOL's New Cybercrime Innovation Center
INTERPOL, the international policing organization, is building a law enforcement tech geek heaven in Singapore. The INTERPOL Global Complex for Innovation will function as a R&D lab, training facility, and forensics lab for all things cybercrime. Michael Moran, INTERPOL's Acting Assistant Director for Cyber Security and Crime, told Fast Company on Wednesday that the main focus for IGCI would be digital security and innovation research for police officers worldwide investigating cybercrime. Fast Company

Syria's Cyberwar
Since media are strictly controlled by the Syrian government, the internet has played a key role in allowing opposition activists share images of alleged atrocities carried out by security forces. You can argue that a high-stakes war of information is being waged in Syrian cyberspace, and in one battle at least the hacking group Anonymous is claiming victory. CNN

Anonymous Launches Cyber-Crusade against Israel 'Reign of Terror'
Anonymous hacker collective has threatened a cyber-crusade against Israel to end what it claims is a reign of terror. In the latest round of cyber-warfare between pro-Palestinians and pro-Israeli hackers, the hacktivists have released a video on YouTube which accuses Israel of committing crimes against humanity. International Business Times

Android malware connects to botnet and makes premium rate calls by rooting itself
The Android operating system has had yet another serious piece of malware sully its name today, as an Android app called com.google.android.smart has been discovered to be a premium rate texts, calls and botnet scam. Tech Digest

Facebook Video Scam: World War III Begins
A new dimension to cyber crime was highlighted with the spreading of fake news of the commencement of World War III in the US for invading Iran and Saudi Arabia. SPAMfighter

Malware authors get social to improve cyber attacks
Security researchers have found that cyber criminals are offering their attack tools in a software-as-a-service (SaaS) model, and creating social networks to build communities around their products to help suggest new features and find bugs. Computing News

Cyber-space now seen as 'fifth dimension of warfare'
The cyber-security challenge is not a national one - it is a global one, as countries around the world recognise the benefits of working together to tackle criminals, who make use of the worldwide web. As the report we recently commissioned found, just under half of experts now think cyber-security is as important as border security; so there is clearly a demand for governments to be more involved in addressing threats which cross borders. Public Service Europe

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

AUDIENCE:

This Information Report is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries. The recipients of this product may further distribute it to technical stakeholders within their organization.

PURPOSE

The purpose of this Information Report is to provide IT security personnel with an introduction to distributed denial-of-service (DDoS) attacks, their modus-operandi and the recommended steps to help with the preparation, identification, containment, recovery and continuous improvement efforts required to limit associated organizational risk. This document may be used by system administrators, computer security incident response teams (CSIRTS), IT security operations centres and other related technology groups.

INTRODUCTION

Denial of service (DoS) attacks are common malicious network actions aimed at disrupting the availability of computing resources from legitimate users. These types of attacks, especially DDoS attacks have recently gained in popularity due to the availability of DoS rental services from botnet operators, as well as the availability of various free and easy to use hacking tools. The latter have enabled activists using hacking to support their causes (also known as hacktivists) to efficiently recruit large numbers of followers to perpetrate cyber attacks, increasing both their distribution and power. Well known examples of DoS attacks include the use of the Low Orbit Ion Cannon DDoS tool in support of Wikileaks[1] used by hacking group "Anonymous" and attacks against national infrastructures such as Korea[2] , Georgia[3] and Estonia[4].

DOS AND DDOS DEFINITION

A DoS attack is an attempt to make a computer resource unavailable to its intended users[5]. A DDoS attack occurs when multiple systems simultaneously flood networked computer resources, rendering them inaccessible. A DDoS attack, in contrast with a DoS attack, comes from many sources, often hundreds or even thousands. As a result, mitigation actions against a DDoS attack are more difficult to coordinate and associated traffic is more damaging to the target.

DDoS attacks often use stateless protocols such as UDP and ICMP, but stateful protocols can also be used when the connections are not fully established such as during a TCP SYN flood attack. Both techniques make it easier for the attacker to use spoofed IP addresses and harder to determine the source of the attack.

---

[1] Introduction to LOIC: http://en.wikipedia.org/wiki/LOIC
[2] http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems
[3] http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/
[4] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[5] Definition: http://en.wikipedia.org/wiki/Denial-of-service_attack

FIVE STEPS TO DEFEND AGAINST DDOS ATTACKS

Preparation

Preparation is the most important step in defending against a DDoS attack. Clear and complete procedures and guidelines should be established well before an attack takes place. Any organization can fall victim to DDoS attacks, either directly or indirectly. Having a solid plan in place will help reduce the risk and lessen the impact should an attack occur.

Identification

Indicators that your organization may be under a DDoS attack could include poor network performance, inaccessible services or system crashes. Being able to identify and understand the nature of the attack and its targets will help in the containment and recovery process. For this purpose, organizations require tools that provide visibility over their managed information technology (IT) infrastructure. Often, prior to a DDoS attack, a reconnaissance of the target is performed by the attacker. This may include scanning the target network for known exposed vulnerabilities or sending malformed packets to the target host to analyze changes in response time. This reconnaissance activity may be hard to detect, especially because it may take place well before the attack itself. A knowledgeable attacker will also ensure scan traffic does not meet the threshold required to trigger alarms from network monitoring tools. However, there may be available intelligence indicating an increased likelihood of a DDoS attack against an organization. Good examples are the Anonymous Operations (aka "anonops")[6] , which broadly advertise their motivation and targets.

Containment

Having a pre-determined containment plan before an attack for a number of scenarios will significantly improve response speed and limit damages resulting from a DDoS attack. For example, the containment strategy for a mail server may differ from one for a web server. Underestimating the importance of this phase can result in mistakes and significant collateral damages. Therefore, understanding the nature of DDoS attacks and documenting the associated decision-making process is critical. An organization should clearly identify its network perimeter and exposed assets. Load balancers, modern firewall technologies (Deep Packet Inspection, proxy, application layer filtering), content caching, content hosting geographic diversity, dynamic DNS service and ISP-based DDoS protection services are some of the tools an organization may leverage to contain an ongoing DDoS attack.

Recovery

Depending on the containment strategy employed and the sensitivity to its collateral impact, an organization may be under different pressure to recover from a DDoS attack. Understanding the characteristics of the attack is required for an appropriate recovery. DDoS may exploit limits in the following resources:

- Server queue length
- Server computing resources
- Client tolerance to level of service variability
- Bandwidth

---

[6] http://anonops.blogspot.com/2011/09/tar-sands-action-september-3-press_04.html

A DDoS attack may exploit any or a combination of these limitations. An organization equipped with a flexible provisioning model for these resources may be able to rapidly adapt and sustain long-term DDoS attacks. However, some attacks may leverage vulnerabilities in protocols or software and achieve unexpected high impact as a result. [7] An organization equipped with packet capture capability may be able to identify the delivery method of the attack and potentially design an accurate Intrusion Prevention System / Firewall signature. Despite mitigation efforts, some DDoS attacks may be persistent over time. An organization using connection logs and other tools may be able to provide a list of potentially offending IP addresses (if not spoofed) to their upstream ISP, law enforcement and national Computer Emergency Response Team (CERT) to coordinate mitigation/investigation of the offending sources.

Lessons Learned

Lessons learned is a very important step that is often overlooked. Lessons learned activities should take place as soon as possible following an incident. All decisions and steps taken throughout the incident handling cycle should be reviewed. All procedures should be reviewed to see where improvements may be made.

Perhaps the most challenging part of performing a Lessons Learned review involves documenting the impact and cost the incident caused to the organization. Although time consuming, this step is essential to allow organizations to properly justify security resources and assess their return on investment. Damages to an organization include tangible metrics, such as loss in sales and productivity, as well as intangible metrics, such as reputation and brand.

By performing this review after each incident, organizations will enable continuous improvement and potentially significant reduction in the impact of incidents.

CHECKLIST

The following checklist is intended to help organizations during the various mitigation phases of DDoS attacks. Many of these mitigations are applicable to other types of cyber attacks as well and should be considered accordingly.

#	Item	In progress	Completed
	Preparation		
1.	Identify your most critical assets and the services they provide. • Are they up to date with the latest patches? • Do they run any unnecessary services such as Telnet or FTP?		
2.	Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.		

[7] http://www.theregister.co.uk/2011/08/24/devastating_apache_vuln/

3. Establish 24/7 contact information for your ISP and alternate methods for communications.

4. Deny all obviously spoofed traffic (e.g., internal IP addresses that should not be coming in or going out of your network). Implement a bogon block list (unallocated address space) at the network boundary.

5. Establish procedures on how to segregate your networks in the event of a DDoS attack. Use existing network devices, such as routers and managed switches, to defend against DDoS attacks. Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.

6. Disable all unnecessary services and restrict access to and from all previously identified critical hosts based on DDoS traffic characteristics.

7. Create a whitelist of the source IPs you must allow if you need to prioritize traffic during an attack.

8. Document your network topology including all IP addresses. Keep it up to date.

9. Review your Business Continuity Plan (BCP) and ensure senior management and legal team understand the significance of a DDoS attack, including their roles.

10. Understand "normal." Establish a baseline of network traffic, CPU usage, connection and memory utilization of critical hosts under normal conditions so that network monitoring tools will trigger on abnormal changes.

11. Acknowledge that your organization may be attacked. Organizations should consider the development and implementation of policies, plans and procedures to defend against DDoS attacks. Identify and planfor resources to implement these plans.

12. Assign roles and responsibilities. Identify who plays a role in defending against a DDoS attack and ensure they are aware of this responsibility. This should include personnel from critical business functions, IT operations, network and IT security teams, legal advisors, and media relations staff. Ensure an up-to-date point-of-contact list with primary and alternate personnel is maintained. As the network may be unavailable, including mobile devices, ensure alternate communications mechanisms are in place.

13.	Conduct exercises. The worst time to test plans and procedures is during an attack.

Identification

1.	Determine if you are the primary target or a collateral victim. (ex: is your upstream internet provider or content hosting provider the target ?)
2.	Understand the logical flow of the attack.
3.	Determine what type of traffic is being used, such as IP addresses, ports and protocols.
4.	Consider using network analysis tools to determine the type of traffic being used in the attack (e.g., TcpDump, Wireshark, Snort).
5.	Review any available logs to understand the attack and what is being targeted.
6.	Notify appropriate personnel. This may include senior management and the legal team.

Containment

1.	Contact your ISP to implement filtering.
2.	Block the traffic as close to the network cloud as possible (router, firewall, load balancer, etc.).
3.	Relocate the target to another IP address if a particular host is being targeted. This is a temporary solution.
4.	If a particular application is being targeted, consider disabling it temporarily.
5.	Identify and correct the vulnerability or weakness that is being exploited. An example of this may be an unused service that is accidently left enabled on a public facing device or unpatched operating system.
6.	Implement filtering based on the characteristics of the attack. An example may be blocking IMCP echo packets.
7.	Implement rate limiting for certain protocols, allowing a certain number of packets per second for a specific protocol or to access a certain host.

Recovery

1.	Confirm that the DDoS attack has finished and services are

reachable again.

2. Confirm that your networks are back to your baseline performance.

3. If necessary, patch and update all affected machines.

4. If possible, identify the source of the attack. Enlist the help of your ISP.

5. Review logs for signs of reconnaissance. Maintain logs for possible future law enforcement requirements.

Lessons Learned

1. Create or update the following documents:
   - Standard Operating Procedures
   - Emergency Operating Procedures
   - Business Continuity Plans

RECOMMENDATIONS

CCIRC recommends that organizations assess their risk exposure to Denial of Service attacks which may be caused accidentally or intentionally and consider mitigation advice herein provided and implement them as appropriate for the specific IM/IT environment.

REFERENCES

1. US-CERT, Understanding Denial-of-Service Attacks
http://www.us-cert.gov/cas/tips/ST04-015.html

2. NIST, Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

3. GovCERT.NL, Factsheet: Protect your online services against dDoS attacks
http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html

4. Societe Generale DDoS Incident Reponse
http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf

REPORTING

Any Canadian Critical Infrastructure Operator wishing to report incidents may do so using the CCIRC Cyber Duty Officer PGP encryption key, found at:
http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx
Associated reports should be sent to:
cyberdo@ps-sp.gc.ca.

Potentially malicious files/samples may be shared with CCIRC by sending them zipped and protected with the password "infected" via email to:
malware@ccirc-ccric.gc.ca

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.

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

Email: communications@ps-sp.gc.ca

For urgent matters please contact the GOC.

s.16(2)(c)
s.15(1) - Subv

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-09-12 8:42 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted]Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 9, 2012 / le 9 février 2012

Print Media / Médias imprimés

NASA hacker faces charges
A Romanian man known as "Ice Man" has been indicted for hacking into computers at the National Aeronautics and Space Administration's Jet Propulsion Laboratory in Southern California, U.S. federal prosecutors said Wednesday.
Windsor Star, A11

Online Media / Médias en ligne

SDA, McAfee mark Canada's card
The Canadian government could try harder in matters of cyber security, according to a report ranking countries on their security stance. Canada received a mediocre ranking in the report, which was co-produced by McAfee and the Security Defence Agenda (SDA), a Brussels-based security think tank. SC Magazine

UK cyber strategy implementation 'too slow', says former security minister

The UK government needs to set out a clear timetable for the implementation of its cyber security strategy, former security minister Baroness Pauline-Neville Jones has said. Neville-Jones, who is now the government's Special Representative to Business on Cyber Security, said that since the government is only starting to implement the policies of the strategy, significant progress will not be seen another 18 months. Computerworld UK

'The internet should be a demilitarised zone'
In a world where governments are spending tens of billions of pounds arming themselves for a cyberwar, Eugene Kaspersky's message is an unfashionable one. As chief executive of one of the largest computer security firms, he flies around the world telling politicians and officials they should instead be working to make the internet a military-free zone. The Telegraph (UK)

Cyber criminals eye Olympics as opportunity to con people
Researchers at internet and software security firm Websense have unearthed a number of Olympic ticket scam sites. The researchers found that most of them had multiple backlinks, suggesting they have been widely spammed over the internet in addition to being promoted via Google AdWords. The Times of India

Can Hackers Destroy The Internet?
Botnets, trojans, SQL injections and DDoS attacks. Most internet users have no idea what those things are, or how they are shaping the future of their connected lives. One thing is certain, more computers and wireless devices are going to be compromised this year than were last year. Some companies will go out of business as a result. State secrets will be revealed. A mysterious charge will appear on your credit card bill each month. Forbes

Cyber bill to put US in charge of global cyber security
In the wake of the SOPA outcry, another controversial bill that puts the US in charge of global cyber dealings is simmering. While industry and public uproar has stalled the controversial online anti-piracy bills known as SOPA and PIPA, American legislators are maintaining an aggressive stance on cybercrime, preparing to vote on a new bill that, if passed, will force other countries to play by US rules. Sydney Morning Herald

Police e-crime hubs announced
Three regional policing e-crime hubs are to be established in the UK, as the Government looks to boost the nation's protection against threats. IT PRO

Hackers break into gov't cyber security head's site
Arab hackers yesterday penetrated the website of the Tel Aviv University Security Studies Program, run by Prof. Isaac Ben-Israel, the head of the National Cyber Defense Authority. The website has resumed regular operations. Globes

Telecom firm KPN targeted by hackers
Telecoms firm KPN was targeted by hackers last month, who managed to break into the company's computer systems and access confidential private and corporate client details, Nos radio reports. DutchNews.nl

Syrian government loves the password 12345
The Syrian government could use some training on web security. Anonymous has released hundreds of e-mails the group claims it obtained by hacking a mail server used by Syrian President Bashar al Assad's office. But a look at the list of e-mail addresses and passwords released shows a hack wasn't necessary—all that was needed to gain access to Syria's sensitive information was one of the world's most common passwords: 12345. Of the 78 passwords Anonymous leaked, 31 used 12345. Others used easy to guess passwords like iloveyou, testing, system and 123456. Both iloveyou and 12345 made SplashData's list of the worst passwords of 2011. Canada.com

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

s.16(2)(c)

s.15(1) - Subv

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-08-12 8:19 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 8, 2012 / le 8 février 2012

Print Media / Médias imprimés

The unforgiving Internet
With over 400 cases of Internet-related child exploitation reported in Alberta last year, police agencies in the province are sending a reminder about practising safe surfing. Alberta Law Enforcement Response Teams' (ALERT) Internet Child Exploitation (ICE) units are among thousands of agencies around the world taking part in Safer Internet Day, doling out advice for parents, schools, and teens on ways to stay safe online. Edmonton Sun, 17

Car Hackers
Omar Ramos-Lopez was none too pleased when fired from his job at an Austin, Tex., car dealership in 2010. So he decided to get even. Getting revenge on former employers may not be a particularly novel reaction, but his choice of payback was cutting-edge. Texas Auto Center, where Ramos-Lopez worked, installs GPS units in leased cars that can remotely prevent the car from starting, or sound the horn on demand. Such functions come in handy if anyone happens to fall behind on their lease payments. National Post, A17

This bill is no SOPA
While hysterical predictions about copyright reform in Canada have been ratcheted up yet again, this time the claims are so outrageous that they can perhaps best be described as having "jumped the shark." Canadians are being told that Bill

C-11, an act to amend Canada's outdated copyright law, could be used to shut down popular websites such as YouTube, fundamentally change the Internet, sabotage online freedoms and hog-tie innovators. National Post, FP13

Online Media / Médias en ligne

MitB attacks not new, but increasing in scale and sophistication, says ActivIdentity
The BBC ecently highlighted so-called man-in-the-browser (MitB) attacks that enable cyber criminals to get around the latest generation of calculator-style two-factor online banking security devices, but this form of attack is really nothing new. Criminal hackers have been wreaking havoc with the ZeuS Trojan for around ten years, attacking everything from bank accounts to government networks, according to security firm ActivIdentity. Computer Weekly

Increasing Malware and Lax Security Biggest Fears for Users: Sophos
67 per cent of people worldwide feel that malware is now on the rise compared to what it was in 2010, according to security vendor, Sophos. The recent report, titled Security Threat Report 2012, made the discovery after people were asked to identify what they consider to be today's biggest threats on the Internet. CSO Online

UK Cyber Security Skills Are 'wholly Inadequate', Says Former Security Minister
The UK needs to significantly bolster its cyber security skills to fight against cyber threats, according to former security minister Baroness Pauline Neville-Jones. Neville-Jones, who is now the government's Special Representative to Business on Cyber Security, said that a lack of skills will hinder the UK's future ability to tackle the challenges of cyber crime. CSO Online

The Private Sector Responds to Cyber Threats
The House Energy Subcmte. on Communications and Technology begins an "aggressive review" of cybersecurity policies as outlined by Chairman Greg Walden (R-OR). According to a press release from the Subcmte., the hearing will focus on "the supply chain vulnerabilities, the man-in-the-middle attacks, the botnets, and the millions of hacking attempts that our cyberdefenses deflect." C-SPAN

Cyber Crime Fight To Be Bolstered By Three New Regional Hubs
Three new regional 'hubs' have been created to help fight cyber crime in the Humber, Northwest and East Midlands areas, it was announced on Wednesday. Cyber crime, or e-crime, includes offences ranging from online fraud, hacking and computer intrusion to distributing "malicious code". Huffington Post

Hactivists Are Like Criminals, Kaspersky Lab CEO Says
What's the difference between the global hactivist groups and true blood cyber crime? Not much, says Eugene Kaspersky, CEO of Kaspersky Lab, a major Russian IT security firm. "To me there is no difference between hactivists that ruin the internet environment and radical protesters who go out and start fires and blow up cars," he said during a conference in Cancun on Tuesday. Forbes

Let us join hands to make Internet safe
With the Safer Internet Day being observed on Feb 7, it's time for more countries to join hands and make concerted efforts to enhance Internet safety. Unfortunately, China is still often accused of cyber espionage. Such baseless accusations will only create a lose-lose situation and increase suspicion and misunderstanding among countries and regions, while the real troublemakers will go scot-free. China Daily

Power grid updates left system vulnerable to cyberattacks, auditors say
A rush by the Energy Department to use stimulus money to modernize the country's power grid has left the system vulnerable to cyberattacks, the agency's internal watchdog found. Inspector General Gregory H. Friedman found "shortcomings" in the cybersecurity plans of more than a third of the utility companies that got federal funding for "smart grid" projects — from incomplete strategies to prevent an attack to vague steps for stopping one if it started. Washington Post

Police bolster attack on cyber crime
Police are to bolster their campaign to target cyber criminals with the formation of three new regional e-crime control centres, senior officers will announce on Wednesday. The programme, to be launched at the Association of Chief Police Officers' cyber crime conference in Sheffield, is a response to the growing threat of online attacks, which are thought to cost the UK £27bn a year, according to Cabinet Office estimates. Financial Times

Open Group security gurus dissect the cloud: Higher or lower risk?

For some, any move to the cloud — at least the public cloud — means a higher risk for security. For others, relying more on a public cloud provider means better security. There's more of a concentrated and comprehensive focus on security best practices that are perhaps better implemented and monitored centrally in the major public clouds. ZDNet

ICS-CERT warns critical infrastructure companies about brute force attacks
The US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is warning critical infrastructure companies about brute force attacks against industrial control systems with secure shell (SSH) command-line access. Many organizations are seeing a large number of access attempts by remote attackers using SSH scans of internet-facing control systems, ICS-CERT said in a recent security advisory. Infosecurity Magazine

Safer Internet Day 2012: Schools and (ISC)2 Professionals Work Together to Educate Children
Parents are unaware of behavioural pitfalls that lead to their children's tiredness in lessons, exposure to abusive and predatory behaviour, and poor habits as they grow up. Schools across the United Kingdom today marked Safer Internet Day 2012 to tackle uninhibited online attitudes that leave children increasingly vulnerable to cyber bullying, abusive gamers, identity theft and malicious threats. 19 (ISC)2 Safe and Secure Online volunteers are out in force today, visiting children and parents in schools across the UK, including South Wales, Kent, Cumbria, Worcester and Teesside. Infosecurity Magazine

AntiSec leaks Symantec pcAnywhere source code after $50k extortion not paid
ymantec had said it would pay $50,000 to a group of hackers associated with Anonymous and AntiSec in order to keep its source code from being leaked online. This was part of a sting operation and email exchange between hackers and Symantec — except it was actually law enforcement posing as Symantec employee "Sam Thomas" and using a fake e-mail address. Computerworld

Has Facebook alerted you to WW3 breaking out? The good news is, it's NOT true. The bad news, you probably now have a computer virus
A fake news page saying, 'U.S. attacks Iran and Saudi Arabia, the begin (sic) of World War 3,' is the latest virus scam to circulate on Facebook. The story uses CNN's logos, and appears to offer video footage of a breaking news story, but says users need to upgrade their Flash video software to watch. Daily Mail

Malware's the next nuclear bomb: Kaspersky
Governments have begun to create malware in the form of cyberweapons, but given that there's no defence against them, they should be handled like nuclear bombs, according to Kaspersky Labs CEO Eugene Kaspersky. "Many countries have already announced they have military cyberdivisions," Kaspersky said at the Kaspersky Lab Cyber Conference 2012 in Cancun, Mexico, quickly recalling from memory a number of countries including the US, Japan, China, North and South Korea, and India. ZDNet

Internet Explorer dominates browser security as Google faces accusations
Internet Explorer 9 should be the go-to browser for organizations concerned about protecting machines from malicious downloads, according to a new study from NSS Labs: Microsoft's browser trounced rivals Chrome, Firefox, and Safari in the security company's more recent malware-blocking tests, a significant win considering that traditional malware remains among the most prevalent threats to users. InfoWorld

Kelihos botnet variant being assembled, claim Kaspersky and Microsoft
Microsoft insist the Kelihos botnet is dead despite reports last week suggesting otherwise; but the company acknowledged that a new botnet is being assembled using a variant of the original malware. The reappearance of a Kelihos-like army of hijacked computers shows just how difficult it is to eradicate a botnet, security experts said yesterday. Computerworld

St-Louis, Danielle

From: St-Louis, Danielle
Sent: February-08-12 2:38 PM
To: CCIRC Weekly Summary
Subject: CYBERSECURITY SUMMARY FOR CIOs
Attachments: PS-SP-#556287-v4-CYBER_EVENT_AND_NEWS_SUMMARY_FOR_14-28_JANUARY_2012.DOC; PS-SP-#527919-v6-FEEDBACK_FORM_FOR_WEEKLY_SUMMARY_FOR_EXECS.DOC

Good afternoon,

Please find attached the Cyber Security Summary for CIOs of significant cyber events and incidents reported to and observed by CCIRC, with analysis where required. Please note this product is *not* intended for wide circulation since it is still in the pilot phase. Here are the highlights:

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- [redacted]
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Strategic Program Manager, at Kenneth.bendelier@ps-sp.gc.ca.

Thank you,

Danielle St-Louis
Administrative Assistant | Adjointe administrative Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: 613-991-7738
Fax | Téléc.: 613-996-0995
E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca

Public Safety Canada | Sécurité publique Canada

CCIRC
Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

CYBER SECURITY SUMMARY FOR CIOs

s.15(1) - Int'l

Reporting Period: JANUARY 14-28, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-002

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations.

This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents reported over the last two weeks. There were reports of Canadian computers being used for malicious purposes, including attacking a US State Police website. A Canadian federal department linked to the signing of the international Anti-Counterfeiting Agreement (ACTA) was targeted through a malicious e-mail. There was also a message on the Internet by hackers to e-mail or launch a cyber attack against this Department. Internationally, hackers attacked government websites in US, Poland, Ireland and the EU to protest signing of ACTA. There are also continued reports of infected computers in Canada and around the world due to the Ghostclick fraud.

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- [redacted]
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

CCIRC Products Released during the reporting period:

- Cyber Flash on cyber attacks by Anonymous related to copyrights and intellectual property (CF12-001)

Noteworthy News in the Media:

- Israeli and Palestinian hackers exchange website attacks
- Hackers around the world protest current and intended anti-piracy measures:
    - MegaUpload's shutdown prompts hacker attacks on US government and music industry websites
    - Proposed US copyright law SOPA being protested: Certain websites elect to go dark for one day in protest; Anonymous attacks US government websites such as DOJ & FBI
    - Signing of the international Anti-Counterfeiting Agreement (ACTA) prompting hacker attacks on US, Poland, Ireland and European government websites.

NEW EVENTS REPORTED IN GOVERNMENT AND OTHER CANADIAN CRITICAL INFRASTRUCTURE SECTORS

Federal Government Sector

Operation SACTA (Stop Anti-Counterfeiting Trade Agreement): An online message signed by Anonymous posted a link to a Canadian federal department website, encouraging users to join the anti-ACTA movement, and attack if necessary. This message was posted on a popular text-file sharing website often used by hackers and is presumably encouraging cyber attacks on websites.

CCIRC provided available technical details to CTEC, the federal Government's CERT, for their further investigation.

> ***Comment:*** *There are provisions in the international Anti-Counterfeiting Trade Agreement that have important implications for content sharing on the Internet. This is a multi-lateral trade agreement which Canada has signed. Canada's new proposed copy-right law, Bill C-11 (former Bill C-32), is currently in Parliament at the second reading stage. There is a great deal of opposition to this agreement around the world by the on-line community and websites of other government have recently been attacked by hackers in protest.*

File Server (FTP) Login Credentials of a Federal Department posted on the Internet. CCIRC learned that the FTP login credentials of a federal department were posted on the Internet. CCIRC advised CTEC and provided known technical details.

> ***Comment:*** *FTP login credentials are used to gain access to a file sharing server where users may upload or download files. If a threat actor used these credentials, the result could be information compromise or the use of the server as a launch point for cyber attacks.*

Non-Federal Government Sector

Canadian computers being used in cyber attacks. CCIRC has learned that a cyber attack on a US State Police website was traced to a Canadian university's computer. In addition, another Canadian university's website was found to host malicious software that could infect website visitors. There were also reports of malicious software being hosted at a website hosting service provider's server and at two other unidentified Canadian entities.

CCIRC contacted the known Canadian organizations, with mitigation advice. The RCMP was informed of items of interest. CCIRC warned the website hosting service provider that the website in question was added to various block lists, possibly resulting in reduced legitimate traffic to this website. The malicious software from the university's website has been removed and is no longer being served.

> ***Comment:*** *It is possible that cyber criminals compromised these Canadian computers to use them remotely for malicious purposes, without their owners' knowledge. Organizations that offer computers for public use, such as universities, can be particularly susceptible to such compromises.*

Some Canadian Industrial Control Systems exposed to potential cyber attacks. A trusted international partner alerted CCIRC that information that could allow remote access to certain Canadian houses and apartment buildings' heating and air conditioning systems, was posted on the Internet. CCIRC alerted those responsible for the buildings and houses, offering mitigation advice. There is no report of any cyber attack in these cases at this time.

> ***Comment:*** *Many Industrial Control Systems (ICS), such as the ones used for heating and cooling buildings, are monitored or even maintained remotely through the use of certain software. It is likely that the technicians responsible for the set-up and maintenance of the heating systems for these buildings did not take cyber security into consideration or did not know the standard practices for protecting against such exposure.*
>
> *Since the Stuxnet virus attack on an Iranian nuclear facility, there has been a heightened awareness, both domestically and internationally, of cyber security for ICS. The trusted international partner who alerted CCIRC is focussed primarily on securing ICS. CCIRC recently moderated discussion at a ICS conference in Montreal.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonating Canadian financial institutions, tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in United States and Taiwan.

Cyber criminals also attempted to solicit personal information by impersonating Service Canada and Canada Revenue Agency.

CCIRC notified the impersonated financial institutions of these fraud attempts and the Government CTEC for the federal government cases. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website compromises and publicized vulnerabilities. CCIRC discovered a small health organization's website was defaced and offered mitigation advice. CCIRC also discovered a foreign Defence Department's website was compromised and contacted the organization, as well as CCIRC's equivalent organization. There was also a list of vulnerable websites posted on the Internet, which includes a Canadian university.

There were additional website compromises in the health and non-critical infrastructure sectors. Website usernames and passwords were posted on the Internet by hackers.

> ***Comment:*** *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

Ghostclick Fraud. There were new and continued reports of infected computers in three provincial governments, three provincial health organizations, an airport authority, an energy organization, two banks, 19 Canadian universities, a national media organization and 13 telecommunications companies.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are currently websites around the world for computer users to check whether their machine is infected by the malicious software used in this fraud. These sites can be found by searching with the keywords "dns-ok".

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in. CCIRC is also working with the Canadian Internet Registration Authority (CIRA) to provide notifications to affected users.

Operation Ghostclick was worldwide fraud campaign, exposed in late 2011 by the FBI. Cyber criminals hijacked users' Internet web searches and diverted them to websites that generated advertising and sales revenues. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

> ***Comment:*** *Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. CCIRC noted that the type and size of affected organizations varied, and were spread across Canada. The number of affected telecommunications companies more than likely indicates number of infected client computers of Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*
>
> *Organizations that offer Internet access, including those that provide publically accessible wireless networks, may be particularly vulnerable. In addition to the cooperative effort underway between CCIRC and CIRA, the Canadian government has launched a website for cyber security public education..*

CCIRC PRODUCTS RELEASED:

Hacktivist attacks related to proposed anti-piracy legislation. There have been coordinated distributed denial-of-service (DDoS) attacks on websites by hacktivists, claiming to be associated with Anonymous. There were multiple international targets, which included governments (Canada, US, Poland, Ireland and EU) and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

In response, CCIRC issued Cyber Flash CF12-001, titled *"Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property"*. This Cyber Flash, was sent to technical and security contacts within stakeholder organizations in government and other critical infrastructure

sectors . Government and industry organizations involved with the Copyright legislation and copyrighted material were encouraged to assess their risk exposure to coordinated DDoS attacks on their networks.

NOTEWORTHY NEWS IN THE MEDIA:

Israeli and pro-Palestinian hackers exchange website attacks. Open sources reported that the websites of Israel's main stock exchange, several banks and the national airline were attacked. Pro-Palestinian hackers claimed responsibility and even claimed to have posted the login credentials for several industrial control systems in Israel on the Internet. Shortly thereafter, there were reports of suspected Israeli hackers bringing down the Saudi Stock Exchange, interfering with the Abu Dhabi Security Exchange, and publishing e-mail addresses & passwords of 30,000 Arab Facebook users.

> ***Comment:*** *It is now becoming commonplace to carry real-world grievances into the cyber world. There could be an adverse impact from these attacks for Canadians and Canadian businesses that do business with the stock exchanges or banks involved. There were some media reports that some of the Israeli banks could block international access to their sites.*

Hackers around the world attack government websites to protest anti-piracy measures.

- **Retaliation for file-sharing service Mega Upload's shutdown:** Hackers, claiming to be with Anonymous, attacked the websites of the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music.

- **Signing of the international Anti-Counterfeiting Agreement (ACTA) and proposed US copyright laws:** Wikipedia shut down for one day to protest the proposed SOPA and PIPA bills. SOPA and PIPA were also cited by Anonymous as a reason for their attacks on the DOJ and FBI websites. Operation STOP ACTA by Anonymous also prompted hacker attacks on websites for US, Poland, Ireland governments as well as for the European Parliament.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

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

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-06-12 8:50 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted]; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

February 6, 2012 / le 6 février 2012

Print Media / Médias imprimés

Neo-Nazi IDs listed

Calgarians whose names have been connected to neo-Nazi and white-supremacist groups are angry that their personal IDs have been published on the Internet. The computer hacking collective "Anonymous" released the addresses and phone numbers of thousands of people who had registered with websites affiliated with white-supremacist causes. The sites included Blood and Honour and Local 1488. Calgarian Ryan Lorentz said he doesn't know how his name appeared on one of the lists: "I have no idea what that website is." Calgary Herald

Hackers Wiretap FBI Conference Call

The international hackers group known as Anonymous turned the tables on the Federal Bureau of Investigation by listening in on a conference call last month between the bureau, Scotland Yard and other foreign police agencies about their joint investigation of the group and its allies. Anonymous posted a 16-minute recording of the conference call on the Web Friday and crowed via Twitter: "The FBI might be curious how we're able to continuously read their internal comms for some time now." An FBI official said Anonymous had not hacked into the conference call or any other bureau facilities.

Instead, it had obtained an email giving the time, telephone number and access code for the call. "It's not really that sophisticated," said the official. National Post

Online Media / Médias en ligne

Anonymous takes down official Homeland Security website
The U.S. Department of Homeland Security's official website DHS.gov was hacked on Friday afternoon, and Anonymous is claiming responsibility. Also on Friday, Anonymous released an audio recording of a January conference call between FBI agents and Britain's Scotland Yard in which the hacktivist group Anonymous was discussed. The FBI released a statement confirming the authenticity of the recording and has since shifted its investigation to how hactivists linked to the Anonymous network managed to intercept a conference call. In the FBI statement, officials said: "The information was intended for law enforcement officers only and was illegally obtained. A criminal investigation is under way to identify and hold accountable those responsible." Examiner.com

German gov't endorses Chrome as most secure browser - Federal security agency touts sandbox, silent update as features that keep citizens safer online
Germany's cyber security agency today recommended that Windows 7 users run Google's Chrome browser, citing the application's sandbox and auto-update features. In a security best practices guideline, Germany's Federal Office for Information Security, known by its German initials of BSI, said Chrome was the best browser. "Your internet browser is the key component for the use of services on the Web and thus represents the main target for cyber-attacks," said BSI in its published advice. "By using Google Chrome in conjunction with the other measures outlined above, you can significantly reduce the risk of a successful IT attack." BSI ticked off Chrome's anti-exploit sandbox technology, which isolates the browser from the operating system and the rest of the computer; its silent update mechanism and Chrome's habit of bundling Adobe Flash, as its reasons for the recommendation. Computerworld

Kelihos : pas de résurrection mais un nouveau malware
Microsoft dément un retour aux opérations du botnet Kelihos. Un nouveau malware ayant des similitudes avec Kelihos est toutefois apparu. La firme de Redmond revient sur la cas de Kelihos pour apporter des précisions. Pour Microsoft, qui a œuvré au démantèlement du botnet avec l'aide de Kaspersky Lab et Kyrus Tech, le botnet n'a pas ressuscité. « À l'heure actuelle, Kaspersky Lab et Microsoft n'ont aucune preuve que le botnet qui a été démantelé en septembre 2011 est retourné sous le contrôle de cybercriminels ou a repris des activités de spam » Génération-NT

Spammers exploit calendar events
Spammers are using holidays and major events to make their mail more appealing. This is according to the Symantec.cloud Intelligence Report, which shows that more than 10 000 unique domain names were compromised with a redirect script written in PHP that contained a reference to the New Year in the file name. These redirect scripts were hosted on compromised Web sites, and links to these were included in spam e-mails, says Symantec. IT Web Security

Hackers may be able to 'outwit' online banking security devices - Investigators probe malware threat to 2-factor authentication
Hackers may already able to use malware to outwit the latest generation of online banking security devices, security watchers warn. An investigation by BBC Click underlines possible shortcomings in the extra security provided by banking authentication devices such as PINSentry from Barclays and SecureKey from HSBC. Using such two-factor authentication devices means that even if hackers trick consumers into handing over their bank login passwords they still won't be able to raid online banking accounts. UK Register

Google launches Android Bouncer
Google has announced its "Bouncer" service which scans for malicious software on Android smartphones amid a massive spike in use of the phones. "Here's how it works: Once an application is uploaded, the service immediately starts analysing it for known malware, spyware and trojans. It also looks for behaviours that indicate an application might be misbehaving, and compares it against previously analysed apps to detect possible red flags," Hiroshi Lockheimer, Android vice-president of engineering wrote on the Google blog. Google has come out fighting suggestions that its Android platform poses a security threat to smartphones. News 24 (South Africa)

Android : Counterclank ne serait pas un cheval de troie, Symantec se rétracte et rejoint l'avis de Lookout
Le cheval de troie Counterclank découvert par Symantec n'aurait en effet pas des fonctionnalités malveillantes selon la firme de sécurité qui revient sur sa position. Counterclank avait été identifié au sein de 13 applications populaires et aurait infecté près de cinq millions de terminaux Android selon Symantec. Le malware lit les données comme l'historique du navigateur, les informations d'identité, les données de localisation, etc., et transmet celles-ci à un serveur distant. L'éditeur Lookout Mobile avait par contre identifié Counterclank comme appartenant à un réseau de publicité agressif.

Symantec rejoint donc la position de Lookout, et pense que le code d'Android. Counterclank proviendrait d'un kit de développement logiciel (SDK), distribué aux tiers pour les aider à monétiser leurs applications principalement par la recherche. Développez.com

Un trojan polymorphe sur Android détecté par Symantec
Des chercheurs de Symantec ont identifié un trojan pour Android qui envoie des SMS à des numéros surtaxés. La particularité de ce trojan est qu'il modifie son code à chaque fois qu'il est téléchargé pour contourner les antivirus. Symantec lance un avertissement sur l'apparition d'un cheval de Troie pour Android qui envoie des SMS à des numéros surtaxés. Le virus modifie son code à chaque téléchargement. Cette technique est connue comme le polymorphisme serveur et a existé pendant des années sur les malwares pour PC. Les cyber-criminels commencent à l'adopter pour les mobiles. A la différence du polymorphisme local où le malware modifie son code à chaque fois qu'il est exécuté, le polymorphisme serveur transforme certaines parties du cheval de Troie à chaque téléchargement. Le Monde Informatique

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

Hayward, Jane

From: Glazer, David on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-06-12 8:10 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
February 6, 2012 / le 6 février 2012

MINISTER / MINISTRE

Harsher sentences for pot growers than for pedophiles caught PM's eye
Media reports that some pot growers will face harsher mandatory-minimum sentences than child rapists under the Conservative government's new crime bill were enough to catch the attention of Prime Minister Stephen Harper. A request by The Canadian Press for cabinet records on the controversial omnibus crime legislation turned up a single document - much of it blacked out under a broad, discretionary exemption in the Access to Information Act. The Oct. 11, 2011, "memorandum for the prime minister" says its purpose was to inform Harper about the controversial sentencing provisions "in light of recent criticism in the media." Bill C-10, the omnibus crime bill, is currently being studied by the Conservative-dominated Senate, where Justice Minister Rob Nicholson has confirmed some flaws will be corrected. **Public Safety Minister Vic Toews** attempted to have those amendments adopted in late November after the bill had left the House of Commons justice committee, but was ruled out of order by the Speaker. Red Deer Advocate, D4 (The Telegram)

Un bateau nauséabond
Ce sont les deux bateaux par lesquels le scandale a été créé. Les bateaux dont s'est servi le gouvernement Harper pour monter son propre bateau justifiant l'injustifiable. L'Ocean Lady, en octobre 2009. Puis, le MV Sun Sea, en août 2010. A bord de ces deux navires qui ont atteint les côtes de la Colombie-Britannique, 600 demandeurs d'asile du Sri Lanka. Ces bateaux ont été érigés en symbole par le gouvernement conservateur. Épouvantails commodes pour qui veut bafouer les droits des réfugiés, préjugés en vogue à l'appui. Les voyant arriver, **le ministre de la Sécurité publique Vic Toews** a tout de suite brandi la menace de l'invasion. Il a dit craindre que d'autres bateaux remplis de Tamouls prennent d'assaut le Canada. Il a invoqué d'importants problèmes de sécurité, des liens avec des organisations terroristes... La Presse, A3

*** Pedophile site appears legal**
Alberta's top cop doesn't think plans for a controversial website outing convicted pedophiles will run into any legal roadblocks. Solicitor General Jonathan Denis, who's also a lawyer, said while he doesn't necessarily support the move by Canada Family Action, a Christian group set to launch findapedophile.com next month, he doesn't think there will be any legal impediments. Denis also met with federal **Public Safety Minister Vic Toews**, who was very supportive of the proposal. Calgary Sun, 5

*** Prison porn pervert - Sex-killer claiming to embrace aboriginal culture a slammer smuggler**
A Haitian-born sex-killer's embrace of Canadian aboriginal traditions and culture didn't stop him from breaking prison rules by hoarding and displaying porn in his cell, helping an inmate smuggle booze and becoming involved in a jailhouse disturbance over the last few years. Gregory Bromby's recent bid for day parole from a federal prison in Manitoba made national headlines after he was granted a culturally-sensitive, "elder-assisted" hearing despite not being aboriginal. His being allowed to make use of the forum sparked outrage from the father of Tara Manning, the 15-year-old girl Bromby sexually assaulted and stabbed 51 times in the mid-90s. **It also drew concern and a promise of parole reform from the office of federal MP and Public Safety Minister Vic Toews.** Winnipeg Sun, 3 (Edmonton Sun)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Top security for bird flu studies**
If Canadian scientists want to conduct research on H5N1 flu viruses modified to enhance their ability to spread, the work will have to be done in laboratories with the top level of biosecurity, the Public Health Agency of Canada says. For the

time being, the advice is moot; the viruses in question are locked up in labs in the Netherlands and the United States. And while controversy rages over whether the teams that created them should be able to publish their work in scientific journals, it's unlikely those labs will share samples, especially across international borders. Red Deer Advocate, D5

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Alleged terrorist's partner wrestles with competing realities
Mr. Sharif has sat in an Edmonton jail since his arrest as the United States attempts to have him extradited to face seven terrorism-related charges in New York state. In December, U.S. President Barack Obama signed a new law into effect allowing accused terrorists to be held indefinitely in military prisons if they're tied to al-Qaeda or related terrorist groups. Justice Canada doesn't believe it would apply in this case, but some lawyers and observers say that's simply wrong. The law is, at best, untested and murky, and Mr. Sharif could be held. Canada doesn't extradite people if they'll face the death penalty. Indefinite detention, however, is new ground. And the only thing standing between Mr. Sharif and that possible fate under an unproven law is a brief extradition hearing and the chance of potential intervention, however slim, by Justice Minister Rob Nicholson, who signs off on all extraditions. Globe and Mail, A8

*** Terror arrest a wake-up call: Expert**
Finding foreign terrorists on home soil should come as no shock to Canadians who may be partially to blame, says an Edmonton professor of international relations. The arrest of Edmonton-based alleged terrorist Sayfildin Tahir- Sharif -- whose extradition hearing was recently delayed -- demonstrates the potential "that there are people self-radicalizing here, and how easily extremist predilections can go unidentified," said University of Alberta political science professor Andy Knight. London Free Press, B5 (Edmonton Sun, Toronto Sun, Whig-Standard, London Free Press)

*** Le Sun Sea, socle étroit du projet de loi C-4**
Après l'arrivée au Canada de l'Ocean Lady et du MV Sun Sea, deux bateaux remplis de demandeurs d'asile tamouls, le gouvernement de Stephen Harper a annoncé une modification en profondeur de la Loi sur l'immigration et la protection des réfugiés : le projet de loi C-4 est l'un des gros morceaux de la rentrée parlementaire. Mais un an et demi après l'accostage du Sun Sea, seuls 14 demandeurs ont été expulsés vers leur pays d'origine, le Sri Lanka. Et aucune accusation n'a encore été portée contre les passeurs. Dans la communauté tamoule, on s'interroge : le Sun Sea n'est-il pas un socle bien étroit pour la loi C-4 ? Seuls six d'entre eux sont encore détenus par l'Agence des services frontaliers du Canada (ASFC), et 14 ont été expulsés pour des raisons de sécurité. La Presse a communiqué avec les cabinets des ministres de l'Immigration et de la **Sécurité publique** afin de commenter ces chiffres. Ils nous ont renvoyés aux fonctionnaires de l'ASFC, où notre demande est restée lettre morte. La Voix de l'Est, 16 (La Presse)

CYBER SECURITY / CYBERSÉCURITÉ

*** Neo-Nazi IDs listed**
Calgarians whose names have been connected to neo-Nazi and white-supremacist groups are angry that their personal IDs have been published on the Internet. The computer hacking collective "Anonymous" released the addresses and phone numbers of thousands of people who had registered with websites affiliated with white-supremacist causes. The sites included Blood and Honour and Local 1488. Calgarian Ryan Lorentz said he doesn't know how his name appeared on one of the lists: "I have no idea what that website is." Calgary Herald, A16

*** Hackers Wiretap FBI Conference Call**
The international hackers group known as Anonymous turned the tables on the Federal Bureau of Investigation by listening in on a conference call last month between the bureau, Scotland Yard and other foreign police agencies about their joint investigation of the group and its allies. Anonymous posted a 16-minute recording of the conference call on the Web Friday and crowed via Twitter: "The FBI might be curious how we're able to continuously read their internal comms for some time now." An FBI official said Anonymous had not hacked into the conference call or any other bureau facilities. Instead, it had obtained an email giving the time, telephone number and access code for the call. "It's not really that sophisticated," said the official. National Post, A11

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

*** Canadian fraud hits foreign markets**
Canadian investors suffer more from market fraud that occurs on other nations' stock exchanges than in Canadian ones. These were the findings of Project Stockholder, a June 2011 internal report by the RCMP criminal intelligence branch that

was obtained by the Financial Post under the Access to Information Act, although some sections were withheld for security reasons. It is the first and only intelligence overview of capital market fraud in Canada since the RCMP Integrated Market Enforcement Team, or IMET, was created in 2003. National Post, FP1

*** Dramatic ice rescue in Bouctouche**
A man in his fifties was rescued by RCMP members in a helicopter yesterday morning after wandering out a couple icy kilometres on the Bouctouche Bay, nearing open waters of the Northumberland Strait. Times & Transcript, A2

*** UN TIERS PUNIS POUR DES AFFAIRES DE DROGUE**
Le tiers des 123 entrepreneurs de construction du Québec inscrits sur la fameuse liste noire de la Régie du bâtiment n'y figurent pas pour des questions de collusion ou d'évasion fiscale, mais plutôt pour des condamnations pour possession ou trafic de drogue, révèle une analyse effectuée par l'Agence QMI. Cette donnée était passée inaperçue avant que l'Agence QMI ne passe cette liste noire au peigne fin. Ce n'est rien pour rassurer ceux qui s'inquiètent des liens troublants entre le crime organisé et le monde de la construction. Journal Montreal, 5

*** La fille d'un caïd gravitait dans le giron familial**
Le travail de policier semblait tellement ancré dans sa famille qu'on l'aurait cru au-dessus de tout soupçon. Mais de nouveaux détails qui filtrent sur la "taupe du SPVM" montrent qu'à la fin de sa vie, Ian Davidson a caché à ses collègues au moins une fréquentation "dérangeante". Et que sa fameuse expertise technologique pouvait aussi se retourner contre la police lorsqu'il l'utilisait pour son propre compte. La Presse, A5

*** Wanted man sought in stabbing**
A man already wanted on a charge stemming from a Fort Qu'Appelle homicide is now being sought for a stabbing in the Maple Creek area. The focus of both probes is Preston Clarence Buffalocalf, a 25-year-old from the Okanese First Nation. RCMP issued a news release late Friday saying Buffalocalf was being sought in connection with a stabbing on the Nekaneet First Nation, near Maple Creek. A 24-year-old man was taken to hospital on Thursday with unspecified injuries. Police did not find out about the incident until the next day. Regina Leader-Post, A1 (Saskatoon Star-Phoenix)

*** Should extradition be different for natives? - Drug smuggling case raises issue for courts**
Lawyers for Zachary Leonard, 24, a member of the Rainy River First Nations in northwestern Ontario, are urging the Ontario Court of Appeal to block his extradition to Minnesota on charges of drug smuggling, arguing it would discriminate on the basis of race and violate his constitutional rights as an aboriginal person. Those include, they say, an enhanced right to remain in Canada. They want Justice Minister Rob Nicholson to prosecute Leonard at home, an option under the Canada-U.S. extradition treaty. But so far, Nicholson has refused. Toronto Star, A6

*** Pipeline opponents take to streets**
First Nations and residents of a community on British Columbia's North Coast are protesting a proposed pipeline which would carry crude oil from Alberta to the west coast for tanker shipment to places like China. The "No Oil Tankers" rally kicked off Saturday morning in a Prince Rupert, B.C. park and wound its way to a civic centre where First Nations leaders were scheduled to speak and musicians like Bif Naked were expected to perform. Marven Robinson, who is a member of the Gitga'at Nation, says his band organized the event. Charlottetown Guardian, A5; Vancouver Sun

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

*** Chasing Truth**
Cameron Ward once had faith in B.C.'s Missing Women Commission of Inquiry, called to examine how police investigated the disappearance of dozens of sex trade workers from Vancouver's notorious Downtown Eastside. From 1997 to 2002, the period under review, prostitutes were murdered by pig farmer Robert "Willie" Pickton, all along a prime police suspect. Mr. Ward is a lawyer who represents the families of 23 missing and murdered women at the inquiry. Five months into public hearings, his faith in the process has crumbled. National Post, A8

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Harm reduction vs. don't touch the stuff
Thirteen of those total deaths, which all occurred late last year and last month, have been linked to paramethoxymethamphetamine (PMMA) a chemical turning up inside Canadian Ecstasy. The broader public health community has backed the harm reduction approach, Dr. Kendall said, but it has run up against some political ambivalence, including from a federal government pushing a tough on-crime mandate. Prime Minister Stephen Harper

kept harm reduction out of his $63.8-million national anti-drug strategy. When it was unveiled in 2007, he said harm-reduction efforts such as Vancouver's Insite needle exchange clinic were a "second-best strategy at best." National Post, A6

*** We need a fact-based policy**
An opinion piece states, "We need a government that prioritizes helping the poor and middle-class, that promotes strong social programs while also emphasizing economic prosperity and job creation. We need a government that bases its decisions not on pre-set notions driven by ideological assumptions, but bases its decisions on facts, evidence and research. Unfortunately, this does not seem to be the modern conservative approach to government... The fact that the Harper government is targeting Old Age Security - which is not under financial pressure and which is important to keeping many seniors out of poverty - is especially appalling as this government has been increasing spending in areas we do not need - building unneeded prisons as part of the Conservative "tough on crime" approach and spending on fighter jets we also do not need." Telegraph-Journal, A5

*** Ashley Smith was destroyed by prison system: mother**
As most know, Ashley Smith was a troubled Moncton teen whose term of probation for throwing apples at a mail carrier eventually led to an accumulation of more than 100 charges and four years in custody, mostly for incidents that occurred while she was behind bars, mostly in isolation. She died while on suicide watch as guards looked on. While Coralee Smith has spoken to reporters on a few occasions in the past, the speaking engagement in the MacNaughton High School auditorium stands out for the size of the audience who got to hear some of Ashley's family's story. Coralee and Herbie recently donated $20,000 to assist programs to help women who have been incarcerated, a gift acknowledged by Kim Pate, the executive director of the Canadian Association of Elizabeth Fry Societies who shared the stage with Coralee. As for the Women &Wellness event, it raised $41,720 for a number of local mental health initiatives. Times & Transcript, A1

*** Projet de loi C-10 - Harper s'est informé des peines minimales**
Des reportages rapportant que des producteurs de marijuana feraient face à des peines minimales plus sévères que les agresseurs d'enfants en vertu du nouveau projet de loi conservateur sur le crime ont suffi à capter l'attention du premier ministre Stephen Harper. La note d'information adressée au premier ministre, qui a été largement censurée, se termine en indiquant que «des analyses supplémentaires» seront nécessaires si les peines minimales sont approuvées dans le projet de loi du gouvernement -- qui se retrouve maintenant devant le Sénat. Le ministre fédéral de la Justice, Rob Nicholson, a par ailleurs mentionné que certains défauts du projet de loi seront corrigés. Le Devoir, A3 (Le Droit, L'Acadie Nouvelle, La Voix de l'Est, La Tribune), The Record (The Telegram, The Chronicle-Herald)

*** Moncton to host new parolee program**
A new program is in place to help people who are released from prison and it's a joint effort between the Findmyway Community Network in collaboration with the Moncton district parole office. Project organizers are seeking volunteer mentors to offer support to people released from prison in an attempt to break the cycle of crime and connect them to the community. Findmyway project facilitator Bert Johnson says a "Preparing for Release" pilot project was undertaken in the latter part of 2009 and the beginning of 2010. It was offered at Dorchester Penitentiary and 15 offenders who were nearing their release date participated in the program. They were teamed up with mentors and the results were overwhelmingly positive. At follow-up meetings on the subject, which included many CSC employees, it was agreed that the program was a success and should be expanded. Times & Transcript, A1

*** Parole rules punish victim**
An opinion piece states, "Family members mourning the loss of a Red Deer couple killed by a drunk driver on Feb. 7, 2010, are being shortchanged by Canada's parole process - as are other victims of crime. And if they feel the offenders' rights supersede their rights under the system, they are bang on the mark. Canada's ombudsman for crime victims agrees and says this obvious imbalance must be corrected now. There's a general consensus among crime victims in Canada that offenders' rights surpass those of the victims. The ombudsman said in her report that information to crime victims under the current parole system is strictly limited and it is time to strike a better balance. O'Sullivan said many victims are frustrated by rules that limit their participation at parole hearings." Red Deer Advocate, A4

*** Cacher son infection au VIH est-il un crime?**
La Cour suprême entendra deux causes, mercredi, pour déterminer si le fait de ne pas dévoiler à ses partenaires sexuels qu'on est atteint du VIH est un crime, et ce, même si les risques de transmission sont faibles. Le plus haut tribunal du pays doit statuer sur les appels déposés par le Manitoba et le Québec sur cette question. Les procureurs soutiennent que les gens atteints du VIH doivent informer leurs partenaires sans tenir compte des risques de transmission. Les partenaires peuvent alors décider s'ils veulent aller de l'avant en connaissant ces risques. Selon ceux qui défendent les droits des personnes atteintes, cette position les criminalise et ne prend pas en compte les données scientifiques. Tous les observateurs espèrent que la Cour suprême va clarifier sa décision de 1998 qui a été interprétée de façons

différentes par les juges dans tout le pays. Le Soleil, 12 (La Voix de l'Est, L'Acadie Nouvelle, Le Nouvelliste, Le Droit, Le Devoir), The Telegram (Red Deer Advocate)

*** Mais arrêtons de dorloter les criminels**
Un article d'opinion déclare, « Plusieurs ont joué le rôle de "vierge offensée" à la suite des propos du sénateur Boisvenu. Ce dernier a dit tout haut ce que plusieurs pensent tout bas. Quand un criminel se fait prendre et qu'il est condamné à la prison, on déroule le tapis rouge pour lui. Des psy analysent et ré-analysent le mental de cet individu en plus de lui fournir un logement convenable ainsi qu'une nourriture de qualité. On lui fera également faire des activités pour l'occuper. Lorsqu'il aura purgé le tiers de sa peine, il sera encore évalué et un comité décidera à la suite des recommandations médicales si ce criminel représentera un risque pour la société. Si ce dernier a bien joué le jeu, il sera remis en liberté. L'individu qui a assassiné la fille de monsieur Boisvenu était justement un récidiviste qui n'aurait jamais dû être remis en liberté. Ce criminel a bénéficié de tous ses droits alors que la victime, monsieur Boisvenu et sa famille ont été ignorés par le système. C'est précisément ce qui irrite le sénateur. Le système judiciaire accorde des droits privilégiés aux criminels et pratiquement rien aux victimes d'actes répugnants… » Le Nouvelliste, 15

*** Positive partnership**
Community policing means a lot more these days than walking the beat. In keeping with a community focus, the Fredericton Police Force has two Neighbourhood Action Teams, with offices on both the north side and the south side of the city. The Daily Gleaner, A10

*** Boisvenu speaks for many Canadians**
An editorial states, "While it may not have been tactful for Tory Sen. Pierre-Hughes Boisvenu to suggest a rope be placed in the prison cells of the most heinous killers so they could have the option of suicide, we do know most Canadians would agree with him. Most Canadians are fed up with victims being ignored while murderers get coddled, and their rights to privacy are honoured to the point of dishonouring the victims… For almost 30 years, until cancer took out this cancer, Canadian taxpayers had to pay out millions for serial killer Clifford Olson's room and board in protective custody… There are now politically-motivated attempts by the opposition to have Sen. Boisvenu removed from the justice committee now studying Bill C-10, the government crime bill that will raise minimum sentences for serious criminal offences. Why? Because he dared to say what the majority of Canadians think?... In 2002, his daughter was raped and murdered by a serial killer and, despite that horror in his life, he is not a proponent of the death penalty. He is well known, however, for being a victims' rights advocate. He therefore belongs on that committee, and has tragically earned the right to be there." Calgary Sun, 14 (Ottawa Sun, Edmonton Sun)

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Do we cut pensions to buy F-35s?**
An opinion piece states, "The Harper government does not admit to any imperfections - and why should it? It has a majority and in its ranks it boasts "the best finance minister on the planet," as the prime minister called Jim Flaherty at Davos a couple of weeks ago… Common sense is bypassed on other fronts. Spending billions to build more prisons at a time when the serious crime rate is falling is one issue that cries out for rethinking. So is the scrapping of the firearms registry over the objection of police forces, who claim the registry helps to save lives. What if the police are right and Conservative strategists are wrong?..." The Record, A7

*** 100,000 reasons to mute latest Conservative attack on CBC**
An opinion piece states "Heritage Minister James Moore releases the earthshaking discovery that of the people who toil at the CBC, 730 earn $100,000 a year or more! Can you believe it? Eighty-seven per cent of CBC employees do not - let me repeat, DO NOT - fall into the top five per cent of income earners in Canada. Polls suggest most of us think the likes of Rex Murphy, Rick Mercer, Hockey Night in Canada and The National are pretty good value. **On the other hand, Conservatives budgeted $1 billion to host a vanity project - the G8 and G20 summits** - involving countries whose recent economic performance suggests, to quote W.A.C. Bennett, they 'couldn't run a peanut stand.' About $50 million of that was siphoned off to fund "legacy" projects like gazebos in the riding of Tony Clement, the minister who now heads up the Treasury Board and who declines to report how many staff in the Prime Minister's Office earn more than $100,000 a year and who they are. 'Nuf said." Vancouver Sun, A1

INTERNATIONAL / INTERNATIONAL

'Tired of Putin'

Russian dissident Boris Nemtsov doesn't expect to see a touch of the Arab Spring in Moscow's winter, but he aims to bring tens of thousands of protesters into the streets Saturday to demand political reform and an end to Vladimir Putin's presidential ambitions. National Post, A15

*** Israeli attack on Iran feared**
For the first time in nearly two decades of escalating tensions over Iran's nuclear program, world leaders are genuinely concerned an Israeli military attack on the Islamic Republic could be imminent -- an action many fear might trigger a wider war, terrorism and global economic havoc. High-level foreign dignitaries, including the UN chief and the head of the American military, have stopped in Israel in recent weeks, urging leaders to give the diplomatic process more time to work. Israel seems unmoved, and U.S. Defence Secretary Leon Panetta has reportedly concluded that an Israeli attack on Iran is likely in the coming months. Winnipeg Free Press, A9 (The Record, Red Deer Advocate, Hamilton Spectator)

*** Al-Qaeda behind wave of terror in Nigeria**
Al-Qaeda operatives in North Africa have helped to transform Boko Haram into a terrorist group capable of killing hundreds in sophisticated attacks. Ottawa Citizen, A7

*** Taliban can depend on NATO to boost their morale**
An opinion piece states "Last week, on the eve of a major NATO summit meeting in Brussels, a rather bleak report was leaked regarding the future fate of Afghanistan. After conducting extensive interviews with more than 4,000 Taliban prisoners, the survey concluded the insurgents' morale remains high and these religious fighters remain convinced that once NATO withdraws its combat forces from Afghanistan in 2014, the Taliban will reclaim the country. Heading into last weekend's NATO summit, U.S. Secretary of Defence Leon Panetta announced that, in view of the financial crisis in Europe, plans need to be made to downsize future Afghan security forces. In other words, we are going to continue recruiting, arming and half-training a demoralized cadre of some 400,000 Afghans for two more years, then cut their funding, lay them off and withdraw our NATO combat forces at the same time. No wonder the morale of those Taliban prisoners is so high." Halifax Chronicle-Herald, B2

OTHER / AUTRE

PM fears Iran's plans
Prime Minister Stephen Harper insisted he is not preparing the Canadian public for war with Iran but, in his starkest warning yet, said he fears the regime in Tehran is prepared to use nuclear weapons, if it manages to produce them. National Post, A1

Turf wars shouldn't block a national securities regulator
Abandoning the idea of a national securities regulator would be the easy way out. To his credit, Finance Minister Jim Flaherty has made it clear he isn't ready to let the issue die, even after the Supreme Court slapped down the federal government in December for constitutional "overreach." The court, he pointed out, recognized that Ottawa still has a legitimate role in setting national standards, collecting data and mitigating risks that threaten financial markets. The current patchwork of 13 provincial and territorial securities regulators also makes the industry particularly vulnerable to fraud and organized crime, according to a report commissioned recently by the **Public Safety** department and obtained by The Canadian Press under the Access to Information Act. "Complicated multi-jurisdictional regulatory systems" make the industry vulnerable, the report found. Globe and Mail, B1

'Honour killings' are sins
A group of Canada's leading Muslim clerics has issued a fatwa against so-called "honour killings," just a week after three members of an Afghan Canadian family were convicted of a quadruple murder that triggered a national debate about cultural values. Vancouver Sun, B2 (London Free Press); * The Record (The Guardian); * La Presse

*** Brutality allegations probed**
Montreal police are investigating allegations of brutality among their ranks after a video of an officer hitting a protester surfaced on the Internet. It comes on the heels of a decision to suspend two Montreal cops for the repeated Tasering in 2007 of a man who died four days after his arrest. Windsor Star, B1 (Edmonton Journal, Daily Gleaner, Times & Transcript)

*** PM likely to ask China about jailed local man**
The plight of a Burlington man in a Chinese jail for what supporters say are trumped-up terrorism charges is expected to be raised by Prime Minister Stephen Harper during his visit to China. Hamilton Spectator, A1

*** Let's discuss mandatory voting**

An opinion piece states, "Let's be honest: Canadians are becoming political dropouts. There's a declining sense of civic duty or democratic responsibility. Growing numbers of Canadians simply can't be bothered to make it to the polling station anymore... In every jurisdiction that has introduced mandatory voting, voter turnout has increased by at least 10 to 15 per cent. This increase has also been most conspicuous among younger voters, who are now compelled to vote. No one is suggesting, of course, that people have to vote a certain way or can't spoil their ballot by not marking an X anywhere. But they do have to show up at the polls if they want to express their displeasure with politicians or the political system as a whole. Many critics will be quick to say that there is something inherently problematic with a voting system that forces citizens to vote in a "free" and "democratic" society. And what about the depressing prospect of uninformed voters actually determining electoral outcomes? Others will say that it won't fly here, that it is repugnant, and that people are entitled to choices in this country... Fine. But then what is the solution to stemming the precipitous drop in voter turnout that we are staring at in the coming years? Do we really want to see only 40 or 50 per cent of Canadians voting on election day?..." The Guard, A7

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-05-12 8:29 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
February 5, 2012 / le 5 février 2012

MINISTER / MINISTRE

Letters to the Editor Column

A letter written by **Public Safety Minister Vic Toews states**, "NDP MP Pat Martin (Winnipeg Centre) once again demonstrated his willingness to use inappropriate language and engage in vicious personal attacks when he used an obscenity to refer to Senator Pierre-Hugues Boisvenu on Wednesday. Martin previously refused to apologize for his use of social media to direct obscenities at those who have challenged him. The NDP and MP Martin should apologize for the shameful personal attack that has been directed at Senator Boisvenu. Pat Martin's constituents, and indeed all Canadians, would be better served if the MP and his soft on crime party, would direct their outrage and vitriol at the criminals who victimize innocent, law-abiding Canadians rather than at a Senator whose family has suffered a terrible loss at the hands of a repeat offender." Winnipeg Sun, 12

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

No damage reported from 5.6 earthquake

A noon shaker off Ucluelet Saturday went largely unnoticed by most of the town's residents. The 5.6-magnitude earthquake was logged by Natural Resources Canada at 12: 05 p.m. The epicentre was about 180 kilometres west of Ucluelet and 337 kilometres west of Victoria, at a depth of 12.8 kilometres. The relatively mild strength and distance meant there was no risk of a tsunami and no damage reported, said Taimi Mulder, federal earthquake seismologist. In the Officials Sports Lounge in Ucluelet, manager Dale Holliday didn't feel the earth move and neither did his customers. At the Water's Edge Resort, the reaction was much the same. Times Colonist, A6; Edmonton Sun; Le Journal de Montréal

CYBER SECURITY / CYBERSÉCURITÉ

WORLD IN BRIEF

A group linked to the hacker network Anonymous on Saturday said it attacked the Swedish government's website, bringing it down for periods of time by overloading it with traffic. CyberForce used Twitter to claim responsibility, saying "We have succeeded in the attack against the government." It also indicated it may launch more attacks at around midnight Saturday, saying "this op starts at 24.00," but it was not immediately clear whom the targets for those attacks may be. The group said it had used a denial of service attack against the government, which essentially swamps a website with false users. Chronicle-Herald, A8

Hackers post audio of FBI secret call

Hacker group Anonymous, in an embarrassment for law enforcement, released a recording Friday of a conference call between the FBI and Scotland Yard discussing operations against the hacking collective. The Federal Bureau of Investigation confirmed the authenticity of the nearly 17-minute recording posted on YouTube and other sites and said it was "intended for law enforcement officers only and was illegally obtained." "A criminal investigation is under way to identify and hold accountable those responsible," the FBI said in a statement. Along with the audio recording, Anonymous also posted online the email invitation from an FBI agent setting up the call for Jan. 17. According to the FBI, no agency computer systems were breached in connection with the incident. Graham Cluley of computersecurity firm Sophos said the hackers were apparently able to access the call "because they have compromised a police investigator's email account." The Province, A22

Online activists claim to name Alberta white supremacists
Calgarians whose names have been connected to neo-Nazi and white-supremacist groups are angry that their personal identification has been published on the Internet. Earlier this week, an informal computer hacking collective that operates under the name "Anonymous" released the addresses and phone numbers of thousands of people who had registered with websites affiliated with white-supremacist causes. Of the more than 70 Canadian residents revealed, more than a dozen were listed in Calgary and Edmonton. Kelly Ernst, a board member with the Rocky Mountain Civil Liberties Association, agreed the computer collective went too far. Calgary Herald, A3

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

RCMP struggling to fill jobs, internal documents show
Internal RCMP documents show the force scrambling to fill jobs in B.C. despite years of warnings that chronic understaffing is putting police and the public at risk. One in 10 Mountie positions in B.C. sits empty, says a management report obtained by the Times Colonist. Jobs left unfilled due to medical, parental and other forms of extended leave push the vacancy rate to almost 16 per cent provincewide and to 17.4 per cent on Vancouver Island. It raises the question of how the RCMP would come up with the officers to create a new 35-member detachment in Esquimalt, should the provincial government agree to that municipality's decision to do so. A separate but similar 2007 report warned that the RCMP risked burning out its members because their workload was growing while the number of resources thinned. Yet it's clear the problem has not been addressed in many areas of B.C., with detachments regularly calling in officers on overtime or having to borrow members from other detachments to reach minimum staffing levels. But RCMP brass aren't willing to acknowledge shortages are affecting front-line policing. Liberal Senator Colin Kenny, who has said for years the national force is understaffed by 5,000 to 7,000 officers, said the officer shortage will get worse in years to come as more senior officers retire. Instead of the Conservative government passing tougher laws which will put more people behind bars, it should be investing in more national police officers to prevent crime, Kenny said. Times Colonist, A1

Island Mounties run off their feet
In Duncan, RCMP officers are running from call to call, scrambling to keep up and letting the proactive policing that can prevent crime fall by the wayside. In Sooke, the detachment commander routinely calls in Mounties on overtime, including from other detachments, as well as reserve constables just to avoid falling below minimum staffing levels. These are scenarios reflected in internal RCMP documents that show one in 10 Mountie positions in B.C. are vacant. Staffing shortages are even higher due to officers off work on extended leave. The shortage of Mounties has been a long-running concern for the province and the municipalities that contract with the RCMP and pay up to 90 per cent of policing costs. Yet the Mounties pursued the contract to police the Town of Esquimalt, promising 35 officers and a stand-alone detachment for the municipality, which has a population of 17,000 in an area of seven square kilometres. Chief Supt. Kevin DeBruyckere, in charge of career development and resourcing for the RCMP in B.C., said he doesn't see systemic vacancies that would prevent the force from entering into a contract with a municipality the size of Esquimalt. B.C.'s director of police services, Clayton Pecknold, was not available for an interview. A spokeswoman for the Public Safety Ministry said the province is aware of staffing shortages in the RCMP and said it is up to local detachment commanders to address the shortfalls with their mayors. Times Colonist, A3

Small-town Mounties pushed to the limit
Their combined ranks are barely enough for a pickup hockey game, yet officers from a pair of small-town RCMP detachments in southern Alberta found themselves involved in two of the largest investigations in recent memory. On most days, the 10 RCMP officers working in Claresholm and Vulcan are enough to handle the routine complaints common in small-town policing. But a mass murder on the highway outside Claresholm and the abduction and killing of a Vulcan-area senior just three weeks apart tested not only the mettle of those RCMP officers, but also the organization's ability to respond. At their height, both cases involved dozens of investigators drawn from RCMP units across the province. But each also began with a lone officer who, despite being more accustomed to handling complaints about traffic and vandalism, had the training to recognize a major event unfolding. While small towns aren't immune to crime, homicides and serious offences are relatively rare. When they happen, detachments rely on specialized RCMP units based in larger centres. Calgary Herald, A3

SYRIAN EMBASSY VANDALIZED IN OTTAWA: PROTESTERS COMMEMORATE 1982 HAMA MASSACRE
The Syrian Embassy in Ottawa was splashed with what appears to be red paint on Saturday. Protesters held a demonstration in front of the embassy - located in midtown Ottawa, about 10 blocks from Parliament Hill - Saturday morning to commemorate the 1982 Hama Massacre, an uprising in which thousands died, and the events that took place Friday in the Syrian city of Homs. A large quantity of red paint covered the embassy door, mailbox, gates and canopy of the embassy's main entrance Saturday afternoon. The gates to the embassy were locked and nobody was available to

speak about the incident. An RCMP officer photographing the vandalism would not comment. Ottawa Citizen, A1; Toronto Star

Five young men missing
The Vancouver police's missing persons unit is calling for tips on five unsolved cases from 2011 - all young men. Foul play is not suspected in any of the cases at this time, Sgt. Kirk Star said Friday. There were 3,700 missing-person reports last year, Star said. The current inquiry into Vancouver's missing women and flawed Vancouver Police Department and RCMP investigations into Robert Pickton is ongoing, and will make recommendations around improving systemic issues in policing. Star said he is reluctant to comment on the inquiry. The Province, A15

Police drug lab photos highlight dangers
Filthy conditions, unknown chemicals and a pill press covered in ecstasy: this is what a drug lab looks like. In their latest effort to showcase the dangers associated with street drugs, police released photographs Friday of an ecstasy lab in Richmond, B.C., in light of the many deaths in Alberta and B.C. tied to ecstasy laced with a toxic chemical. Seven people in Calgary, and one person in Red Deer, have died from taking ecstasy (MDMA) laced with para-methoxymethamphetamine (PMMA). Two additional cases are still awaiting toxicology results. There have been five deaths reported in B.C. The chemical, a cheaper alternative than MDMA, is being cut into ecstasy. B.C. RCMP Sgt. Duncan Pound said when officers entered the lab in full protective suits in 2008, they found 750,000 pills and enough drugs to make 3.3 million tablets. Edmonton Journal, A5

The ecstasy and the agony
Not so long ago, Myles Murphy popped "E" caps like they were candy. These days, however, the gregarious 19-year-old from Abbotsford has a different take on the so-called "love drug" that is so popular among clubbers and partygoers and whose properties, it is commonly said, jack up the senses to the point where you can "see the music" and "hear the colours." The warning is being echoed by police and public health officials in the wake of a spate of ecstasy-related deaths in Western Canada. It is possible, police and health officials say, that a crackdown on precursor chemicals used to make methylenedioxymethamphetamine, or MDMA - which is ecstasy in its traditional or pure form - has led drug producers to turn to other synthetic drugs, such as PMMA. It is also possible that inexperienced producers intended to add meth into the toxic blend but ended up creating PMMA by accident. Ottawa-based RCMP Cpl. Luc Chicoine, a synthetic-drug expert who provides support to the force's drug investigators, said MDMA is made by mixing MDP2P, a light oil extracted from the bark of a tree, with various chemicals common in paint thinners and drain cleaners. The solution is then mixed with hydrochloric acid to turn it into a powder, which can be consumed as a powder or pressed into tablets or wrapped in capsules. The Province, A4; Calgary Sun

Two men charged in $4M fraud
Two Quebec men face fraud charges following an investigation by the RCMP into a mortgage scam that cost victims more than $4 million. Kinh Ho Quan, 56, and Hermel Bosse, 58, were arrested this week on charges alleging they took part in at least 20 fraudulent transactions totalling nearly $4.5 million and bilked individuals, financial institutions and the Canada Mortgage and Housing Corporation, which provides mortgage loan insurance. According to a news release, the RCMP's Major Fraud Unit of Commercial Crime Section of Montreal probed a total of 80 suspicious transactions worth an estimated $18 million since the investigation was launched in April 2008. The RCMP said many have since had to declare bankruptcy and saw their credit history ruined. The RCMP warn that mortgage fraud "is a form of crime increasingly observed by police." Ottawa Citizen, A3

Cops should collect race stats: study
Canadian police departments should collect race-based crime data, two Ontario criminologists say. Akwasi Owusu-Bempah, a doctoral candidate at the University of Toronto's Centre for Criminology, and Paul Millar, a criminal justice professor at Nipissing University, make their controversial argument in a report titled Whitewashing Criminal Justice in Canada: Preventing Research through Data Suppression. The study appears in the current issue of the Canadian Journal of Law and Society. Edmonton Sun, 29

Man charged after four-year-old approached by suspicious Santa
Police in B.C. have arrested a suspect in a case where a man allegedly tried to lure a child by claiming he was Santa. David Warren Buchanan, 67, has been charged with two counts of attempted child abduction and police say he is a suspect in a third case. Buchanan was arrested Friday in Penticton, B.C., after RCMP spotted his vehicle outside a hotel. Chronicle-Herald, A4; Edmonton Sun

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Prison contraband soars
Cocaine, alcohol, explosives, knives and handcuff keys are part of the haul at federal prisons as officials across the country struggle with a rising tide of contraband. Between 2007 and 2011, the amounts of drugs, intoxicants, weapons and other unauthorized items confiscated by prison staff has steadily risen, in some cases by more than 170 per cent, according to documents obtained by the Star. The number of seizures of intoxicants, for example - LSD, THC, amphetamines and steroids, to name just a few - rose to 1,779 in 2010-11, up from 1,295 three years earlier. Similarly, the number of seizures of weapons, including razor blades, homemade knives, firearms, explosives and pipes, rose by 22 per cent to 900 over the same period. Perhaps most striking is the surge in seizures of other unauthorized items, such as cellphones, tattoo-making materials, lock picks and rope, from 991 to 2,697. "I suspect that detection is getting better, so you do see an increase in seizures," said Howard Sapers, Canada's Correctional Investigator. "What we really don't know is whether drug use inside prisons is up or down, whether the presence of weapons is greater or lesser than it used to be." The Star also asked the Correctional Service of Canada for the number of employees disciplined for bringing contraband items into prison, but the agency said it did not have any such records. However, last September, CSC commissioner Don Head told a parliamentary committee that it had dismissed 12 staff members that year for smuggling contraband into prisons. CSC could not provide the Star with budget expenditures for 2010-11 due to "temporary technical issues," but a 2010 overview of the agency pegs total corrections expenditures 2008-09 at $2.28 billion, up nearly 40 per cent since 2004-05. The average cost of keeping an inmate incarcerated rose from $87,919 to $109,699. Toronto Star, A11

34 imams condemn 'honour' killings
More than 30 American imams signed a fatwa Saturday condemning honour killings, after a Canada court convicted Afghan immigrants for murdering four female relatives accused of damaging the family's reputation. ISCC founder Syed Soharwardy, said the group put out the fatwa "because of the Shafia trial, because it has been a large focus [for] the Islamic community and people said a lot of things," adding that imams wanted to clear up "some misunderstandings about Islam" by non-Muslims. The Province, A21; Toronto Star; Chronicle-Herald; Le Soleil; Le Journal de Montréal

Sicko ID site
Plans by a Calgary-based group to out convicted pedophiles are raising questions among lawyers and police who monitor sex offenders. Canada Family Action, a Christian group, plans to launch findapedophile.comnext month, a site aimed at educating the public on how to identify potential victims and share convict information. It said the idea stems from their belief the sex offender registry is inadequate and not available to the public. Calgary lawyer Raj Sharma scoffed at the plans. RCMP said they haven't heard any details on the site, but the concept is raising questions. Sgt. Rich Veldhoen with Calgary police high-risk offender program believes efforts already in place to monitor violent and sex offenders in the community are working. Calgary Sun, 3

The 'just' punishment that dares not speak its name
An opinion piece states, "Senator Pierre-Hugues Boisvenu was wrong to suggest vicious killers be offered a rope. They shouldn't have any choice in the matter. His suggestion, since retracted, was technically flawed because it's illegal to counsel suicide in this country. It's apparently OK to say if people aren't as sharp, limber, sexy and healthy as they used to be, they should be allowed to off themselves. Just not Paul Bernardo, Clifford Olson or Mohammad Shafia. But clearly most of the beautiful people's objections weren't on this narrow ground. Rather, they found the suggestion too, too shocking." Ottawa Sun, 16

INTERNATIONAL / INTERNATIONAL

Russia, China veto UN resolution on Syria
Russia and China vetoed on Saturday a UN resolution that backed an Arab plan calling on Syrian President Bashar al-Assad to quit, stalling global efforts to end his bloody crackdown on unrest after hundreds were reported killed in the city of Homs. The veto left Canada "disappointed in the extreme," Foreign Affairs Minister John Baird said Saturday. Ottawa Citizen, A1

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

Williston, Sandra

From: Luc Beaudoin <[redacted]>
Sent: February-04-12 11:45 AM
To: [redacted]
Cc: Beaudoin, Luc
Subject: FBI and Anonymous

s.16(2)(c)
s.19(1)

For RCMP attention/info.

I shoundn t but I wonder why they are not on this distro.

lessons learned: let s change our govIRT #code once in a while !

http://pastebin.com/[redacted]

[redacted]

Pages 39 to / à 40

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-04-12 10:37 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - Final / Finale

Daily Media Summary / Revue de presse quotidienne
February 4, 2012 / le 4 février 2012

MINISTER / MINISTRE

NDP MP in hot water again for profanity-laced tirade

Winnipeg NDP MP Pat Martin added fuel to the obscenity-laden firestorm he created this week when he cursed at a Conservative senator who suggested murderers should be given ropes to hang themselves. On Wednesday, Martin cursed Sen. Pierre-Hugues Boisvenu sparking controversy. When demands for an apology were made Thursday, Martin refused. He added perhaps his only mistake was that he didn't include the required honorific when addressing a senator. Boisvenu triggered his own controversy with his comments Wednesday when he was asked about the government's omnibus crime bill, which gives stiffer penalties for certain violent crimes. Boisvenu is an outspoken victims' rights advocate. His daughter was raped and murdered by a repeat offender in Quebec in 2002. He was appointed to the senate in 2009. Manitoba Senior Minister and **Public Safety Minister Vic Toews** demanded Martin apologize. "***Pat Martin's constituents, and indeed all Canadians, would be better served if the MP and his soft-on-crime party, would direct their outrage and vitriol at the criminals who victimize innocent, law-abiding Canadians rather than at a senator whose family has suffered a terrible loss at the hands of a repeat offender***," **Toews said** in a letter to the editor. Telegraph-Journal, A9

Trotting out the bogeyman

An opinion piece states, ""***I don't know if the statistics demonstrate that crime is down ... I'm focused on danger.***" That's **federal Public Safety Minister Vic Toews**, speaking to the Senate Committee on Legal and Constitutional Affairs about the Conservatives' "tough on crime" legislation. If nothing else, the next few years are going to have more than their fair share of unintentional hilarity - because unless I completely misunderstood that particular quote, **Toews** has just confirmed what opponents of the new crime legislation have been saying all along. And that's that the legislation has nothing to do with crime, and everything to do with marketing... Rewind a little further, back to when **Vic Toews** actually did realize that statistics demonstrated that crime rates were down to levels last seen in the early '70s. (He must have since forgotten about those statistics, because he clearly doesn't know about them anymore.) He said that the Tory crime bill was to help address the increase in unreported crimes. "***We see this continuing trend of more and more crimes going unreported, and that ... I believe is an indication of a lack of confidence in the justice system***," **Toews** told CTV in September 2010. "***And that is why our government is taking the measures that we are taking.***" All right. To get this straight, then: it's the increase in unreported crime (that's a great thing to try and measure in any form - it's big, it's bad, it's ... unreported, hence statistically, well, void) and the increase in ... wait for it ... danger..." The Telegram, A20

Hat's not impressed with Tory justice

A satirical opinion piece states, "Mousie MacKay got a beer from the bar at Louie The Leggers and carried it over to the table where Hat McInnes was sitting, sipping on a beverage, and playing with a small computer... "No, the story I was referring to was the one where, once again the **minister of public safety**, boy, that's an Orwellian mouthful, **minister of public safety**. Anyway, yet another judge has criticized the minister for not allowing a Canadian in prison in the States to serve their time in a Canadian prison." "Seven years for a marijuana bust, that's pretty heavy," said Mousie, "But the Americans are paranoid about drugs. Can you imagine how tense things will get if the Liberals try to legalize marijuana? How come the government slammed the door on this guy, a bit of weed doesn't seem like a capital crime?" "That's one of the problems the judge had, **the minister** didn't really provide any reasons for his denial," said Hat, "so the judge has ordered **the minister** to review the case and provide some good reasons for denying the man a chance to serve his sentence in Canada." "So who stopped the marijuana guy from coming back to a Canadian prison?" asked Mousie. "That was **Vic Toews**, another guy who's made up his mind and doesn't want to be confused by the facts..." The Guardian, A15

One to watch...

A letter states, "Bill C-10: The crime bill. It's not so much the crime bill itself that needs watching; a minority of Canadian voters graciously granted Prime Minister Stephen Harper a majority government, so the bill will pass. What will be interesting to watch is how the bill will play out after it is passed. Even some Tory senators wonder why the Harper government is so fixated on crime, in light of statistics that show crime has actually been decreasing for quite some time. **Public Safety Minister Vic Toews** told a Senate committee reviewing the legislation: "***I don't know if the statistics demonstrate that crime is down. I'm focused on danger.***" **The minister** then went on to say his concern is that the public is in danger as long as criminals walk the streets, "***and this legislation addresses that.***" Given the statistical decline of murderers, rapists, violent robbers and other shady types, the question has to be asked: Who is **Toews** afraid of when he walks the streets of Canada? Panhandlers? Homeless people?" Winnipeg Free Press, J12

Have your say
A letter states, "OK, Pat Martin lips off again, and again **Vic Toews** runs to the media. He reminds me of a schoolyard child running to his teacher to tattle on another for saying a bad word. And for what? To say sorry? Really! Canadian politics has come down to this? Now that's obscene." Winnipeg Free Press, A17

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Despite weather, flood forecast in works
Manitoba Water Stewardship is working on a spring flood forecast despite this winter's mild and relatively dry weather. Provincial flood forecasters plan to unveil a preliminary flood outlook before the end of February, spokesman Paul White said Friday. Although much of southern Manitoba has experienced dry conditions since June, ground moisture levels -- one of the factors that increases the probability of localized or regional flooding -- remain significant in some areas of the province. While moisture levels are well below those recorded last winter, when the province began preparing for major spring flooding, conditions are comparable to the early months of 1997, the year of the Flood of the Century in the Red River Valley, White said. But across most of southern Manitoba, the snowpack -- another major factor in determining flooding -- is much lower this year. That can change significantly before the spring snowmelt, as one or two blizzards can be the difference between a major flood and no flooding whatsoever. Winnipeg Free Press, A13

B.C. avalanche kills man
One man is dead after a small group of recreational skiers got caught in an avalanche Friday morning on Meadow Mountain, near Kaslo, B.C. The man's name isn't being released until Mounties notify his family. The B.C. Coroner's Service and RCMP are still investigating the death. Windsor Star, A13; Edmonton Journal; * Vancouver Sun

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Conditions eased for suspect
Mohammad Mahjoub, a Toronto man detained and subsequently held under house arrest for the past 12 years on a national security certificate because of alleged terrorist ties, was granted more freedoms by a federal court Friday. Mahjoub, 51, was arrested in Toronto in 2000 on a security certificate, which allows the government to detain terror suspects indefinitely without charges or a trial. In his decision, Judge Edmond P. Blanchard said the federal government failed to provide "reasonable grounds to believe" that Mahjoub's security threat has not reduced. While Blanchard said there remains "compelling and credible evidence" that Mahjoub "poses a threat to the security of Canada," evidence during the latest review of Mahjoub's case and his current circumstances suggest that this threat "is now significantly diminished." Windsor Star, A13; National Post; The Telegram

Defenceless
Just what legally constitutes a foreign activity in Canada that is detrimental to this country's national security interests these days, anyway? As it turns out, Canada is practically incapable of answering that question with any enforceable coherence. When it comes to the recent and rapid-succession manoeuvres that have given Chinese state-owned entities the spigot key at critical flow points in Canada's oil and gas industry, mysteries abound. But it is now clear that slowly but surely, Canada's regulatory defences have been almost completely hollowed out. Way back in the 1980s, the Security Intelligence Review Committee was urging amendments to the Canadian Security Intelligence Service Act to spell out what Canadians mean when we talk about foreign-power connivings that are "detrimental" to Canada's national interests. "It is almost wholly subjective: no criteria are provided to offer any standard for determining what is 'detrimental'," a SIRC report once pointed out. The definitions in the CSIS Act still don't clearly define what "detrimental" means, but unlike Investment Canada, CSIS has muddled through and is properly content to couple Canada's "national security" with "the security and economic welfare of Canada." Ottawa Citizen, B7

Muslim group slams 'terrorist' treatment

A Canadian Muslim businessman became a terror suspect for telling sales staff in a text message to "blow away" the competition at a New York City trade show, an association said Friday. Moroccan-born Saad Allami was arrested three days after he sent the message in January 2011 and detained while police searched his home, said the Muslim Council of Montreal. Ottawa Citizen, A4; Le Soleil

MacKay quiet on iran plans
Regional troublemaker Iran poses "a grave threat to peace and security" and is "fanatical and dangerous," Prime Minister Stephen Harper said Friday. Harper made the comments during an interview with Postmedia, and warned that Iran would be ready to use a nuclear weapon if it was able to produce one. But in an interview with QMI Agency, Defence Minister Peter MacKay wouldn't speculate whether Canada -- a staunch ally of Israel -- would join that country in a possible strike against the Islamic regime. Toronto Sun, 24

CYBER SECURITY / CYBERSÉCURITÉ

Confidential police call hacked, leaked
Trading jokes and swapping leads, investigators from the FBI and Scotland Yard spent the conference call strategizing about how to bring down the hacking collective known as Anonymous, responsible for a string of embarrassing attacks across the Internet. Unfortunately for the cyber sleuths, the hackers were in on the call too - and now so is the rest of the world. Anonymous published the roughly 15-minute-long recording of the call on the Internet on Friday, gloating in a *Twitter message that "the FBI might be curious how we're able to continuously read their internal comms for some time* now." The humiliating coup exposed a vulnerability that might have had more serious consequences had someone else been listening in on the line. The leak was one of a slew of Anonymous hacks that hit websites across the United States Friday, including in Boston, where the police site was defaced, and in Salt Lake City, where officials said that personal information of confidential informants and tipsters had been compromised. Anonymous also claimed credit for defacing the Greek Justice Ministry's website and stealing a mountain of data from the Virginia-based law firm that defended a U.S. Marine recently convicted for his role in the bloody 2005 raid in Iraq that became known as the Haditha massacre. Red Deer Advocate, A5; * Ottawa Citizen

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

$1M worth of drugs, 13 charged in 'high-level' raid
Thirteen people alleged by police to be "high-level" drug dealers were charged Friday in connection with the latest large-scale sweep orchestrated by Manitoba's organized crime unit. Project Deplete, a police investigation that began last August and culminated Friday with arrests in Winnipeg and Edmonton, is the latest effort of Manitoba's Integrated Organized Crime Task Force, a joint RCMP-Winnipeg police unit that has famously used informants over the past several years to take down primarily the Hells Angels and their associates, with great success. The latest sweep saw charges laid against people police accuse of being major players in the city's drug trade. Some of the accused have gang associations, others are more "independent," police said. Winnipeg Sun, 2; * Winnipeg Free Press

*** Mountie pleads not guilty to assault**
A Rimbey RCMP officer who was suspended over criminal assault charges pleaded not guilty in Rimbey provincial court on Friday. A trial date of Oct. 2 was set for Const. Jesse Charles Lambright, 52, who was charged with assault and uttering threats in connection to an off-duty relationship. The officer was suspended from duty after the charges were laid. An RCMP code of conduct investigation was also suspended, pending the outcome of Lambright's criminal charges. Red Deer Advocate, A9

*** Toy gun prompts dramatic RCMP takedown at Subway**
A toy gun police say was altered to look like the real thing led to a standoff outside a Kelowna Subway restaurant Thursday. At about 1: 40 p.m., an RCMP officer conducting another surveillance operation at the Capri Centre Mall reported seeing a young man putting a gun into his sweatpants as he walked across the parking lot. RCMP followed the suspect, who was with a group of 12 young men and two women, as they made their way to a Subway food outlet. Staff were removed from the restaurant as police surrounded the site, and a RCMP helicopter circled overhead. Vancouver Sun, A12

DNR finds barrels of pot
Approximately 29 kilograms of marijuana has been seized following the discovery of the drug by New Brunswick *Department of Natural Resources Conservation Officers. Last week, conservation officers were working on an illegal* possession of moose meat investigation when they discovered the drug in a number of barrels in a wooded area near a

residence in Scoudouc. They then called the District 4 RCMP who began an investigation. Times & Transcript, A6; * L'Acadie Nouvelle

*** RCMP seize drugs at Truro bus terminal**
RCMP seized cocaine and prescription drugs during a bust Thursday at the Acadian Lines bus terminal in Truro. Mounties arrested a 43-year-old man from Cambridge, Ont., during the bust, which netted 825 grams of cocaine and about 400 oxycodone prescription pills. Sylvain Joseph Matte faces charges of possession of cocaine for the purpose of trafficking and possession of oxycodone for the purpose of trafficking. Chronicle-Herald, A5

Police make arrest and seize cocaine, marijuana
A 33-year-old Saint John man has been arrested after police seized a large amount of cocaine and marijuana from the city's east side. Russell William McCain of Canterbury Street faces a number of drug-related charges, police said in a release. McCain's arrest came after a three-month investigation by members of the Saint John Police Force street crime unit and the Fundy Integrated Intelligence Unit. The RCMP and the Rothesay Regional Police Force participated in the drug raid on Thursday. Telegraph-Journal, B3

*** Alleged pimp faces human trafficking rap**
A 42-year-old Hamilton man is facing a litany of charges, including human trafficking, for allegedly coercing women into prostitution. Police claim the man is a pimp who used threats of violence, intimidation and extortion as a means of control. Victor Bettencourt, 42, is charged with human trafficking, procuring a person to engage in prostitution, procuring for living off the avails of prostitution, extortion, two counts of trafficking in cocaine, possession of cocaine for the purpose of trafficking, possession of the proceeds of crime under $5,000 and failing to comply with recognizance by breaching bail terms. Hamilton Spectator, A6

Mountie rescues child from car
Surrey, B.C. Mom Alyse McDonald will be forever grateful to RCMP Const. Aaron Jabs. The off-duty police officer went out his way Wednesday morning to pull McDonald's two-year-old daughter Haylee from the wreckage of the family car, which was upside down in a watery ditch in Delta. Telegraph-Journal, A4

*** Des accusations criminelles contre des adeptes du flip immobilier**
La GRC a arrêté mardi Kinh Ho Quan, 56 ans, et Hermel Bossé, 58 ans, deux individus impliqués dans plusieurs cas de fraudes hypothécaires, principalement dans la région de Montréal. Ils ont été libérés rapidement. On n'a pas pu connaître les conditions de leur libération. Ils comparaîtront en cour le 30 mars. Ils sont accusés de fraude de plus de 5000$. S'ils sont reconnus coupables, ils risquent une peine de prison maximale de 14 ans. Une enquête approfondie menée par l'Unité des fraudes majeures de la Section des délits commerciaux de Montréal de la GRC a porté plus spécifiquement sur 20 transactions suspectes qui se sont toutes avérées frauduleuses pour un total s'élevant à près de 4,5 millions de dollars. La Presse, S4; Le Journal de Montréal

Arrest in $200k scam on senior
A man accused of scamming a 90-year-old B.C. homeowner out of more than $200,000 was busted in northern Manitoba last week and sent back to Vancouver Island. Richard Patterson, 47, was arrested Jan. 25 in Norway House on the strength of a Canada- wide warrant for fraud over $5,000, according to Manitoba RCMP. He was charged by Victoria police last summer for allegedly bilking a 90-year-old resident of the B.C. capital out of more than $200,000 for renovations he was supposed to be doing on the man's house. Winnipeg Sun, 13

Porn sting may yield more arrests
The different investigations, some of which lasted eight months, came to a head Jan. 31 and Feb. 1. Police executed 76 search warrants and laid 213 charges against 60 people, including three young offenders. The people nabbed in Windsor face a range of charges including accessing child pornography, possession of child pornography, distribution of child pornography and luring a child for sexual purposes. Staff Sgt. William Donnelly with Windsor police said additional arrests are possible, but that could take awhile as police sift through child porn photos that are "traded around like hockey cards." Windsor Star, A5

Alleged cyber sicko
She thought she knew him and she wasn't alone. Toronto Police claim many teen girls across the country met Alex Sirop online and believed he was a good-looking 19-year-old. They had no idea when they sent "compromising" images of themselves over the web that a 42-year-old Scarborough man named Shiraz Nariman was allegedly adding them to his collection of child porn. Nariman is one of 54 people rounded up recently by police in Ontario during a massive child pornography sweep. The RCMP first learned of him when a teenage girl, who can't be named, came forward in September 2010. Toronto Sun, 7; Toronto Star

Man charged with making child porn
A man has been charged with producing child pornography following a year-long investigation by the Edmundston City Police Force and the New Brunswick RCMP's Internet Child Exploitation Unit. Shane Evan McCabe, 34, of no fixed address, was arrested on Thursday upon his release from jail where he was serving time for failing to register with the National Sex Offender Registry for past convictions. The investigation began in March 2011 when images of child sexual abuse were found scattered around the City of Edmundston. The Fredericton Police Force, the RCMP's Technological Crime Unit, the National Child Exploitation Coordination Centre, the Canadian Centre for Child Protection (cybertip.ca), the RCMP's Violent Crime Linkage Analysis System and the National Sex Offender Registry also assisted with the investigation. Times & Transcript, A9

Two grow-ops found same day
London police busted two marijuana grow-ops in less than three hours, seizing nearly $600,000 in drugs. Both grow operations, located less than eight kilometres apart, were in middle-class north London neighbourhoods. London Free Press, A8

Police reveal drug lab photos to highlight ecstasy dangers
Filthy conditions, unknown chemicals and a pill press covered in ecstasy: this is what a drug lab looks like. In their latest effort to showcase the dangers associated with street drugs, police released photographs on Friday of an ecstasy lab in Richmond, B.C., in light of the many deaths in Calgary and B.C. tied to ecstasy laced with a toxic chemical. Seven people in Calgary, and one person in Red Deer, have died from taking ecstasy (MDMA) laced with para-methoxymethamphetamine (PMMA). Two additional cases are still awaiting toxicology results. There have been five deaths reported in B.C. The chemical, a cheaper alternative than MDMA, is being cut into ecstasy, but is believed to be more toxic. B.C. RCMP Sgt. Duncan Pound said when officers entered the lab in full protective suits in 2008, they found 750,000 pills and enough drugs to make 3.3 million tablets. Calgary Herald, B1

Date-rape drugs among $17K bust
Mounties in Red Deer say they've made a major seizure of so-called date rape drugs that were meant to be trafficked. On Thursday, Mounties executed a warrant on a Red Deer residence, where a search turned up two kinds of drugs known to be used to incapacitate unwitting victims who are then sexually assaulted. In the search of the house and garage, they found three litres of gamma hydroxybutyric acid (GHB), as well as 10.8g of ketamine, which can be slipped into drinks. Calgary Sun, 20

*** 135 000 cigarettes dans le coffre**
Une Néo-Écossaise a été arrêtée alors qu'elle était en possession de quelque 135 000 cigarettes de contrebande du Québec qui étaient destinées au marché de la région de Halifax. La suspecte, une femme de 35 ans de Timberlea, en Nouvelle-Écosse, a été interpellée par les autorités plus tôt cette semaine lors d'une perquisition effectuée par la GRC et les autorités provinciales dans une Chevrolet Impala 2011. Le Journal de Montréal, 22

*** Notorious B.C. brother guilty of drug conspiracy**
One of three brothers among a notorious family with reputed links to Vancouver's gang world "fabricated" a story that he was simply planning to steal drugs, instead of scheming to traffic them with his ex-girlfriend's father, a B.C. Supreme Court judge said Friday. Jarrod Bacon, 28, and Wayne Scott, 55, were each found guilty of one count to conspire to traffic cocaine by Associate Chief Justice Austin Cullen following a four month trial that ended mid-January. Red Deer Advocate, A3; * Calgary Herald; * Vancouver Sun

Remains found on reserve
Human remains have been found in a vacant home on the Nak'azdli reserve in B.C., RCMP said Friday. The remains were reported to police Wednesday afternoon. The reserve is located about 150 km northwest of Prince George. It is considered a suspicious death at this point, Corp. Annie Linteau said. Edmonton Sun, 23

Civilian oversight of police a must
An opinion piece states, "The continuing fall-out over the violent arrest of Adam Nobody during the G20 raises serious doubts about the adequacy of civilian oversight of the police. Eighteen months later, one officer, Const. Babak Andalib-Goortani, has been charged criminally with assault by the province's Special Investigations Unit. Another provincial body, the Office of the Independent Police Review Director, has recommended Andalib-Goortani and four others -- Constables Michael Adams, David Donaldson, Geoffrey Fardell and Oliver Simpson -- face disciplinary charges. But the SIU says since the standard of evidence for identifying officers is higher for a criminal case than disciplinary hearings, no new criminal charges will be laid... But the larger issue is the lack of co-operation the SIU has received from police, not just in G20 cases in Toronto, but across the province." Ottawa Sun, 12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** Hamilton mother facing deportation loses reprieve**
The final government word for Lucene Charles, the Hamilton mother of three Canadian boys fighting deportation to St. Vincent, is that she must go, expeditiously. Charles, who has been on an emotional roller-coaster ride since losing her final appeal last summer, was told Friday a review of her case supports the original deportation order. She was ordered to return to the Canada Border Services Agency (CBSA) offices on Tuesday to show that she has purchased one-way, non-refundable tickets to St. Vincent for herself and her five-year-old African-born daughter leaving Canada by Feb. 17. Charles, 36, was ordered in January to leave by Feb. 2, but received a reprieve a few days later. She was recently summoned to meet with CBSA agents again on Friday. CBSA officials said Charles is being deported because she entered and remained in Canada without authorization. Hamilton Spectator, A4

*** Un traitement royal pour Mugesera**
Le Rwandais Léon Mugesera a eu droit à un traitement royal lors de sa déportation du Canada vers son pays natal : avion privé, personnel médical et agents de sécurité, a appris l'Agence QMI. L'ancien homme politique a été expulsé du pays la semaine dernière, pour retourner au Rwanda, où il devra faire face à des accusations relativement au génocide survenu en 1994. L'Agence des services frontaliers du Canada (ASFC) a confirmé que le renvoi de M. Mugesera avait nécessité " un vol nolisé avec plusieurs escortes (agents de sécurité) et un infirmier ", pendant un voyage d'une durée de 30 heures. L'ASFC a refusé de dévoiler les coûts de l'extradition, mais selon des informations affichées sur le site Web de Citoyenneté et Immigration, les dépenses relatives aux renvois " peuvent s'élever jusqu'à 300 000 $ lorsqu'il s'agit d'affréter un avion dans certains cas ". Le ministère précise que des coûts d'environ 200 $ par jour s'ajoutent à cela, lorsque la mise en détention s'avère nécessaire. L'ASFC précise qu'un renvoi ne requérant pas d'escorte coûte en moyenne 1 500 $. Cependant, lorsque des agents de l'Agence doivent escorter un individu à bord d'un vol commercial " pour des raisons de sécurité ", le renvoi coûte en moyenne 15 000 $. Le Journal de Montréal, 19

Deportation for dirtbag
Clato Mabior's time on Canadian soil appears to be quickly winding down. Mabior, convicted of aggravated sexual assault for failing to disclose his HIV status to sexual partners, will be deported to Sudan in the next 30 days -- likely on Feb. 15, according to his immigration lawyer. Mabior, 34, was ordered held in custody at a review of his ongoing detention Friday. He's been behind bars on the strength of a deportation order since October 2010. The Immigration and Refugee Board has repeatedly ruled that Mabior is a flight risk and a danger to the public. Winnipeg Sun, 3

*** Une sexagénaire d'origine française menacée d'expulsion pour un vol de 80 $**
Jeannine Poloni, une femme de 67 ans d'origine française est menacée d'expulsion pour avoir volé pour 80 $ de nourriture dans une épicerie et parce qu'on la considère maintenant comme une "grande criminelle ". M me Poloni est arrivée au Canada en 1964. Elle a son statut de résidente permanente, mais n'a jamais fait de demande de citoyenneté canadienne. Elle a travaillé toute sa vie et a fondé une fa-mille au Québec. C'est en 2009 qu'elle a été arrêtée pour avoir volé pour 80 $ de nourriture dans une épicerie et condamnée à une peine de neuf mois de prison avec sursis. Lorsqu'une personne qui n'est pas citoyenne canadienne est condamnée à une peine criminelle de plus de six mois, les autorités peuvent demander son expulsion pour cause de " grande criminalité ". C'est ce qui arrive à M me Poloni. Le Journal de Montréal, 22

The hangover
On May 13, 2011, a prominent Canadian DJ crossed the Alberta-B.C. border near Lake Louise with a case of red wine, daring authorities to arrest him. The Mounties refrained but Terry David Mulligan had made a point of mocking a lingering hangover of Alberta alcohol prohibition 87 years after its repeal. Yet, it's still illegal to cross provincial borders with booze. While flamboyant bootleggers such as Al Capone, furtive speakeasies and rumrunners are colourful legends of the 1920-1933 U.S. prohibition, Canada's own doomed attempt at shutting off the taps has barely had a last recall. Calgary Sun, 18

Mugesera finally finds Rwandan lawyer
Rwandan lawyers haven't been lining up to defend Léon Mugesera - wanted for almost two decades for his role in the 1994 Rwandan genocide - but one has stepped forward, despite possible security issues and little pay. Guy Bertrand, the Quebec City lawyer who helped the suspected war criminal dodge deportation from Canada for years, said it was difficult to find someone willing to take on his client. He fears for the Rwandan attorney's safety but can't afford to hire a bodyguard. For security reasons, Bertrand didn't want to reveal the lawyer's name or put The Gazette in touch with him, but Rwandan news organizations reported he is Donat Mukunzi. Montreal Gazette, A8

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VICTIMS TREATED CRIMINALLY

It's about time someone started talking about the rights of victims in the criminal justice system. Canada's ombudsman for victims' rights Sue O'Sullivan released a special report this past week on the need for governments, the courts and corrections to start taking the rights of victims of crime far more seriously than they have in the past. And her report is bang-on. I recommend every elected official in Canada read it. I've met enough victims of crime over the years to know exactly what O'Sullivan is talking about. We spend a lot of time in the justice system dealing with the criminals themselves -- their sentences, their rights, etc. -- but not enough time ensuring victims have the legislated rights they deserve. Winnipeg Sun, 5

*** Haitian-born killer got aboriginal-style hearing**

Federal documents have offered a glimpse into a controversial hearing last month in which a Haitian-born convicted killer was able to access an aboriginal-style parole hearing at Manitoba's Stony Mountain Institution, a medium-security facility. Gregory Bromby, 35, was convicted of first-degree murder in 1997 for the stabbing death of 15-year-old Tara Manning in Quebec in 1994. He claims working with aboriginal elders on a special unit at the prison taught him to respect women. The parole hearing was attended by Michael Manning, the Mont-real-based father of the young murder victim. Bromby's attempt at day parole ultimately was denied. Documents released by the Parole Board of Canada say Bromby participated in aboriginal spirituality and ceremonies, while living on a special unit designed to honour the spiritual and cultural ways of aboriginal people. Edmonton Journal, A8

Group aims to 'out' pedophiles

A Christian-oriented activist group said Friday it plans to launch a website for identifying pedophiles. Canada Family Action said its website will be called FindA-Pedophile.com. Brian Rushfeldt, president of the organization, said he hopes to have the site operational by March. The Calgary-based group said the recent bust of 60 people in Ontario on hundreds of child pornography charges is proof that such a resource is needed. Rushfeldt said the information will be gathered from sources such as the courts, police and media reports. Montreal Gazette, A15; Ottawa Sun

Quebec man wants senator prosecuted for suicide comments

A Quebec man has filed a police complaint against Conservative Senator Pierre-Hugues Boisvenu for remarks he believes could lead someone to commit suicide. The complaint came after Boisvenu said Wednesday in Ottawa that some convicted killers - he referred specifically to Paul Bernardo, Clifford Olson and Robert Pickton - should be given a rope in their prison cells in case they want to hang themselves. The senator later apologized for his comments, but 26-year-old Jacques McBrearty said Boisvenu went too far. The Sûreté du Québec will investigate the complaint, which could eventually be handed over to the RCMP since the events occurred in Ontario, where Boisvenu lives. Montreal Gazette, A10; * Waterloo Region Record

*** Le sénateur Boisvenu est une victime d'abord**

Tous les collègues conservateurs du sénateur Pierre-Hugues Boisvenu viennent maintenant à sa défense. Ils disent qu'on n'a pas le droit d'attaquer ses propos parce qu'il est une victime et qu'il a donc parlé avec ses émotions. Lorsque le sénateur conservateur, mercredi, a émis son opinion sur la peine de mort, lâchant sa phrase devenue rapidement célèbre, " il faudrait que chaque assassin (ait) le droit à sa corde dans sa cellule ", le premier ministre Stephen Harper a cherché à étouffer l'affaire le jour même en soulignant que le sénateur avait retiré ses propos. Mais comme M. Boisvenu continue de partager publiquement son opinion sur la peine de mort, la nuançant plus ou moins, se vantant même d'avoir reçu des centaines d'appuis pour son commentaire, la défense du gouvernement a changé. A l'intérieur comme à l'extérieur des Communes, les élus conservateurs disent dorénavant que personne n'a le droit d'attaquer M. Boisvenu à cause de sa douloureuse histoire familiale, faisant référence à l'assassinat de sa fille. La Tribune, 14

*** Pas une première pour le sénateur Boisvenu**

Même si les propos du sénateur Pierre-Hugues Boisvenu ont suscité la controverse d'un bout à l'autre du pays, cette semaine, ce n'est pas la première fois qu'il tient un tel discours. Dans une entrevue accordée au Journal de Québec en juillet 2010, le sénateur conservateur s'interrogeait sur les coûts que l'État doit payer pour garder incarcérés les criminels dangereux dont la " réhabilitation est impossible ". " Est-ce que, dans ces cas-là, on devrait laisser le libre choix au criminel ? Est-ce que, dans ces cas-là, on pourrait dire : " Regardez, on tire la plogue " ? ", soulevait alors M. Boisvenu. Le sénateur admettait aussi être favorable " dans certains cas " à la peine de mort, par exemple ceux des meurtriers en série Clifford Olsen et Robert Pickton. Le Journal de Montréal, 19

*** Sex attacker high risk to re-offend**

A "high-risk" repeat sex offender who admitted in court Friday to brutally raping an Edmonton woman in the river valley is to face a dangerous offender hearing. Anthony Winston Clark, 34, pleaded guilty in Court of Queen's Bench to kid-

napping, sexual assault causing bodily harm, attempted choking and uttering death threats. If Clark is designated a dangerous offender, he will be handed an indefinite prison sentence. Edmonton Sun, 4

Kamloops jail too easy to break in to
A review conducted before two recent break-ins at the Kamloops Regional Correctional Centre, apparently to smuggle contraband - possibly drugs - to prisoners, revealed the Interior British Columbia jail must beef up its security practices. Dean Purdy, spokesman for the B.C. Government Employees' Union, said in each case someone scaled the jail's two-metre high perimeter fence and cut a hole in a cell window in the segregation unit. Early reports suggested a laser was used to drill into one of the pieces of Lexan glass. The Daily News has learned a blowtorch was used. Purdy believes the breaches were made to smuggle contraband - possibly drugs - into the prison. The incident raises alarm bells for the union, which is conducting its own investigation along with the province's corrections branch and RCMP. Edmonton Journal, A19

No honour in killing
Imams across North America are condemning the act of "honour killing" on the heels of the guilty verdict and life sentences handed to the Shafia family last Sunday. Mohammad Shafia, 59, his second wife Tooba Mohammad Yahya, 42, and the couple's son, Hamed, 21, were each convicted on four counts of first-degree murder for killing Shafia daughters Zainab, 19, Sahar, 17, Geeti, 13, and Mohammad's first wife, Rona Amir Mohammad, 52. "There is no such thing in Islam that if somebody is bringing disgrace to your family's honour that you go out and kill that per-son," said Imam Syed Soharwardy, founder of the Islamic Supreme Council of Canada. Soharwardy will be issuing a Fatwa on Saturday, a type of religious edict, with more than 34 signatures from imams across North America supporting its position against honour killings, domestic violence and misogyny. Toronto Sun, 9; * National Post

*** This regressive bill will undermine previous work**
Re: the Canadian Bar Association's (CBA's) position on the omnibus crime bill.
A letter states, "We write further to the story written by Nadine Sander-Green on Jan. 27 stating that our justice minister, Mike Nixon, reconfirmed his support for Bill C-10. With respect, the CBA and particularly the Criminal Law Section of the Yukon branch of the CBA strongly disagree with the omnibus federal crime bill... Many years of research have shown what actually reduces crime: a) addressing child poverty; b) providing services for people with mental illness or FASD; c) diverting young offenders from the adult justice system; and d) rehabilitating prisoners and helping them to reintegrate into society. Bill C-10 will actually eliminate conditional sentences for minor and property offenders and instead send those offenders to jail. Mandatory minimums replacing conditional sentences will victimize the most vulnerable by shipping people from remote, rural and northern communities far from their families to serve time. In Yukon, aboriginal people are already over-represented in the justice system." Whitehorse Daily Star, 12

*** Mon agresseur aussi a des droits**
Lettre ouverte au sénateur Pierre-Hugues Boisvenu
Une lettre écrit par Steve Foster, président-directeur général du CQGL dit, « Vos dernières déclarations, selon lesquelles chaque assassin devrait avoir sa corde dans sa cellule pour se pendre et que nous devrions réévaluer la peine de mort pour les cas irrécupérables, m'ont grandement attristé. J'aimerais partager avec vous et le public ce texte pour offrir matière à réflexion... » Le Soleil, 34

*** Senator's remarks ill-advised - but consider his pain**
An opinion piece states, "The Conservative senator who suggested that murderers in Canadian prisons be given rope with which to hang themselves is an emblem of the degradation of our political discourse... Sen. Pierre-Hugues Boisvenu, a victim's rights campaigner appointed to the Senate by Stephen Harper in 2009, ignored the fact that 28 prisoners in federal custody have killed themselves since 2008 and that hanging is the means of choice for 90 per cent of such suicides. So Boisvenu's offer of prison-issue paraphernalia was unnecessary. Human beings, even depraved ones, who make this decision will find a way. Boisvenu has since offered a conditional apology to families of suicides. He has not further amplified his suggestion that immigrants be "filtered" for anti-Canadian attitudes like the ones of the murderous Shafia trio. Who would admit to being willing to slaughter a disobedient daughter? And this is how half-baked plans to improve the world appear. They are blurted out... Boisvenu, who has helped build a women's shelter and a youth camp, is a hero, if flawed." Toronto Star, A12

*** À la défense du sénateur**
Un article d'opinion dit, « Au risque de me faire traiter de suppôt de l'extrême droite, je me porte à la défense de Pierre-Hugues Boisvenu. Après tout, si des meurtriers ont le droit à une défense pleine et entière, je ne vois pas pourquoi on refuserait le même privilège à un sénateur qui n'a rien fait de mal, sauf exprimer un point de vue impopulaire auprès d'une certaine élite bien pensante. À moins que vous me disiez qu'aller à l'encontre de la rectitude politique ambiante est plus répréhensible qu'asséner 40 coups de couteau à ses propres enfants. » Le Journal de Montréal, 6

Des propos condamnables
Un article d'opinion dit, « Une fois de plus, une personnalité publique, en l'occurrence un sénateur bien connu au Québec, s'enflamme et tient des propos qui ne devraient jamais sortir de la bouche d'une personne qui exerce une aussi grande influence sur l'opinion publique. Bien que l'incommensurable souffrance associée à la perte d'un enfant puisse nous amener à comprendre ses motivations profondes, il n'en demeure pas moins que ce genre de propos qui viennent plus du coeur que de la tête sont condamnables lorsqu'on occupe une position politique importante. Cette idée de laisser une corde dans la cellule des criminels ayant commis un homicide est barbare et rétrograde et n'a pas sa place dans une société moderne comme la nôtre. » Le Nouvelliste, 21

*** Un sénateur à "tasser"**
Un article d'opinion dit, « Le premier ministre Stephen Harper passe trop facilement l'éponge dans le cas du sénateur Pierre-Hugues Boisvenu qui a dit que chaque assassin devrait avoir une corde dans sa cellule et décider lui-même de la suite de sa vie. Ce sénateur qui a aussi affirmé que l'emprisonnement à vie des Shafia coûtera à l'État canadien quelque 10 millions$ que celui-ci n'aura donc pas pour investir ailleurs parce qu'il les consacrera à l'entretien de criminels où il n'y a aucune possibilité de réhabilitation. Certes, le sénateur s'est-il excusé, comme le relève le premier ministre en réplique à ceux qui critiquent vertement le sénateur et en réclament la démission ou la destitution comme porte-parole officiel du gouvernement en matière de justice et criminalité. Or, M. Harper ne semble pas avoir l'intention de "tasser" le sénateur, ne serait-ce qu'en le mutant à un autre dossier, et M. Boisvenu n'a lui-même pas l'intention de démissionner, que ce soit comme porte-parole officiel ou sénateur. » La Voix de l'Est, 14

*** Propos du sénateur Boisvenu - Pas de voie unique pour soutenir les victimes**
Un article d'opinion dit, « Les personnes qui ont été victimes de violence sont dans une position «privilégiée» pour comprendre les manifestations et les conséquences de cette violence. Comme société, nous devrions les encourager à prendre la parole et nous devrions considérer leur point de vue dans l'élaboration de politiques et de programmes sociaux. Au cours des dernières décennies, plusieurs mesures ont été mises en place en réponse aux revendications de groupes représentant des victimes de violence; certaines de ces mesures s'inscrivaient dans une logique de contrôle social, tandis que d'autres visaient davantage le soutien aux individus et aux communautés. Lorsqu'il est question de violence, je crois que nous devons faire appel à une combinaison de mesures de contrôle et de mesure d'aide. » Le Devoir, B5

PUBLIC SERVICE / FONCTION PUBLIQUE

Whistleblowers in public service face reprisal: integrity group
Public servants who disclose wrongdoing invariably face workplace reprisals despite laws promising protection, says the head of an organization that promotes integrity and accountability within government. David Hutton, executive director of FAIR (Federal Accountability Initiative for Reform), said he's received hundreds of calls from whistleblowers since assuming his volunteer position in 2008. In some jurisdictions, those who punish whistleblowers can lose their jobs, go to jail and be sued. Australia and Britain are "decades ahead of us" in comparison to the "absolutely dreadful" whistleblower law in Canada, Hutton said. He was responding to a report, prepared for the Office of the Public Sector Integrity Commissioner, which says government employees fear career-limiting reprisals if they blow the whistle on wrongdoers in the federal public service. The report summarizes the findings of 10 focus groups held last November to explore public servants' perceptions about disclosing wrongdoing in their workplaces. It paints a picture of a public service that recognizes its responsibility to disclose wrongdoings, at least in principle, but is fearful of the consequences. Ottawa Citizen, A3; Le Droit

INTERNATIONAL / INTERNATIONAL

Inquiry urged over bribery case
Indian opposition leaders are calling for a government inquiry into allegedly corrupt dealings at the country's Ministry of Civil Aviation, following a Globe and Mail report on bribery and bid-rigging allegations that implicate, among others, cabinet minister Praful Patel. The Globe has detailed the allegations against Nazir Karigar, a 64-year-old Indian-born Canadian citizen and the first individual to be charged under Canada's foreign bribery law - the Corruption of Foreign Public Officials Act. As part of its case against Mr. Karigar, the Royal Canadian Mounted Police alleges that he divulged to others that he had channelled a $250,000 bribe to Mr. Patel while he was minister of Civil Aviation, with the help of a political ally, in 2007. Mr. Patel, who is now Heavy Industries Minister, has said he had no knowledge of the scheme. There is no evidence that he accepted the money. The story dominated the Indian media Friday as supporters from the ruling Nationalist Congress Party (NCP) and the government rose to his defence. Globe and Mail, A15

OTHER / AUTRE

Ottawa a fait la promotion des aliments du Canada après le tsunami au Japon
Ottawa a vu dans le violent séisme et le tsunami survenus l'an dernier au Japon une occasion d'aiguiser l'appétit pour la cuisine canadienne. Le gouvernement fédéral a en effet proposé une activité pour faire la promotion de «la marque Canada» sur le marché japonais. Le plan visait à faire connaître des produits comme le sirop d'érable du Québec, le boeuf de l'Alberta et d'autres denrées aux personnes laissées sans abri par la catastrophe. Selon des documents obtenus par La Presse Canadienne, le Canada devait démontrer son appui en organisant un café en plein air et en nourrissant des victimes avec des produits canadiens afin qu'ils puissent se sentir comme s'ils étaient en visite au Canada. L'Acadie Nouvelle, 9; Whitehorse Star

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-04-12 9:07 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - Part One / Première partie

Daily Media Summary / Revue de presse quotidienne
February 4, 2012 / le 4 février 2012

MINISTER / MINISTRE

NDP MP in hot water again for profanity-laced tirade

Winnipeg NDP MP Pat Martin added fuel to the obscenity-laden firestorm he created this week when he cursed at a Conservative senator who suggested murderers should be given ropes to hang themselves. On Wednesday, Martin cursed Sen. Pierre-Hugues Boisvenu sparking controversy. When demands for an apology were made Thursday, Martin refused. He added perhaps his only mistake was that he didn't include the required honorific when addressing a senator. Boisvenu triggered his own controversy with his comments Wednesday when he was asked about the government's omnibus crime bill, which gives stiffer penalties for certain violent crimes. Boisvenu is an outspoken victims' rights advocate. His daughter was raped and murdered by a repeat offender in Quebec in 2002. He was appointed to the senate in 2009. Manitoba Senior Minister and **Public Safety Minister Vic Toews** demanded Martin apologize. "***Pat Martin's constituents, and indeed all Canadians, would be better served if the MP and his soft-on-crime party, would direct their outrage and vitriol at the criminals who victimize innocent, law-abiding Canadians rather than at a senator whose family has suffered a terrible loss at the hands of a repeat offender***," **Toews said** in a letter to the editor. Telegraph-Journal, A9

Trotting out the bogeyman

An opinion piece states, ""***I don't know if the statistics demonstrate that crime is down ... I'm focused on danger***." That's **federal Public Safety Minister Vic Toews**, speaking to the Senate Committee on Legal and Constitutional Affairs about the Conservatives' "tough on crime" legislation. If nothing else, the next few years are going to have more than their fair share of unintentional hilarity - because unless I completely misunderstood that particular quote, **Toews** has just confirmed what opponents of the new crime legislation have been saying all along. And that's that the legislation has nothing to do with crime, and everything to do with marketing… Rewind a little further, back to when **Vic Toews** actually did realize that statistics demonstrated that crime rates were down to levels last seen in the early '70s. (He must have since forgotten about those statistics, because he clearly doesn't know about them anymore.) He said that the Tory crime bill was to help address the increase in unreported crimes. "***We see this continuing trend of more and more crimes going unreported, and that ... I believe is an indication of a lack of confidence in the justice system***," **Toews** told CTV in September 2010. "***And that is why our government is taking the measures that we are taking***." All right. To get this straight, then: it's the increase in unreported crime (that's a great thing to try and measure in any form - it's big, it's bad, it's ... unreported, hence statistically, well, void) and the increase in ... wait for it ... danger…" The Telegram, A20

Hat's not impressed with Tory justice

A satirical opinion piece states, "Mousie MacKay got a beer from the bar at Louie The Leggers and carried it over to the table where Hat McInnes was sitting, sipping on a beverage, and playing with a small computer… "No, the story I was referring to was the one where, once again the **minister of public safety**, boy, that's an Orwellian mouthful, **minister of public safety**. Anyway, yet another judge has criticized the minister for not allowing a Canadian in prison in the States to serve their time in a Canadian prison." "Seven years for a marijuana bust, that's pretty heavy," said Mousie, "But the Americans are paranoid about drugs. Can you imagine how tense things will get if the Liberals try to legalize marijuana? How come the government slammed the door on this guy, a bit of weed doesn't seem like a capital crime?" "That's one of the problems the judge had, **the minister** didn't really provide any reasons for his denial," said Hat, "so the judge has ordered **the minister** to review the case and provide some good reasons for denying the man a chance to serve his sentence in Canada." "So who stopped the marijuana guy from coming back to a Canadian prison?" asked Mousie. "That was **Vic Toews**, another guy who's made up his mind and doesn't want to be confused by the facts…" The Guardian, A15

One to watch...

A letter states, "Bill C-10: The crime bill. It's not so much the crime bill itself that needs watching; a minority of Canadian voters graciously granted Prime Minister Stephen Harper a majority government, so the bill will pass. What will be interesting to watch is how the bill will play out after it is passed. Even some Tory senators wonder why the Harper government is so fixated on crime, in light of statistics that show crime has actually been decreasing for quite some time. **Public Safety Minister Vic Toews** told a Senate committee reviewing the legislation: "***I don't know if the statistics demonstrate that crime is down. I'm focused on danger***." **The minister** then went on to say his concern is that the public is in danger as long as criminals walk the streets, "***and this legislation addresses that***." Given the statistical decline of murderers, rapists, violent robbers and other shady types, the question has to be asked: Who is **Toews** afraid of when he walks the streets of Canada? Panhandlers? Homeless people?" Winnipeg Free Press, J12

Have your say
A letter states, "OK, Pat Martin lips off again, and again **Vic Toews** runs to the media. He reminds me of a schoolyard child running to his teacher to tattle on another for saying a bad word. And for what? To say sorry? Really! Canadian politics has come down to this? Now that's obscene." Winnipeg Free Press, A17

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Despite weather, flood forecast in works
Manitoba Water Stewardship is working on a spring flood forecast despite this winter's mild and relatively dry weather. Provincial flood forecasters plan to unveil a preliminary flood outlook before the end of February, spokesman Paul White said Friday. Although much of southern Manitoba has experienced dry conditions since June, ground moisture levels -- one of the factors that increases the probability of localized or regional flooding -- remain significant in some areas of the province. While moisture levels are well below those recorded last winter, when the province began preparing for major spring flooding, conditions are comparable to the early months of 1997, the year of the Flood of the Century in the Red River Valley, White said. But across most of southern Manitoba, the snowpack -- another major factor in determining flooding -- is much lower this year. That can change significantly before the spring snowmelt, as one or two blizzards can be the difference between a major flood and no flooding whatsoever. Winnipeg Free Press, A13

B.C. avalanche kills man
One man is dead after a small group of recreational skiers got caught in an avalanche Friday morning on Meadow Mountain, near Kaslo, B.C. The man's name isn't being released until Mounties notify his family. The B.C. Coroner's Service and RCMP are still investigating the death. Windsor Star, A13; Edmonton Journal

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Conditions eased for suspect
Mohammad Mahjoub, a Toronto man detained and subsequently held under house arrest for the past 12 years on a national security certificate because of alleged terrorist ties, was granted more freedoms by a federal court Friday. Mahjoub, 51, was arrested in Toronto in 2000 on a security certificate, which allows the government to detain terror suspects indefinitely without charges or a trial. In his decision, Judge Edmond P. Blanchard said the federal government failed to provide "reasonable grounds to believe" that Mahjoub's security threat has not reduced. While Blanchard said there remains "compelling and credible evidence" that Mahjoub "poses a threat to the security of Canada," evidence during the latest review of Mahjoub's case and his current circumstances suggest that this threat "is now significantly diminished." Windsor Star, A13; National Post; The Telegram

Defenceless
Just what legally constitutes a foreign activity in Canada that is detrimental to this country's national security interests these days, anyway? As it turns out, Canada is practically incapable of answering that question with any enforceable coherence. When it comes to the recent and rapid-succession manoeuvres that have given Chinese state-owned entities the spigot key at critical flow points in Canada's oil and gas industry, mysteries abound. But it is now clear that slowly but surely, Canada's regulatory defences have been almost completely hollowed out. Way back in the 1980s, the Security Intelligence Review Committee was urging amendments to the Canadian Security Intelligence Service Act to spell out what Canadians mean when we talk about foreign-power connivings that are "detrimental" to Canada's national interests. "It is almost wholly subjective: no criteria are provided to offer any standard for determining what is 'detrimental'," a SIRC report once pointed out. The definitions in the CSIS Act still don't clearly define what "detrimental" means, but unlike Investment Canada, CSIS has muddled through and is properly content to couple Canada's "national security" with "the security and economic welfare of Canada." Ottawa Citizen, B7

Muslim group slams 'terrorist' treatment

A Canadian Muslim businessman became a terror suspect for telling sales staff in a text message to "blow away" the competition at a New York City trade show, an association said Friday. Moroccan-born Saad Allami was arrested three days after he sent the message in January 2011 and detained while police searched his home, said the Muslim Council of Montreal. Ottawa Citizen, A4; Le Soleil

MacKay quiet on iran plans
Regional troublemaker Iran poses "a grave threat to peace and security" and is "fanatical and dangerous," Prime Minister Stephen Harper said Friday. Harper made the comments during an interview with Postmedia, and warned that Iran would be ready to use a nuclear weapon if it was able to produce one. But in an interview with QMI Agency, Defence Minister Peter MacKay wouldn't speculate whether Canada -- a staunch ally of Israel -- would join that country in a possible strike against the Islamic regime. Toronto Sun, 24

CYBER SECURITY / CYBERSÉCURITÉ

Confidential police call hacked, leaked
Trading jokes and swapping leads, investigators from the FBI and Scotland Yard spent the conference call strategizing about how to bring down the hacking collective known as Anonymous, responsible for a string of embarrassing attacks across the Internet. Unfortunately for the cyber sleuths, the hackers were in on the call too - and now so is the rest of the world. Anonymous published the roughly 15-minute-long recording of the call on the Internet on Friday, gloating in a Twitter message that "the FBI might be curious how we're able to continuously read their internal comms for some time now." The humiliating coup exposed a vulnerability that might have had more serious consequences had someone else been listening in on the line. The leak was one of a slew of Anonymous hacks that hit websites across the United States Friday, including in Boston, where the police site was defaced, and in Salt Lake City, where officials said that personal information of confidential informants and tipsters had been compromised. Anonymous also claimed credit for defacing the Greek Justice Ministry's website and stealing a mountain of data from the Virginia-based law firm that defended a U.S. Marine recently convicted for his role in the bloody 2005 raid in Iraq that became known as the Haditha massacre. Red Deer Advocate, A5

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

$1M worth of drugs, 13 charged in 'high-level' raid
Thirteen people alleged by police to be "high-level" drug dealers were charged Friday in connection with the latest large-scale sweep orchestrated by Manitoba's organized crime unit. Project Deplete, a police investigation that began last August and culminated Friday with arrests in Winnipeg and Edmonton, is the latest effort of Manitoba's Integrated Organized Crime Task Force, a joint RCMP-Winnipeg police unit that has famously used informants over the past several years to take down primarily the Hells Angels and their associates, with great success. The latest sweep saw charges laid against people police accuse of being major players in the city's drug trade. Some of the accused have gang associations, others are more "independent," police said. Winnipeg Sun, 2

DNR finds barrels of pot
Approximately 29 kilograms of marijuana has been seized following the discovery of the drug by New Brunswick Department of Natural Resources Conservation Officers. Last week, conservation officers were working on an illegal possession of moose meat investigation when they discovered the drug in a number of barrels in a wooded area near a residence in Scoudouc. They then called the District 4 RCMP who began an investigation. Times & Transcript, A6

Police make arrest and seize cocaine, marijuana
A 33-year-old Saint John man has been arrested after police seized a large amount of cocaine and marijuana from the city's east side. Russell William McCain of Canterbury Street faces a number of drug-related charges, police said in a release. McCain's arrest came after a three-month investigation by members of the Saint John Police Force street crime unit and the Fundy Integrated Intelligence Unit. The RCMP and the Rothesay Regional Police Force participated in the drug raid on Thursday. Telegraph-Journal, B3

Mountie rescues child from car
Surrey, B.C. Mom Alyse McDonald will be forever grateful to RCMP Const. Aaron Jabs. The off-duty police officer went out his way Wednesday morning to pull McDonald's two-year-old daughter Haylee from the wreckage of the family car, which was upside down in a watery ditch in Delta. Telegraph-Journal, A4

Arrest in $200k scam on senior

A man accused of scamming a 90-year-old B.C. homeowner out of more than $200,000 was busted in northern Manitoba last week and sent back to Vancouver Island. Richard Patterson, 47, was arrested Jan. 25 in Norway House on the strength of a Canada- wide warrant for fraud over $5,000, according to Manitoba RCMP. He was charged by Victoria police last summer for allegedly bilking a 90-year-old resident of the B.C. capital out of more than $200,000 for renovations he was supposed to be doing on the man's house. Winnipeg Sun, 13

Porn sting may yield more arrests

The different investigations, some of which lasted eight months, came to a head Jan. 31 and Feb. 1. Police executed 76 search warrants and laid 213 charges against 60 people, including three young offenders. The people nabbed in Windsor face a range of charges including accessing child pornography, possession of child pornography, distribution of child pornography and luring a child for sexual purposes. Staff Sgt. William Donnelly with Windsor police said additional arrests are possible, but that could take awhile as police sift through child porn photos that are "traded around like hockey cards." Windsor Star, A5

Alleged cyber sicko

She thought she knew him and she wasn't alone. Toronto Police claim many teen girls across the country met Alex Sirop online and believed he was a good-looking 19-year-old. They had no idea when they sent "compromising" images of themselves over the web that a 42-year-old Scarborough man named Shiraz Nariman was allegedly adding them to his collection of child porn. Nariman is one of 54 people rounded up recently by police in Ontario during a massive child pornography sweep. The RCMP first learned of him when a teenage girl, who can't be named, came forward in September 2010. Toronto Sun, 7; Toronto Star

Man charged with making child porn

A man has been charged with producing child pornography following a year-long investigation by the Edmundston City Police Force and the New Brunswick RCMP's Internet Child Exploitation Unit. Shane Evan McCabe, 34, of no fixed address, was arrested on Thursday upon his release from jail where he was serving time for failing to register with the National Sex Offender Registry for past convictions. The investigation began in March 2011 when images of child sexual abuse were found scattered around the City of Edmundston. The Fredericton Police Force, the RCMP's Technological Crime Unit, the National Child Exploitation Coordination Centre, the Canadian Centre for Child Protection (cybertip.ca), the RCMP's Violent Crime Linkage Analysis System and the National Sex Offender Registry also assisted with the investigation. Times & Transcript, A9

Two grow-ops found same day

London police busted two marijuana grow-ops in less than three hours, seizing nearly $600,000 in drugs. Both grow operations, located less than eight kilometres apart, were in middle-class north London neighbourhoods. London Free Press, A8

Police reveal drug lab photos to highlight ecstasy dangers

Filthy conditions, unknown chemicals and a pill press covered in ecstasy: this is what a drug lab looks like. In their latest effort to showcase the dangers associated with street drugs, police released photographs on Friday of an ecstasy lab in Richmond, B.C., in light of the many deaths in Calgary and B.C. tied to ecstasy laced with a toxic chemical. Seven people in Calgary, and one person in Red Deer, have died from taking ecstasy (MDMA) laced with para-methoxymethamphetamine (PMMA). Two additional cases are still awaiting toxicology results. There have been five deaths reported in B.C. The chemical, a cheaper alternative than MDMA, is being cut into ecstasy, but is believed to be more toxic. B.C. RCMP Sgt. Duncan Pound said when officers entered the lab in full protective suits in 2008, they found 750,000 pills and enough drugs to make 3.3 million tablets. Calgary Herald, B1

Date-rape drugs among $17K bust

Mounties in Red Deer say they've made a major seizure of so-called date rape drugs that were meant to be trafficked. On Thursday, Mounties executed a warrant on a Red Deer residence, where a search turned up two kinds of drugs known to be used to incapacitate unwitting victims who are then sexually assaulted. In the search of the house and garage, they found three litres of gamma hydroxybutyric acid (GHB), as well as 10.8g of ketamine, which can be slipped into drinks. Calgary Sun, 20

Remains found on reserve

Human remains have been found in a vacant home on the Nak'azdli reserve in B.C., RCMP said Friday. The remains were reported to police Wednesday afternoon. The reserve is located about 150 km northwest of Prince George. It is considered a suspicious death at this point, Corp. Annie Linteau said. Edmonton Sun, 23

Civilian oversight of police a must

An opinion piece states, "The continuing fall-out over the violent arrest of Adam Nobody during the G20 raises serious doubts about the adequacy of civilian oversight of the police. Eighteen months later, one officer, Const. Babak Andalib-Goortani, has been charged criminally with assault by the province's Special Investigations Unit. Another provincial body, the Office of the Independent Police Review Director, has recommended Andalib-Goortani and four others -- Constables Michael Adams, David Donaldson, Geoffrey Fardell and Oliver Simpson -- face disciplinary charges. But the SIU says since the standard of evidence for identifying officers is higher for a criminal case than disciplinary hearings, no new criminal charges will be laid... But the larger issue is the lack of co-operation the SIU has received from police, not just in G20 cases in Toronto, but across the province." Ottawa Sun, 12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Deportation for dirtbag
Clato Mabior's time on Canadian soil appears to be quickly winding down. Mabior, convicted of aggravated sexual assault for failing to disclose his HIV status to sexual partners, will be deported to Sudan in the next 30 days -- likely on Feb. 15, according to his immigration lawyer. Mabior, 34, was ordered held in custody at a review of his ongoing detention Friday. He's been behind bars on the strength of a deportation order since October 2010. The Immigration and Refugee Board has repeatedly ruled that Mabior is a flight risk and a danger to the public. Winnipeg Sun, 3

The hangover
On May 13, 2011, a prominent Canadian DJ crossed the Alberta-B. C. border near Lake Louise with a case of red wine, daring authorities to arrest him. The Mounties refrained but Terry David Mulligan had made a point of mocking a lingering hangover of Alberta alcohol prohibition 87 years after its repeal. Yet, it's still illegal to cross provincial borders with booze. While flamboyant bootleggers such as Al Capone, furtive speakeasies and rumrunners are colourful legends of the 1920-1933 U.S. prohibition, Canada's own doomed attempt at shutting off the taps has barely had a last recall. Calgary Sun, 18

Mugesera finally finds Rwandan lawyer
Rwandan lawyers haven't been lining up to defend Léon Mugesera - wanted for almost two decades for his role in the 1994 Rwandan genocide - but one has stepped forward, despite possible security issues and little pay. Guy Bertrand, the Quebec City lawyer who helped the suspected war criminal dodge deportation from Canada for years, said it was difficult to find someone willing to take on his client. He fears for the Rwandan attorney's safety but can't afford to hire a bodyguard. For security reasons, Bertrand didn't want to reveal the lawyer's name or put The Gazette in touch with him, but Rwandan news organizations reported he is Donat Mukunzi. Montreal Gazette, A8

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

VICTIMS TREATED CRIMINALLY
It's about time someone started talking about the rights of victims in the criminal justice system. Canada's ombudsman for victims' rights Sue O'Sullivan released a special report this past week on the need for governments, the courts and corrections to start taking the rights of victims of crime far more seriously than they have in the past. And her report is bang-on. I recommend every elected official in Canada read it. I've met enough victims of crime over the years to know exactly what O'Sullivan is talking about. We spend a lot of time in the justice system dealing with the criminals themselves -- their sentences, their rights, etc. -- but not enough time ensuring victims have the legislated rights they deserve. Winnipeg Sun, 5

Group aims to 'out' pedophiles
A Christian-oriented activist group said Friday it plans to launch a website for identifying pedophiles. Canada Family Action said its website will be called FindA-Pedophile.com. Brian Rushfeldt, president of the organization, said he hopes to have the site operational by March. The Calgary-based group said the recent bust of 60 people in Ontario on hundreds of child pornography charges is proof that such a resource is needed. Rushfeldt said the information will be gathered from sources such as the courts, police and media reports. Montreal Gazette, A15; Ottawa Sun

Quebec man wants senator prosecuted for suicide comments
A Quebec man has filed a police complaint against Conservative Senator Pierre-Hugues Boisvenu for remarks he believes could lead someone to commit suicide. The complaint came after Boisvenu said Wednesday in Ottawa that some convicted killers - he referred specifically to Paul Bernardo, Clifford Olson and Robert Pickton - should be given a rope in their prison cells in case they want to hang themselves. The senator later apologized for his comments, but 26-

year-old Jacques McBrearty said Boisvenu went too far. The Sûreté du Québec will investigate the complaint, which could eventually be handed over to the RCMP since the events occurred in Ontario, where Boisvenu lives. Montreal Gazette, A10

Kamloops jail too easy to break in to
A review conducted before two recent break-ins at the Kamloops Regional Correctional Centre, apparently to smuggle contraband - possibly drugs - to prisoners, revealed the Interior British Columbia jail must beef up its security practices. Dean Purdy, spokesman for the B.C. Government Employees' Union, said in each case someone scaled the jail's two-metre high perimeter fence and cut a hole in a cell window in the segregation unit. Early reports suggested a laser was used to drill into one of the pieces of Lexan glass. The Daily News has learned a blowtorch was used. Purdy believes the breaches were made to smuggle contraband - possibly drugs - into the prison. The incident raises alarm bells for the union, which is conducting its own investigation along with the province's corrections branch and RCMP. Edmonton Journal, A19

No honour in killing
Imams across North America are condemning the act of "honour killing" on the heels of the guilty verdict and life sentences handed to the Shafia family last Sunday. Mohammad Shafia, 59, his second wife Tooba Mohammad Yahya, 42, and the couple's son, Hamed, 21, were each convicted on four counts of first-degree murder for killing Shafia daughters Zainab, 19, Sahar, 17, Geeti, 13, and Mohammad's first wife, Rona Amir Mohammad, 52. "There is no such thing in Islam that if somebody is bringing disgrace to your family's honour that you go out and kill that per-son," said Imam Syed Soharwardy, founder of the Islamic Supreme Council of Canada. Soharwardy will be issuing a Fatwa on Saturday, a type of religious edict, with more than 34 signatures from imams across North America supporting its position against honour killings, domestic violence and misogyny. Toronto Sun, 9

Des propos condamnables
Une article d'opinion dit, «Une fois de plus, une personnalité publique, en l'occurrence un sénateur bien connu au Québec, s'enflamme et tient des propos qui ne devraient jamais sortir de la bouche d'une personne qui exerce une aussi grande influence sur l'opinion publique. Bien que l'incommensurable souffrance associée à la perte d'un enfant puisse nous amener à comprendre ses motivations profondes, il n'en demeure pas moins que ce genre de propos qui viennent plus du coeur que de la tête sont condamnables lorsqu'on occupe une position politique importante. Cette idée de laisser une corde dans la cellule des criminels ayant commis un homicide est barbare et rétrograde et n'a pas sa place dans une société moderne comme la nôtre.» Le Nouvelliste, 21

PUBLIC SERVICE / FONCTION PUBLIQUE

Whistleblowers in public service face reprisal: integrity group
Public servants who disclose wrongdoing invariably face workplace reprisals despite laws promising protection, says the head of an organization that promotes integrity and accountability within government. David Hutton, executive director of FAIR (Federal Accountability Initiative for Reform), said he's received hundreds of calls from whistleblowers since assuming his volunteer position in 2008. In some jurisdictions, those who punish whistleblowers can lose their jobs, go to jail and be sued. Australia and Britain are "decades ahead of us" in comparison to the "absolutely dreadful" whistleblower law in Canada, Hutton said. He was responding to a report, prepared for the Office of the Public Sector Integrity Commissioner, which says government employees fear career-limiting reprisals if they blow the whistle on wrongdoers in the federal public service. The report summarizes the findings of 10 focus groups held last November to explore public servants' perceptions about disclosing wrongdoing in their workplaces. It paints a picture of a public service that recognizes its responsibility to disclose wrongdoings, at least in principle, but is fearful of the consequences. Ottawa Citizen, A3

INTERNATIONAL / INTERNATIONAL

Inquiry urged over bribery case
Indian opposition leaders are calling for a government inquiry into allegedly corrupt dealings at the country's Ministry of Civil Aviation, following a Globe and Mail report on bribery and bid-rigging allegations that implicate, among others, cabinet minister Praful Patel. The Globe has detailed the allegations against Nazir Karigar, a 64-year-old Indian-born Canadian citizen and the first individual to be charged under Canada's foreign bribery law - the Corruption of Foreign Public Officials Act. As part of its case against Mr. Karigar, the Royal Canadian Mounted Police alleges that he divulged to others that he had channelled a $250,000 bribe to Mr. Patel while he was minister of Civil Aviation, with the help of a political ally, in 2007. Mr. Patel, who is now Heavy Industries Minister, has said he had no knowledge of the scheme.

There is no evidence that he accepted the money. The story dominated the Indian media Friday as supporters from the ruling Nationalist Congress Party (NCP) and the government rose to his defence. Globe and Mail, A15

OTHER / AUTRE

Ottawa a fait la promotion des aliments du Canada après le tsunami au Japon
Ottawa a vu dans le violent séisme et le tsunami survenus l'an dernier au Japon une occasion d'aiguiser l'appétit pour la cuisine canadienne. Le gouvernement fédéral a en effet proposé une activité pour faire la promotion de «la marque Canada» sur le marché japonais. Le plan visait à faire connaître des produits comme le sirop d'érable du Québec, le boeuf de l'Alberta et d'autres denrées aux personnes laissées sans abri par la catastrophe. Selon des documents obtenus par La Presse Canadienne, le Canada devait démontrer son appui en organisant un café en plein air et en nourrissant des victimes avec des produits canadiens afin qu'ils puissent se sentir comme s'ils étaient en visite au Canada. L'Acadie Nouvelle, 9; Whitehorse Star

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

Williston, Sandra

From: Beaudoin, Luc
Sent: February-03-12 1:13 PM
To: Cameron, Bud; Turbide, Frank
Cc: Bendelier, Kenneth
Subject: Re: Well, if anyone is looking to understand Anonymous TT&P

Add a + at the end of the goo.gl link for more info...

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: Cameron, Bud
Sent: Friday, February 03, 2012 11:32 AM
To: Beaudoin, Luc
Cc: Bendelier, Kenneth
Subject: RE: Well, if anyone is looking to understand Anonymous TT&P

Seems like Ken is awfully knowledgeable about the inner workings of Anon.
Should we turn him in?

From: Bendelier, Kenneth
Sent: February-03-12 9:08 AM
To: *
Subject: Well, if anyone is looking to understand Anonymous TT&P

Pages 59 to / à 60

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

s.16(2)(c)

"We are not put on this earth to sit still and know; we are put into it to act."
Woodrow Wilson

Bonvie, Jeff

From: Bonvie, Jeff
Sent: February-03-12 1:49 PM
To: Grigsby, Alexandre; Dvorkin, Corey; Bradley, Kees
Subject: Oops...

If you didn't see this previously...

http://www.wired.com/threatlevel/2012/02/anonymous-scotland-yard/

Williston, Sandra

From: Beaudoin, Luc
Sent: February-03-12 10:38 AM
To: CYBERDO
Subject: Anonymous released fbi

s.15(1) - Int'l
s.16(2)(c)

[redacted]. This was on a maillist... Could be interesting

>

[redacted]

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

Dincoy, Rana

From: Bendelier, Kenneth
Sent: February-01-12 12:41 PM
To: Dincoy, Rana; Klassen, Nathan
Subject: Anonymous

s.16(2)(c)

- Anonymous
- AnonOps - GeneralActions
Source: anonops
Complete item: [redacted]

Description:
STOP War Against Iran.
STOP Economic shocks.
NO MORE S.O.P.A / A.C.T.A. / Biden-Sinde-Wert-Law / ...
NO MORE Censorship.
OPEN DATA.
FREE Manning, FREE Assange, FREE Anons.
FREE KNOWLEDGE.

SPREAD THE WORD.
EXPECT US!

Ken's Assessment: No worries Anonymous, we'll have all these requests fulfilled by noon tomorrow. Thank you for pointing these issues out to us.

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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 66 to / à 73

are withheld pursuant to sections

sont retenues en vertu des articles

20(1)(b), 20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Page 74

is withheld pursuant to sections

est retenue en vertu des articles

19(1), 20(1)(b), 20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 75 to / à 169

are withheld pursuant to sections

sont retenues en vertu des articles

20(1)(b), 20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-03-12 8:35 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; Houston, Laura; Jones, Scott; ; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 3, 2012 / le 3 février 2012

Online Media / Médias en ligne

Neo-Nazi member calls hacking 'an invasion of privacy'
Some Canadians whose associations with white supremacist and neo-Nazi groups were recently revealed, are defending their involvement with the organizations, while others deny having anything to do with the groups anymore. CBC News reported Wednesday that the names of 74 Canadians were found in files leaked by computer hackers in Europe who were intent on exposing hate movements. The identities were revealed on a website called nazi-leaks.net, which is now offline. "It is an invasion of privacy," said Joel Henry, of Langley, B.C., in a telephone interview with CBC News Thursday. Police and government security organizations should be able to make use of the hacked information, according to Simon Fraser University professor Andre Gerolymatos, who has written extensively on espionage. CBC News; Yahoo! News Canada

FBI: Cyber threat might surpass terror threat
Today, FBI Director Robert Mueller told the U.S. House Permanent Select Committee on Intelligence that he believes "the cyber threat will equal or surpass the threat from counter terrorism in the foreseeable future." He elaborated on the breadth of the threat, saying "there is very little we do in this day and age that is not on or somehow associated with the internet. The theft of intellectual property, the theft of research and development, the theft of the plans and programs of a

corporation for the future, of all which are vulnerable to being exploited by attackers." On Tuesday, Mueller testified at the Senate Select Intelligence committee's hearing on worldwide threats. He had similar warnings about cyber security, and elaborated on three ways the FBI and intelligence agencies need to address the concern. CBS News; Infosecurity Magazine

Intelligence Leaders Urge Congress to Act on Cyber Laws
The threat to U.S.-based computer networks is one of the country's most pressing security problems, and Congress needs to act on it soon, the director of national intelligence told a congressional panel today. James R. Clapper Jr. said he and all of the U.S. intelligence leadership agree the United States is in a type of cyber Cold War, losing some $300 billion annually to cyber-based corporate espionage, and sustaining daily intrusions against public systems controlling everything from major defense weapons systems and public air traffic to electricity and banking. Clapper was joined by CIA Director David H. Petraeus, Defense Intelligence Agency Director Army Lt. Gen. Ronald L. Burgess Jr. and FBI Director Robert S. Mueller for a House Select Intelligence Committee hearing on worldwide threats. He urged lawmakers to pass a bill that forces intelligence sharing between the government and the private sector, such as the Defense Industrial Base pilot program that then-Deputy Defense Secretary William J. Lynn III launched last year. U.S. Department of Defense News Release

Security Slackers Risk Internet Blackout on March 8
Companies and home users whose computers or routers are infected by the DNSChanger Trojan risk being unable to access the Web come March 8, 2012. That could represent a substantial number of users, too, as half of Fortune 500 companies and government agencies are infected with the malware, according to a new report. Back in November, the feds famously took down the DNSChanger botnet network, which a cyber criminal gang was using to redirect Internet traffic to phony websites that existed simply to serve up ads. The feds replaced the criminals' servers with legitimate ones that would push along traffic to its intended destination. That surrogate network was supposed to be temporary -- in operation just long enough for companies and home users to remove DNSChanger malware from their machines. Said network is slated to be unplugged on March 8. Once the surrogate server network is unplugged, computers infected with DNSChanger will not be able to access the Internet: The malware will send requests to servers that will no longer be online. PC World; BCS

Symantec warns of Android Trojans that mutate with every download
Researchers from security vendor Symantec have identified a new premium-rate SMS Android Trojan horse that modifies its code every time it gets downloaded in order to bypass antivirus detection. This technique is known as server-side polymorphism and has already existed in the world of desktop malware for many years, but mobile malware creators have only now begun to adopt it. A special mechanism that runs on the distribution server modifies certain parts of the Trojan in order to ensure that every malicious app that gets downloaded is unique. This is different from local polymorphism where the malware modifies its own code every time it gets executed. Symantec has identified multiple variants of this Trojan horse, which it detects as Android.Opfake, and all of them are distributed from Russian websites. PC World Australia

MSUpdate trojan attacked companies in the defence sector
Unknown attackers have tried to use an invitation to a prestigious conference to inject a trojan into companies in the defence sector. The security firms Seculert and Zscaler report that opening an attached PDF flyer caused recipients' computers to be infected with spyware via a previously undisclosed hole in Acrobat Reader. According to the report, the attack mainly targeted government-related organisations, including military and aerospace contractors, in Europe and in the US. The security firms said that the attacks started back in 2009 and peaked in autumn 2010. Talking to The H's associates at heise Security, Seculert CTO Aviv Raff added that compromised computers, some of which had been infected for two years, were only discovered a few weeks ago. A zero day hole in Adobe Reader was exploited to inject the msupdater.exe trojan into systems; once injected, the trojan did its best to look like a regular update process... The H Security; Infoboom; CIO Insight

Trojan found breaking Yahoo CAPTCHA security in minutes
Researchers have discovered a malware engine that appears to be able to break the CAPTCHA security used by Yahoo's webmail service after only a handful of attempts. There is nothing new in malware that tries to break CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) - a low-level war has been ongoing since this type of security was first implemented almost a decade ago - but what matters is how quickly and invisibly this can de done. Websense has posted an online video showing the effectiveness of the engine it found working as part of the Cridex banking Trojan malware in breaking down Yahoo's CAPTCHA process. Cridex itself is a traditional if rather dangerous login harvester that targets online banks and social media sites from victim PCs, uploading stolen data to a command and control server. PC World New Zealand

Drive-by Downloads Observed in Over 50% of Malware Assaults

Sophos the company for data protection and IT security, which released its new "Security Threat Report 2012," evaluates in detail the threat scenario starting with hacktivism as well as notes that over 50% of malware assaults against Web-surfers currently comprise drive-by download assaults. Specifically as per the report, a certain attack code for drive-by download is responsible for 31% of the total assaults over the Web spotted during H2-2011. SPAM Fighter

Brazil-Focused Hackers Hit HSBC's Global Banking Sites
Hackers on Thursday kept up their campaign to cripple Brazilian banking websites and, in a new twist, their efforts appeared to affect both local and global websites of U.K.'s HSBC Holdings PLC. This is the fourth attack in as many days by the Anonymous Brasil group, which says the effort is part of a campaign aimed at social activism in Brazil, and not theft. Earlier this week, the attacks hampered operations on the websites of Banco do Brasil SA, Itaú Unibanco Holding SA and Banco Bradesco SA. A spokesman for HSBC in New York confirmed the bank experienced "technical difficulties" with some of its websites, but said the issues are now resolved. The issue was part of the "unauthorized Internet activity" in Brazil that affected the North American sites, he added. But "customer accounts have not been compromised in the U.S. or Canada," the spokesman said. Wall Street Journal

Android Bouncer boots out 40 per cent of malware
The Android Market, like Newcastle's Bigg Market, is getting too rowdy, but with malware and viruses instead of Scouse hen parties. Now Google's Bouncer is manning the doors, looking for potential troublemakers and booting out offending apps. Google says it's been working on Bouncer for several months now -- and the search giant already claims to have achieved a 40 per cent drop in malware. Bouncer scans both new and existing apps for spyware and trojans that could steal your data or mess with your phone, as well as monitoring the behaviour of developers so it can kick out offenders and stop them from coming back. It also virtually runs all apps on the market to see how it would perform on an Android device. If it detects a new type of threat, it rescans everything to see if it's present elsewhere. CNet; Computerworld; The H Security; Wall Street Journal

Banking malware 'a growing threat', as new variant of Zeus is detected
Malware that steals users' identity and empties their bank accounts has been cited as a growing threat to Britain. According to Parliament's Science and Technology Select Committee report, which was released this week, a lack of awareness is to blame and it called for greater use of the Get Safe Online website. The report claimed that infection with malware takes cyber crime to a different level as "experts use their technical skills to, among other things, take over computers worldwide to steal bank details and identity information". It also claimed that Dr Richard Clayton, research assistant at the University of Cambridge who was involved in gathering the research, did not believe it was possible to bring the population up to the level of technical knowledge required to defend itself; instead we needed to "rely on those who make the software to adapt it in such a way that you no longer need to read the URL in order to be safe". SC Magazine UK

Hackers manage to outsmart online banking security systems
They use the Man in the Browser (MitB) scheme to steal account holders money. Hackers have started targeting banking institutions by managing to outwit the latest online banking security techniques. The hackers fool the account holders with an offer of training in a new "upgraded security system" after being logged into the bank's real site. They later move out the money out of the account holders, without leaving any traces of evidence to the user about the theft, according to the BBC. This method of victimising users, which has been dubbed the Man in the Browser (MitB), uses malware to manipulate what is seen on the screen or keyed in by the user. CBR Online

Sophos says Counterclank is not Android malware
SECURITY OUTFIT Sophos has classed the controversial Counterclank Trojan as advertising not malware. At the beginning of the week Symantec revealed the Counterclank Trojan, which it claimed was the biggest malware distribution of the year. Mobile security firm Lookout disagreed, saying it was just an aggressive form of an ad network, an assessment with which Sophos agrees. Symantec found the code present in 13 apps on the Android Market and classed it as malware because it sends information about the phone to a remote server called Apperhand. Vanja Svajcer, principal virus researcher at Sophos said, "It turns out that the Apperhand framework is related to an advertising framework used more than half a year ago by the Plankton app." The Inquirer; PC Magazine

Kelihos botnet makes a comeback
A once-dead botnet has been resurrected and resumed its spamming ways. The original Kelihos botnet compromised only about 41,000 computers but was capable of sending 3.8 billion spam e-mails each day promoting unregulated pharmaceuticals, fraudulent stock scams and, in some cases, sites dealing with sexual exploitation of children. Microsoft and Kaspersky Lab took down the malware last September using a "sinkhole" technique that tricked the infected computers into getting their instructions from a computer the companies controlled. However, while the technique was effective at disabling the botnet quickly, it was merely a temporary fix as many computers remained infected, and "as this particular case showed, it is not very effective if the botnet's masters are still at large," Kaspersky Lab's Maria Garnaeva

said in a blog post. "Our investigation revealed that the new version appeared as early as September 28, right after Microsoft and Kaspersky Lab announced the neutralization of the original Hlux/Kelihos botnet." CNet

Facebook, Microsoft, Google, Yahoo team up for anti-phishing standards
Fifteen tech giants and email service providers have put their heads together to combat phishing, the practice of sending a deceptive email that spoofs a legitimate entity. The Domain-based Message Authentication, Reporting and Conformance (www.dmarc.org) has developed standards to combat the threat from phishing as well as spam. DMARC.org said it "draws upon a history of private industry collaboration with 18 months of dedicated work, to outline an enhanced vision for email authentication that can scale up to today's Internet needs." DMARC.org is an unincorporated working group made up of 15 of the world's leading email providers, financial institutions and service providers, including: AOL, Gmail, Hotmail, Yahoo! Mail (email), Bank of America, Fidelity Investments, PayPal (financial institutions), American Greetings, Facebook, LinkedIn (social media properties), Agari, Cloudmark, eCert, Return Path, and Trusted Domain Project (email security solutions providers). The group aims to develop Internet standards to reduce the threat of email phishing and to improve coordination between email providers and mail sender domain owners. GMA News; Sophos

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-02-12 9:05 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: ADDENDUM: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 2, 2012 / le 2 février 2012

Online Media / Médias en ligne

Hacked neo-Nazi websites reveal Canadian connections
The names of dozens of alleged white supremacists in Canada are contained in files leaked by computer hackers in Europe intent on exposing hate movements, CBC News has learned. The alleged white supremacists' names were revealed earlier this month by members of a loose-knit group of hackers called Anonymous on a website called nazi-leaks.net, which is now offline. CBC News

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

s.16(2)(c)

Williston, Sandra

From: Beaudoin, Luc
Sent: February-01-12 7:08 PM
To: CYBERDO
Subject: Anonymous

To add to existing anonymous activity
Anonymous claim to have breached the Irish Department of Foreign Affairs (www.dfa.ie) and posted userids and passwords to pastebin http://pastebin.com/

It appears the site affected is the

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-01-12 8:40 AM
To: Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Black, Dave; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hebert, Brigitte; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki; * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Arruda, Filo; Baker, William V.; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Forster, John; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
February 1, 2012/ le 1 février 2012

Print Media

Kim Dotcom faces charges - Megaupload founder facing extradition
In a New Zealand jail awaiting extradition to the U.S. on charges of racketeering, money-laundering and copyright crimes, (Kim) Dotcom has found himself at the centre of a high-stakes battle over Internet freedom versus copyright protection. It is a fight touching institutions from Congress to Silicon Valley and pitting the recording industry against some hip-hop artists who see Megaupload as a way to bypass record-label middlemen. In the days after Dotcom's arrest, the case has triggered an angry response from the hacker group Anonymous, which began an attack that briefly shut down websites, including the Justice Department, FBI, Universal Music and others. Vancouver Province

Online Media

Cyber Assault Aiming at Defense Department's Access Cards Sourced to China

Service members are reportedly getting an e-mail that has a formal-appearing PDF file infected with one new PC-virus facilitating keystroke logging, says California-located cyber-security company Alien Vault's lab manager Jaime Blasco. Miliatry.com published this in news on January 24, 2012. The virus, by recording keystrokes, garners the service member's PIN for Common Access Card, a type of smart-card as he reaches for a government system. According to Blasco, the cyber assault possibly has its source in China since the malware's written code contains Chinese characters. Blasco also explains that from the time of tracing the attack, the security company discovered software, which was solely utilized in China. Alien Vault's researchers are 99% sure, though not 100%, but quite certain that the attack originated out of China, Blasco adds. DoD BUZZ published this in news on January 24, 2012. SPAMFighter News

Report: Israel well prepared for cyber war
According to SDA-McAfee report, Jewish state experiences 1,000 cyber attacks per minute, but is most prepared to defend itself and deal with them. On the other hand, Israel initiates most attacks against its enemies – alongside Russia, China. "Israel has a national computer emergency readiness team (CERT), it participates in the informal CERT communities, it has a cyber strategy and a cyber command," says a report on cyber-preparedness authored by Brussels' specialist security and defense think-tank Security & Defense Agenda (SDA) with the support of computer security company McAfee. The report gives Israel a score of 4.5 out of 5 for its preparedness for a cyber attack. YNet News

An apocalyptic fantasy or an actual threat? How crippling would a cyberattack on the nation's power grid be?
Former chairman of the Joint Chiefs of Staff Adm. Michael Mullen, who retired in September, said during his tenure that cyberattacks pose an "existential threat" to the United States. While spies, cyberthieves and garden-variety hackers have caused untold economic loss to governmental agencies, companies and individuals by stealing information, the threat of a downed power grid and damage to other critical infrastructure presents a far greater risk, security analysts say. Measures are under way to bolster security, but some analysts say they offer too little. Asbury Park Press

'Make cyber laws enforcing websites to respond faster to govt'
Setting up a regulatory mechanism and making a law to force websites to respond faster would be a better solution than completely blocking websites if they carry objectionable content, a cyber security expert said here today. "I support not completely blocking popular social networking websites. In terms of illegal content, the government should create a regulatory authority where they will closely work with all these different websites. Whenever there is something offensive that is posted, it will be removed," Ankit Fadia, a prominent computer security expert and ethical hacker, told PTI. The regulatory mechanism should be broad-based without the government representatives alone having monopoly, he said. Daily News and Analysis (India)

"Slain" Kelihos botnet still spams from beyond the grave
A botnet capable of delivering almost four billion spam messages per day has been confirmed resurrected—more than four months after Microsoft celebrated its untimely demise. Researchers with Kaspersky Lab reported on Tuesday that Kelihos, a peer-to-peer botnet that also goes by the name Hlux, continues to spew spam in a variety of languages. A new version of the underlying malware appeared as early as September 28, 2011, a day after Microsoft took credit for disrupting the rogue network by commandeering the infected computers and obtaining a court order seizing the Internet addresses used to help control them. The resurrection highlights the difficulty of permanently severing botnets from the Internet. ARS Technica

Update: Windows Media Player vulnerability
New research from M86 Labs adds further insight on the MIDI exploit first highlighted by Trend Micro last week. The attack uses the methodology described by Vupen; a non-trivial exploit that works in Internet Explorer 6 to 9. Microsoft fixed this vulnerability in its January patch release. M86 describes how an infected web page hosted in South Korea loads a malicious MIDI file. The MIDI file is used to download an executable which is itself a downloader. This fetches the ultimate payload; a basic rootkit. Info Security

Defense companies persistently targeted by cyber spies
Researchers from security companies Zscaler and Seculert have issued a warning about bogus emails targeting employees of defense-related organizations around the world in order to trick them into installing malware. "Dear Sir, It is a conference that you may possibly be interested in. More information is attached below," says in the recent emails. The attached file is a specially crafted PDF that, at first glance, looks like a completely harmless invitation to a relevant industry conference such as the IEEE Aerospace Conference or an Iraq Peace Conference. But, once downloaded and opened, the file exploits vulnerabilities within Adobe Reader in order to drop and run a Trojan that opens a backdoor into the system. Help Net Security

BitDefender Finds Fresh Threat that's Mixture of Malicious Programs
BitDefender, which analyzed 10m contaminated files, found approximately 40,000 samples of "Frankenmalware." Reportedly, these samples represent some 0.4% of detected malicious programs. Thus, according to the company, the

situation suggests about 260,000 hybrid samples as potentially floating in cyber-space. ITProPortal published this on January 24, 2011. Understandably, the company began its research of the malware sandwiches when it discovered the Rimecud worm that a file infector, Vitrob contaminated. The former malicious program filches passwords for e-mail accounts, social-networking, online shopping, e-banking, amidst other functions. In the meantime, Vitrob lets the remote attacker issue commands, while the file-infector effectively evades firewalls as well as makes sure it stays on the host PC via performing a code-insertion inside one critical process namely Winlogon. SPAMFighter News

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

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: February-01-12 8:11 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
February 1, 2012 / le 1 février 2012

MINISTER / MINISTRE

Top Mountie says he is moving fast to end harassment on force
A day after the RCMP Public Complaints Commission issued a call for citizen input in its probe of harassment complaints involving the Mounties, Canada's new RC-MP commissioner outlined the steps he's already taken to address the issue. Testifying before a Commons committee Tuesday, Bob Paulson said he has centralized oversight of all harassment complaints in Ottawa to ensure they are dealt with in a timely fashion. Paulson also faced a barrage of questions Tuesday about whether the federal government was trying to muzzle him. He denied the allegations, which surfaced earlier this month after Senator Colin Kenny unveiled details of an email exchange he had with Paulson in which he was told that all meetings with the commissioner had to be routed through **Public Safety Minister Vic Toews' office**. Paulson told parliamentarians that it's always been the RCMP's practice to inform **the minister** responsible for the force about meetings that may have political implications and that the guidelines have simply been consolidated into a single communications protocol. He even hinted that the real reason he "routed" Kenny through **the minister's office** was because he didn't really want to meet with the outspoken Liberal who has a keen interest in justice issues. "I'd just as soon not meet with Sen. Kenny, to be honest with you," Paulson said, refusing to elaborate later. Ottawa Citizen, A3 (Edmonton Journal, Calgary Herald)

Top Mountie dogged by accusation he's muzzled
The commissioner of the RCMP has batted away allegations the federal government is trying to muzzle him. He was called to testify over recent allegations that **Public Safety Minster Vic Toews** stopped him from meeting Liberal Senator Colin Kenny, prompting the NDP to accuse the Conservatives of trying to control Mountie communications. Calgary Sun, 23 (Edmonton Sun); Toronto Star; The Province; * National Post

We're now a banana republic
A letter to the editor states, "It would seem that **Vic Toews** has a problem with memory. The utopian parliamentary system he speaks of is not in Canada. I have watched Parliament for quite a few years. Among other egregious behaviour, the dysfuntionality of parliamentary committees is legendary - ask any opposition member. Under this government, Parliament has degenerated almost beyond redemption. It is ludicrous to expect Canadians to believe anything coming out of the PMO, where all messages originate..." Toronto Star, A24

Smugglers dump Canada-bound Tamils in Togo
Two hundred Tamil refugees from Sri Lanka are stranded in West Africa, BBC reports, after the human smuggling ring they hired to bring them to Canada marooned them in Togo. The BBC says the contingent travelled by ship from Sri Lanka to India, then on to Ethiopia before flying to Togo. After being assured they could fly to Canada from neighbouring Ghana, they say their human smuggler abandoned them, the report says. **Public Safety Minister Vic Toews** said Tuesday he could not confirm reports about the wayward refugee claimants. "***I understand that there's some rumours going around in respect of another illegal migrant boat***," he said. ***"I can assure you that our agencies work closely with governments around the world in order to stop criminal activities with respect to human smuggling"..."We will continue to work with allies overseas and ensure that human smugglers do not involve themselves and criminally take advantage of unfortunate people,***" he added. **Toews** said the government hopes to quickly pass a bill titled the Preventing Human Smugglers from Abusing Canada's Immigration System Act. "***We urge our opposition parties here to support that legislation to ensure that we have the appropriate tools by which to deal with human smuggling and criminal operations,***" he said. Ottawa Citizen, A6 (Edmonton Journal, Times & Transcript, Vancouver Sun, Calgary Herald, National Post); Edmonton Sun (Winnipeg Sun, Toronto Sun, London Free Press, Calgary Sun)

Ministers scolded over prison transfers

Public Safety Minister Vic Toews and his two Conservative predecessors have been criticized in a recent Federal Court decision for repeatedly failing to provide adequate reasons when refusing to let Canadians jailed abroad be transferred to a prison in Canada. The ruling is the latest case to pit the government against judges who say the **public safety minister** has not used his discretionary powers in a transparent, reasonable way. In the latest court case, Mr. Justice Robert Barnes ruled on Jan. 19 that **Mr. Toews** didn't provide proper grounds to explain why he turned down a bid by Richard Goulet, a Quebec man serving time at a low-security penitentiary in Pennsylvania for smuggling marijuana. The judge noted that in 12 previous cases, **Mr. Toews** and his predecessors have failed to follow the requirement in the transfer of offenders act to justify their decision. The cases, starting in 2008, were decided by **Mr. Toews** and his predecessors Peter Van Loan and Stockwell Day. In several of those files, **the minister's** decision went against assessments by Correctional Service of Canada that the applicants were at a low risk of reoffending. Mr. Goulet, a bankrupt construction contractor who is serving a seven-year sentence, has no previous criminal record, and a Correctional Service Canada report given to **the minister** said the 42-year-old Quebecker is not likely to reoffend. **Mr. Toews's** decision wasn't reasonable because it was "a recitation of some of the relevant facts and a bare conclusion that ran contrary to the overwhelming weight of the evidence [in the CSC report]," the judge noted. He ordered **Mr. Toews** to review the case again and provide more thorough reasons if he rejects it. A **spokeswoman for Public Safety** Canada said the court's decision will be appealed. Globe and Mail, A5

Pro gun-registry reports suppressed
The NDP accused the government of suppressing RCMP reports on Canada's long-gun registry Tuesday, saying the government delayed releasing two reports because they clashed with Tory messaging on gun control. NDP justice critic Jack Harris raised the issue in question period Tuesday. **Public Safety Minister Vic Toews** told the House of Commons he released the report at the earliest opportunity. "***I understand that the report was provided by the RCMP to the Department of Public Safety on December 16***," he said. ***"It was then forwarded by the Department of Public Safety to my office on December 20 and we tabled it on the first available tabling date, as I understand it.***" Montreal Gazette, A11 (Times & Transcript); Waterloo Region Record (The Guardian)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Flood deal accepted**
On Monday the members of the Sakimay First Nation voted to accept the $21-million flood claim settlement. The Sakimay First Nations will receive $21,191,732 as part of a settlement agreement. The settlement and compensation were arrived at after lengthy negotiations between Sakimay and the federal and provincial governments. Leader-Post, A3

*** U.S. panel defends call to censor bird flu studies**
A potentially deadlier form of the bird flu virus poses one of the gravest known threats to humans and justifies an unprecedented call to censor the research that produced it, a top U.S. biosecurity official said on Tuesday. Whig-Standard, 13; The Guardian

*** H5N1**
Les magazines scientifiques Science et Nature publiaient hier les explications formulées par le Bureau national américain de la science pour la biosécurité (NSABB) qui recommande de censurer pour des raisons de sécurité deux articles scientifiques qui décrivent par le menu comment ont été créés des mutants de la souche H5N1 de la grippe aviaire, lesquels mutants seraient désormais capables de se transmettre entre mammifères, voire entre humains -- et de ce fait, feraient réapparaître le spectre d'une pandémie. Le Devoir, A2

*** L'influenza s'est rarement tenu aussi tranquille au Québec**
Même si le nombre de cas est en hausse depuis quelques jours, la saison de la grippe saisonnière a rarement été aussi calme au Québec. Le virus de l'influenza circule peu, c'est "exceptionnel", et il faut croire que la réponse immunitaire de la population est bonne, estime l'Institut national de santé publique du Québec (INSPQ). La Presse, A9 (Le Soleil, Le Quotidien)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** U.S. intelligence chiefs give mixed news**
Decapitation strikes killed Osama bin Laden and other top al-Qaeda leaders in the past year but new, even more dire threats loom - among them a nuclear-armed Iran or paralyzing cyber-attacks - President Barack Obama's top intelligence chiefs warned Tuesday. The killing of top al-Qaeda leaders marginalized the group's operational threat, said James Clapper, Director of National Intelligence. Globe and Mail, A6

*** Le Canada expulse deux diplomates russes**
Deux diplomates russes ont été renvoyés du Canada en lien avec une affaire d'espionnage impliquant un sous-lieutenant de la marine canadienne, a annoncé hier la chaîne de télévision CTV, citant des sources qu'elle n'a pas identifiées. L'un de ces diplomates, Dimitri Guerasimov, était en poste au consulat russe à Toronto, tandis que l'autre, Sergueï Joukov, était l'attaché militaire à l'ambassade à Ottawa, a indiqué le quotidien The Globe and Mail. La Presse, A19 (Journal Montreal)

*** THOSE WHO HATE CANADA**
A letter states, "It boggles my mind when we can have people who clearly hate the West, be it for its culture, religion, or even its democratic values, come to this country and call it home. They thrust their barbaric ideology, its sixth-century religious law and archaic cultural traditions on us, while spitting, disrespecting and devaluing Canada's own culture, history and religious background. From the Shafias who murdered their three female children and first wife over a false idea of honour. To Khadr, a misguided child soldier who clearly has the family background to prove his disdain and hatred for the West. My ultimate question to those people who hate Canada, the U.S and the West is: Why move to a country you clearly hate? I can sum it up to three reasons: 1) Better wages, 2) Free education, health care and social programs, 3) A lax justice system that usually favours the politically correct crowd. If you hate Canada and the West, please go back to your country of origin. Canada will be a better place." Ottawa Sun, 14

CYBER SECURITY / CYBERSÉCURITÉ

*** Kim Dotcom faces charges - Megaupload founder facing extradition**
In a New Zealand jail awaiting extradition to the U.S. on charges of racketeering, money-laundering and copyright crimes, (Kim) Dotcom has found himself at the centre of a high-stakes battle over Internet freedom versus copyright protection. It is a fight touching institutions from Congress to Silicon Valley and pitting the recording industry against some hip-hop artists who see Megaupload as a way to bypass record-label middlemen. In the days after Dotcom's arrest, the case has triggered an angry response from the hacker group Anonymous, which began an attack that briefly shut down websites, including the Justice Department, FBI, Universal Music and others. Vancouver Province, A28 (Calgary Herald)

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

RCMP commissioner asserts his independence
RCMP Commissioner Bob Paulson is backtracking on his call for MPs and senators to go through the Department of Public Safety to hold a meeting with him, saying he will safeguard his independence from the rest of government "like a terrier." Commissioner Paulson told a parliamentary committee on Tuesday he intends to give notice to his political bosses only about meetings that might be of interest to them, such as with diplomats or politicians. He added that he has no obligation to debrief the government after he meets with RCMP outsiders. Regarding an e-mail in which he recently called on Liberal Senator Colin Kenny to "route" his request through **Public Safety**, Commissioner Paulson suggested that it was a polite brush-off. Globe and Mail, A4; Windsor Star

Dead wrong on guns
An opinion piece states, "Matt Gurney is dead wrong when he states that the gun registry has no statistical connection to the decline in Canada's suicide rate. I suggest he read the 2008 Master's thesis of Marie-Pier Gagné on this specific subject. Controlling for virtually every factor imaginable, it clearly demonstrated that the registry could be clearly shown to have reduced firearm related-suicide deaths by 250 per/100,000 population each and every year..." National Post, A11

Bring back the right to self-defence
An opinion piece states, "On Monday, Ian Thomson of Port Colborne, Ont., went on trial on two charges of unsafe storage of a firearm, relating to a well-publicized self-defence incident...Four men were later arrested and charged with arson (yet not, strangely, for attempted murder or assault with a deadly weapon) for the attack, thought to be related to a long-running property dispute between Mr. Thomson and his neighbour. But Mr. Thomson himself was then arrested and charged with the counts of unsafe storage of a firearm, as well as unsafe use of a firearm and pointing a firearm...The federal government, in part due to public outcry relating to Mr. Thomson's case and other similar stories, has promised to review the myriad laws that serve to make self-defence cases so complex and difficult...Mr. Thomson has already been a victim of one attack. The government has no business now subjecting him to an assault upon his liberty." National Post, A10

Red Deer man's death linked to 'bad' ecstasy

A 38-year-old man from Red Deer died last month after taking ecstasy that may have contained a chemical linked to other deaths in Alberta and British Columbia, police say. The man was taken to hospital on Dec. 10 after he took what was believed to be ecstasy, RCMP said in a news release. Preliminary toxicology results from the medical examiner's office show that the dominant drug in the man's body was paramethoxymethamphet-amine (PMMA), a chemical linked to the deaths of at least six people in Calgary who took ecstasy before they died. Police said the final results from the autopsy are not yet available. It is not known where the man purchased the ecstasy, said Cpl. Kathe Deheer with the Red Deer RCMP. Edmonton Journal, A5; * Calgary Sun * Calgary Sun; * Calgary Herald; * Times & Transcript; * Yellowknifer; * Red Deer Advocate; * Edmonton Sun; * Edmonton Sun

Gangs catch eye of cops
A spike in the number of shootings in the city has police extending a crackdown on gun violence in Ottawa. Extra officers assigned to help the police's guns and gangs unit investigate a surge in gunplay across the city in recent weeks was supposed to end on Tuesday. But with six shootings and three stabbings (not counting a homicide) since the start of January, the 60-day campaign is being extended another 30 days, until March 1. Ottawa Sun, 11

*** Keep meetings in committee**
A letter to the editor states, “Senator Colin Kenny's point that only about two dozen parliamentarians "have expressed serious interest in security issues," is in itself reason enough to deny him a meeting with the RCMP commissioner. If we run a democratically elected government, which we do, then I submit that parliamentary committees should be where and when the RCMP commissioner meets and not with individual members of the Commons or Senate…” Toronto Star, A24

*** Report slams Mounties' treatment of suspect**
The RCMP watchdog is blasting cops in B.C. for "excessive" use of Tasers on a suspect in custody who later died. Seven officers from the Prince George RCMP were involved in the arrest and transport of Clay Alvin Willey on July 21, 2003. Willey was pepper-sprayed, punched, kicked, hog-tied, dragged face-down across a concrete floor and stun-gunned by two officers simultaneously. The Commission for Public Complaints Against the RCMP found that the use of force by constables John Graham, Holly Fowler and Kevin Rutten during the initial arrest -- including the pepper- spraying and hog-tying -- was "reasonable under the circumstances." Edmonton Sun, 26 (London Free Press); Toronto Star; The Province; Times Colonist

*** Ex-Mountie accused in theft**
RCMP in Cranbrook have charged a former Mountie with theft under $5,000 after a seized laptop went missing. At a press conference Tuesday in the B.C. town, about 390 km southwest of Calgary, Supt. Mike Sekela said the former member -- then a constable -- was suspended from duty in October when the investigation was launched and he resigned in December. The investigation stemmed from a complaint in October made by a pawn shop owner who called police asking for the return of a laptop seized by the former officer. Calgary Sun, 16

*** Mountie latest to call photo radar mere cash grab**
A retired Mountie vows he won't set foot in Winnipeg again until he has to show up for his day in court to fight two traffic tickets totalling $600 -- fines he claims go more to pad Mayor Sam Katz's pledge to freeze property taxes than road safety. Arborg resident David Sigvaldason, who served 12 years with the RCMP in British Columbia before setting up a business in the Interlake town, also said the city's ongoing debate about photo radar and police speed traps is a black eye for the city. Winnipeg Free Press, A4

*** Le registre des armes à feu n'est pas la solution**
Un piece d'opinion déclare, « Je suis une mère de famille, propriétaire d'une arme à feu, tireuse sportive, chasseuse, diplômée du CÉGEP, j'ai un bon travail et, surtout, je suis une personne respectueuse des lois. Je suis celle qui prône la tolérance et la non-violence. Je compatis et suis sensible à la douleur des victimes de violence et leurs familles…Commençons par le plus simple : le coût. Les partis d'oppositions et autres groupes de défense du registre des armes à feu répètent sans cesse que le coût du registre est marginal, soit environ 2 à 4 millions par année…J'aimerais que les gens fassent preuve de professionnalisme et soient critiques face à l'information véhiculée, quitte à la vérifier par eux-mêmes. Faites votre propre analyse objective des faits même si je sais bien que ce n'est pas le point fort de notre société. J'espère juste que d'ici là cesseront la désinformation et les campagnes de peur et que je pourrai continuer à pratiquer le tir, sport qui après tout est assez noble pour être aux Olympiques. » La Tribune, 17

*** Seized pot plants worth $416K**
Winnipeg police seized $416,000 worth of marijuana plants in a bust Sunday night. They raided a home in the 400-block of Agnes Street around 8:30 p.m. Jan. 29, seizing 372 pot plants and $10,000 in grow op equipment. No arrests were made in the bust. Winnipeg Sun, 13

*** Civilian oversight of police a must**

The continuing fall-out over the violent arrest of Adam Nobody during the G20 raises serious doubts about the adequacy of civilian oversight of the police. Eighteen months later, one officer, Const. Babak Andalib-Goortani, has been charged criminally with assault by the province's Special Investigations Unit (SIU). Another provincial body, the Office of the Independent Police Review Director (OIPRD) has recommended Andalib-Goortani and four others--Constables Michael Adams, David Donaldson, Geoffrey Fardell and Oliver Simpson, face disciplinary charges. Toronto Sun, 20

*** B.C. Mountie suing RCMP legal-aid society**
A B.C. Mountie who is suing the RCMP over a series of alleged sexual assaults at the hands of a male colleague has filed a new lawsuit. Karen Katz is taking a society that funds legal aid for Mounties to small claims court for failing to help her in her sexual-assault suit in B.C. Supreme Court. In the new writ filed in small claims court, Katz, a Mountie since 1988, says that since 1998 she has been a member of the Mounted Police Members Legal Fund, a registered society that boasts nearly 17,000 members. The Province, A12

*** Changes for Crown prosecutors in rural areas**
A recent organizational change involving Crown prosecutors who work in rural communities around Calgary should help enhance the working relationship with RCMP officers, say officials. Under the newly created Calgary Rural and Regional Response Office prosecutions branch, prosecutors in rural areas, what is called the "circuit unit," are now permanently assigned to the district courts. Calgary Herald, B2

*** CMP dog taken out of service after mauling**
An RCMP dog handler has been placed on administrative duty and his dog taken out of service while an investigation into a mauling of a North Surrey teen is undertaken. Police were called to a break-in at a gas station in the area of the 14900-block 108th Avenue in Surrey at 2 a.m. on Saturday. A few dozen energy drinks were allegedly stolen. The handler, who has 8½ years of experience in the RCMP and 16 months of experience as a handler, was able to track a suspect. The Province, A4; The Guardian

*** Penhold gains satellite RCMP office**
Innisfail detachment has 10 officers, a schools resource officer and two corporals. A vacant staff sergeant position has not yet been filled. A corporal and four officers are responsible for rural areas, but Penhold is regularly patrolled by any officers available. The Town of Penhold is making space for an RCMP satellite office. In a move to save residents the drive to the Innisfail detachment for minor police business, Penhold is donating office space at the multiplex for a part-time RCMP office. Red Deer Advocate, C2

*** Saisie de chandails du Canadien**
Les policiers de la Gendarmerie royale du Canada (GRC) ont saisi près de 1 000 articles de mode contrefaits, dont des imitations de chandails officiels du Canadien de Montréal et des anciens Nordiques de Québec, hier avant-midi, dans un commerce de Rivière-du-Loup, dans le Bas-Saint-Laurent. Journal de Montréal, 18

*** Crown surprises defence with take on gun law**
Canada's laws on the storage and handling of guns and ammunition are so complicated that a veteran judge needed to adjourn court to allow two experienced lawyers more time for legal arguments and a search of case law to help parse and dissect them. It was a dud of an ending after two days of trial in the case of Ian Thomson, a 54-year-old Port Colborne man who fired three shots from a legally owned gun to scare off three masked men who were firebombing his secluded farmhouse while one threatened: "Are you ready to die?" National Post, A5

*** Québec suggère une médiation**
Le gouvernement du Québec veut nommer l'ex-juge Louise Otis comme médiatrice auprès des Hurons-Wendat et des Innus de Mashteuiatsh, qui se disputent la réserve faunique des Laurentides. Les premiers sont d'accord, les seconds posent leurs conditions. Le ministre responsable des Affaires autochtones, Geoffrey Kelley, a lu le rapport du juge à la retraite John Gomery sur les accrochages entre les deux nations pendant la saison de chasse à l'orignal. Bien qu'il juge "ordinaire" que M. Gomery ait distribué des blâmes au gouvernement provincial et au fédéral aussi sans avoir recueilli sa version des faits, le ministre s'est servi des conclusions pour demander aux chefs impliqués de baisser le ton. Le Quotidien, 4

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Officer 'grief-stricken' over probe delay
Wracked by personal grief and disillusioned by a loss of confidence in the Vancouver Police Department and RCMP, Vancouver police Det. Const. Lori Shenher broke down on the stand at the Missing Women's Commission of Inquiry on Tuesday. Shenher's two days of testimony painted a very grim picture of policing in the Lower Mainland, suggesting badly

flawed efforts by the VPD and RCMP, which possibly allowed drug-addicted prostitutes to die needlessly. Leader-Post, A7 (Starphoenix, The Province, Times Colonist, Starphoenix); Globe and Mail; National Post; Windsor Star; * Vancouver Sun; * Waterloo Region Record (Red Deer Advocate, Whitehorse Star)

*** A killer in plain sight**
An editorial states, "The heartbreak just never ends for family and friends of Robert Pickton's murder victims. This week Vancouver Police Det. Const. Lori Shenher provided some of the most graphic testimony yet that police had Pickton squarely in their sights as a potential serial killer for years before he was finally charged...Victims' families deserve the truth, however painful. And the public needs to know that police have learned the appropriate lessons." Toronto Star, A24

*** World-class incompetence**
An opinion piece states, "For revelations of incompetence, ineptitude and sheer professional bumbling, it would be difficult to top the details emerging from the inquiry into police handling of the Robert Pickton case. The evidence says it all, and it is coming from the mouths of the very people who handled the case. Detective-Constable Lori Shenher says she realized quickly that Pickton was probably the serial killer who was murdering Vancouver area women when she got involved in the case in the summer of 1998. "I thought, 'Bingo, this is the kind of guy we're looking for,' " she told the inquiry on Monday...It doesn't require "the benefit of hindsight, and when measured against today's current investigative standards and practices," to appreciate how appallingly police mishandled virtually every aspect of the Pickton murders. As ineptitude goes, this was world class. It should be matched by an equal level of shame on the part of police, but so far there's no sign it is." National Post, A12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** Human trafficking haven seeks funds**
Red Deer may soon be home to a safe haven for victims of human trafficking in Canada. The doors could be open as early as September, should funding come through in the next federal budget or other avenues, says David Bouchard, president of the city's Magdalene House Society. Human trafficking is the illegal trade of human beings for slavery, sexual exploitation or forced labour. Red Deer Advocate, C2

*** Seize ans de prison pour contrebande de comprimés d'ecstasy**
Une Canadienne qui s'est fait prendre à tenter d'entrer aux États-Unis avec plus de 70 000 comprimés d'ecstasy a été condamnée lundi à près de 16 ans d'emprisonnement. La Montréalaise Tara Haynes, 34 ans, a été reconnue coupable en août de contrebande de comprimés d'une substance contrôlée. Le Soleil, 11 (L'Acadie Nouvelle)

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Province touts tuition squeeze
Ontario's post-secondary education minister took the feds to task Tuesday, as he promoted a new initiative to trim students' tuition. "I would love to see a national education and training strategy under the federal government," said Glen Murray during a press conference at Algonquin College. "I wish they paid as much attention to this as they did to prisons." Murray said the federal government could make a big difference to students if the $10 billion it put into prisons was invested in education instead. Ottawa Sun, 8

*** Feces, urine attacks against guards on rise**
Guards at B.C. jails say they are increasingly being targeted in a new kind of attack - where inmates are throwing feces and urine at them. Vancouver Sun, A6

*** Police 'Whitewash' stats, study says**
The majority of Canadian police forces are "whitewashing" crime statistics by refusing to provide information about the race of people they come into contact with, says a new report by two Ontario criminologists. Toronto Star, A8

*** Woman who chopped up roommate to appear before National Parole Board**
A Calgary woman convicted of chopping her roommate to death with an axe and concealing dismembered body parts in boxes is going before the National Parole Board today. Calgary Herald, B1

*** High-risk sex offender coming to 'Peg: cops**

Police are warning that convicted sex offender Brett Russell Jeffrey Pilch, 46, is being released from prison and moving to Winnipeg. Pilch has a history of sexually harassing women he doesn't know, police say. Females are also at risk of possible physical sexual violence. Winnipeg Sun, 14

*** No parole for 17 years for beating boss to death**
Parole ineligibility was set at 17 years Tuesday for a young Kitchener man who beat his boss to death as he slept more than four years ago. Cory-James Kaufmann, 23, pleaded guilty last November to second-degree murder in the death of Ray Wechzelberger, 59, in September, 2007. He was automatically sentenced to life in prison. At his sentencing hearing, Justice Steve Glithero decided he cannot apply for parole for 17 years from the date of his arrest, which would be in 12 years and eight months. The Record, B1

*** Report cites web of deceit, scant signs of remorse**
Ian Thow's history of deceit, lack of remorse and an inadequate plan for life after prison combined to keep the former investment adviser behind bars for at least another year, according to a National Parole Board report. Times Colonist, A1

*** ROPE squad tracks offender to Six Nations**
A federal offender, wanted on a Canada-wide warrant for breaching his parole, has been located by police on Six Nations. Nicholas Hill, 25, was arrested around 1 p.m. Tuesday by the Repeat Offender Parole Enforcement (ROPE) Squad. Hamilton Spectator, A2

*** Crime 'fix' primitive, pointless**
An opinion piece states, "Governing based solely on perceptions of public sentiment is a little like playing chess with yourself: You can never actually win without also losing... Statistics Canada continues to report that overall rate of offence is 17 per cent lower than it was a decade ago, a finding that recently moved Steve Sullivan, executive director of Ottawa Victims Services, to suggest that "if the government is telling taxpayers it is going to spend millions and billions of dollars on getting tough on crime, I think it at least has to have some evidence that it is addressing a real problem. Neither these statistics nor the other surveys we have would suggest that we are in some kind of crime wave." And yet, at a time when the feds are looking for billions of dollars in spending cuts (and will likely find them by laying off thousands of public employees and tinkering with old age security), the budget for Correctional Service of Canada is expected to jump to $3.1 billion by 2013, or roughly 90 per cent since 2006..." Times & Transcript, D6

PUBLIC SERVICE / FONCTION PUBLIQUE

Pension row could be diversion
It might just be my overly suspicious nature, but has anyone else considered that Prime Minister Stephen Harper's so-called assault on public pensions is really about something else? The StarPhoenix, A10

*** PMO staff salaries sought**
The federal NDP is calling on Treasury Board president Tony Clement to bring the same light to salaries in the Prime Minister's Office as the government shone on the highly paid staff at the CBC. The government on Monday introduced a written response to a written question from an MP who asked for salary details of top CBC executives and on-air staff. The response indicated more than 700 CBC staff earn $100,000-plus annually, though it did not provide the names MP Brent Rathbeger had asked for before Christmas. He also had asked for the pay levels of CBC newscaster Peter Mansbridge and host George Stroumboulopoulos, but those were not provided. Clement declined to give the total number of $100,000-plus salaries in the PMO. Victoria Times-Colonist, A8 (Ottawa Citizen); Toronto Sun (Winnipeg Sun; London Free Press; Ottawa Sun; Edmonton Sun)I; National Post

*** Tories won't commit to MP pension cuts - All spending will be reviewed, government says**
The federal Conservative government won't commit to scaling back lucrative pensions for MPs, as it searches for billions of dollars in cuts to federal programs and considers overhauling Old Age Security. Federal politicians of all stripes are under increasing pressure to take a haircut on what spending watchdogs call a "goldplated" pension plan, especially as government reins in expenditures to help eliminate a $31-billion deficit by 2015-16. The final decision on politicians' pensions falls with Treasury Board president Tony Clement, who said Tuesday all spending - including pensions for MPs - will be examined. But the government refuses to commit to cutting pension benefits for parliamentarians. Victoria Times-Colonist, B4 (Calgary Herald; Fredericton Daily Gleaner; Moncton Times and Transcript; Winnipeg Free Press)

*** Reform MPs' pensions first**
An opinion piece states "It might be understandable if a number of Canadians didn't appreciate Prime Minister Stephen Harper talking recently about reforming public sector pensions and Old Age Security (OAS) social assistance payments. After all, nobody likes the idea of their retirement plans changing, whether it is by way of a downturn in the market or a

change in a government policy. This is likely especially true recently, with Harper's musings coming on the heels of two reports on MP pensions, one by the not-for-profit Canadian Taxpayers Federation and the other from the esteemed C.D. Howe Institute. What these reports made abundantly clear is, Harper must reform MPs' pensions first, if he has any hope of looking at anyone else's. Canadians have been phoning, writing, and emailing their politicians in huge numbers, letting them know how they feel about platinum-plated MP pensions. With the next federal budget coming soon, taxpayers need to turn up the heat, and make sure the pork-laden MP pension plan is put on the chopping block, front and centre, with a big carving knife close at hand for Harper. It's the necessary first step in long, but ultimately needed, process." Waterloo Region-Record, A7

*** CBC mum on who's paid what**
The CBC pays 730 staffers more than $100,000 in salary per year, but won't say who they are. "Their salary information is also protected in accordance with the federal Privacy Act," wrote Heritage Minister James Moore in response to written questions in the House of Commons. When the Tory MP tabled his CBC questions, the NDP countered with a question about salaries of staffers in the Prime Minister's Office. Treasury Board president Tony Clement responded that PMO pay is comparable to the public service. Edmonton Sun, 28 (Ottawa Sun, London Free Press, Winnipeg Sun)

*** Arbitration awards hit taxpayers hard**
The key to Premier Dalton McGuinty's success in getting re-elected three times is this: He takes the line of least resistance. The best example is the way the government's dealt with public sector union pay demands. Ottawa Sun, 15 (Toronto Sun)

*** Canadians need pensions like their public servants**
A letter states, "Barbara Yaffe does a great disservice rolling together her criticism of MP and public service pensions. As her own figures show, members of Parliament contribute four per cent toward their plan while public servants contribute 35 per cent. Further, the government has raised public employee contributions to bring their share up to 40 per cent by 2013..." Vancouver Sun, A10

INTERNATIONAL / INTERNATIONAL

*** Man relocated to United States now facing terrorism charge**
A man from Uzbekistan whom the United States and the United Nations helped relocate to the Western U.S. state of Colorado was arrested Jan. 21 and now faces a terrorism charge. Jamshid Muhtorov opposed his home country's dictator following a 2005 massacre, endured a brutal detention, and saw his sister arrested on a false murder charge. The Record, A4

*** Iran has means to build bomb, but hasn't decided to do so yet, say U.S. intelligence officials**
Top U.S. intelligence officials on Tuesday asserted that Iran has the means to build a nuclear weapon but has not yet decided to follow through, in contrast to Israel's insistence that time is running out to stop Iran from developing such a weapon. Red Deer Advocate, D5

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-30-12 8:10 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; ; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; Houston, Laura; Jones, Scott; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 30, 2012 / le 30 janvier 2012

Online Media

Dutch DigiD vulnerable to DDoS attacks – NCSC
The Dutch National Cyber Security Center (NCSC) has warned that the ICT servers of the minister of interior could be vulnerable, with DigiD open to DdoS attacks. Logius is set to upgrade their server environment on 6 February. The Dutch Govcert (Government Computer Emergency Response Team) merged on 1 January with the National Cyber Security Center (NCSC). Telecom Paper

Anonymous : les cyberactivistes vont-ils faire leur coming-out en France ?
Comment qualifier Anonymous ? Exercice difficile. Les contours sont flous. « Ce n'est pas un mouvement de pirates. Pas non plus du hacking d'amateurs (terme qu'ils refusent) », considère Jean-Philippe Bichard, journaliste, expert en sécurité IT (ex-Kaspersky) et animateur du blogAttypique.com. « Anonymous appartient au 5% de cyber-attaquants que l'on peut qualifier « d'idéologique » par opposition au 95% de cyber hacker qui recherchent l'appât du gain. » Globalement, la communauté Anonymous considère qu'il ne faut pas attaquer les sites médias et les réseaux sociaux (Facebook, Twitter...). Mais vaut mieux se méfier de ses amis... IT Espresso

A new initiative to tackle cyber threats launched at WEF

Davos: A new initiative on cyber security has been launched at the World Economic Forum to strengthen efforts to combat rising cyber risks. The initiative 'Partnering for Cyber Resilience' is a set of shared principles, endorsed by chief executives of firms that recognise interdependence of organisations in tackling cyber risks, according to a statement from the WEF. The new programme would engage the corporate firms into working towards a safer digital environment. IBN Live (India)

La Freebox victime d'un cheval de Troie
Les utilisateurs de Freebox sont la cible d'un virus malveillant dont on ignore pour l'instant comment il réussit à pénétrer les systèmes de protection. Prudence ! La firme Trusteer, spécialisée en sécurité informatique a prévenu les utilisateurs de Freebox contre le cheval de Troie (trojan) Carberp, capable de subtiliser des coordonnées bancaires. Le malware a recours à la méthode via la méthode transparente du "man in the browser". MaxiSciences

Cybersecurity efforts trigger privacy concerns
The federal government's plan to expand computer security protections into critical parts of private industry is raising concerns that the move will threaten Americans' civil liberties. In a report for release Friday, The Constitution Project warns that as the Obama administration partners more with the energy, financial, communications and health care industries to monitor and protect networks, sensitive personal information of people who work for or communicate with those companies could be improperly or inadvertently disclosed. While the government may have good intentions, it "runs the risk of establishing a program akin to wiretapping all network users' communications," the nonpartisan legal think tank says. The Associated Press obtained a copy of the report in advance. Associated Press (link to KVAL)

Call for cyberwar 'peacekeepers' force
The US Army's Cyber Command is recruiting. Its mission? To create "a world class cyberwarrior force", and to develop cyberspace as an "active domain". That's according to Lieutenant General Rhett Hernandez, Arcyber commander, speaking at a London conference on cyber defence this week. He spoke of the explosive complexity of living in a digital age, and a cyber threat that was "growing, evolving and sophisticated". BBC News

Des mises à jour dangereuses sur Androïd...
Un virus de type cheval de Troie identifié par Bitdefender sous le nom d'Android.Trojan.FakeUpdates.A s'attaque aux systèmes Android via des versions alternatives de la plate-forme de téléchargement Android Market... Ce virus, caché dans une application validée comme saine, s'installe sur le système du GSM de la personne qui a téléchargé ce programme. Lors de l'installation, une dizaines d'autorisations sont demandées et les utilisateurs les moins attentifs ouvrent la sécurité de leurs appareils sans se rendre compte du danger. Cette méthode de piratage n'est pas nouvelle mais semble être de plus en plus fréquente. Next51.net

Android.Counterclank Found in Official Android Market
Symantec has identified multiple publisher IDs on the Android Market that are being used to push out Android.Counterclank. This is a minor modification of Android.Tonclank, a bot-like threat that can receive commands to carry out certain actions, as well as steal information from the device. For each of these malicious applications, the malicious code has been grafted on to the main application in a package called “apperhand”. When the package is executed, a service with the same name may be seen running on a compromised device. Another sign of an infection is the presence of the Search icon above on the home screen. The combined download figures of all the malicious apps indicate that Android.Counterclank has the highest distribution of any malware identified so far this year. Symantec.com

Chinese Hackers Led Western Attacks, Symantec Charges
Researchers with Symantec have uncovered additional clues that point to Chinese hacker involvement in attacks against a large number of Western companies, including major U.S. defense contractors. The attacks use malicious PDF documents that exploit an Adobe Reader bug patched last month to infect Windows PCs with "Sykipot," a general-purpose backdoor Trojan horse. According to findings published Thursday by Symantec's research team, a "staging server" used by the attackers is based in the Beijing area, and is hosted by one of the country's largest Internet service providers, or ISPs. Symantec did not identify the ISP. PC World

Accused Kelihos botnet controller protests his innocence
A Russian programmer accused by Microsoft of being behind the Kelihos botnet has protested his innocence. Last week, Microsoft accused Andrey Sabelnikov of being responsible for the operations of the Kelihos botnet, saying that he had written the code for, and either created or participated in creating, the malware; it also claimed that he registered more than 3,700 'cz.cc' sub-domains, which were used to control and operate the botnet. It was also revealed that Sabelnikov had worked as a software engineer and project manager at Russian anti-virus firm Agnitum, a provider of firewalls, anti-virus and security software. Sabelnikov said that upon arriving in the US on 21 January, he learned from the press that he was accused of a felony in connection with the activities of a botnet. In a statement, Sabelnikov said: “I am a programmer with nine years' experience, graduated from St. Petersburg State University of Aerospace Instrumentation in 2003, [and

have worked] in the highly respected Russian and international IT companies. "I did not commit this crime, have never participated in the management of botnets or any other similar programs, and especially not extracted from it any benefit."
SC Magazine

Android malware makes use of steganography
Security firm F-Secure have released details on how Android malware makes use of steganography to hide the control parameters for rogue code. First, what is steganography? It's the technique of hiding messages within something else, in this case, an icon file. F-Secure first suspected that Android malware was making use of steganography when researchers came across this line of code:

```
localObject2 = ((ByteArrayOutputStream)localObject2).toByteArray();
int k = paramInt + (-4 + new String(localObject2).indexOf("tEXt"));
if (k < 0)
  throw new IOException("Chank tEXt not found in png");
```

ZDNet

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-28-12 9:09 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - First Part / Première partie

Daily Media Summary / Revue de presse quotidienne
First Part / Première partie
January 28, 2012 / le 28 janvier 2012

MINISTER / MINISTRE

Fredricton's gun registry extends to Nerf toys

The looming end to the federal long-gun registry will soon leave Fredericton in a unique position: the only major Canadian city with a municipal gun registry. Except that its registry covers anything that shoots a projectile by means of compressed air, spring or mechanical means. That covers pellet and paintball guns and, in theory, even such toys as Nerf guns. Since 2005, Fredericton has maintained Canada's only mandatory registry regime for such items, complete with fees, fines, databases and, in one instance, a SWAT team raid on a home. But it could also represent the wave of the future, as **Public Safety Minister Vic Toews** says municipalities have full freedom to implement registries of their own - whether for real guns or fake ones. The Guardian, A7 (Vancouver Sun, Calgary Herald, Edmonton Journal, Telegraph-Journal, Times & Transcript, Montreal Gazette, Leader-Post, Ottawa Citizen)

Province ranks highest for fear of crime

Canadians are more likely to believe crime is going down now than they were a year ago, a new poll reveals. Except if they live in Manitoba. While fewer than half of Canadians believe crime is getting worse, more than two-thirds of Manitobans believe it is. That is by far the highest number of any province. Manitoba is also the only province to show a significant increase in the number of people who think crime is getting worse. Almost every other province showed a decrease in that number . . . **Public Safety Minister Vic Toews** said the Environics survey results are consistent with the Harper government's crime strategy. ***"I'm glad that people are beginning to feel safer. That's exactly what we want to see. But that doesn't mean that we should in any way take our foot off the gas. It's a lot like saying to a patient who's been taking a course of medicine that, 'Gee, you're feeling better now. Get off the medicine.' You keep on with the medicine until the problem is in fact cured."*** Winnipeg Free Press, A4

'Scourge' takes its toll

RCMP are trying to tackle what they call a "disturbing trend" surrounding elaborate marijuana grow operations in Manitoba, after last year seizing enough pot plants to almost cover a football field . . . Federal Public Safety Minister Vic Toews said the ***"scourge of drugs"*** takes a ***"huge toll ... on our families."*** Winnipeg Sun, 4; Winnipeg Free Press

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Seniors may be prone to new swine flu virus

There may be a lot more vulnerability in the population to a new swine influenza virus than was first thought, new Canadian research suggests. It has been believed that while children and teens are probably vulnerable to the new H3N2 variant, people over the age of 20 or so would have antibodies that would either block infection or protect against severe disease caused by the viruses. Hamilton Spectator, G8; Toronto Star

1663: séismes terrifiants

Un article d'opinion déclare, «...On se souvient par ailleurs de la catastrophe nucléaire survenue l'an dernier au Japon à la suite du tremblement de terre. Tous les pays civilisés ont remis en cause l'utilisation de l'énergie nucléaire suite à cette catastrophe. Enfin presque tous. Il reste au Québec et au Canada quelques irréductibles promoteurs de dangers publics... » Le Nouvelliste, 19

Green groups warn of deepwater drilling risks

Environmental groups are sounding the alarm that a new round of deepwater drilling off the coast of Nova Scotia could end in another natural disaster such as the Gulf Coast spill of 2010. The Ecology Action Centre and the Sierra Club are urging regulatory bodies to proceed with extreme caution and toughen up regulations before allowing drilling to go ahead. Chronicle-Herald, A1

Flood is not over, nor is the fight
An opinion piece states, "One senses that a general malaise has set in about the Lake Manitoba flood, that it is over and that the construction of the emergency channel has solved the problem. But it is far from over and the construction of the emergency channel has not solved the problem. It is only the beginning of a solution to the problem..." Winnipeg Free Press, J11

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Tories to Hamas: Stay home
Two federal ministers have put up a "not welcome" sign for members of Hamas, a banned terrorist group in Canada, who might attend an International Parliamentary Union (IPU) meeting in Quebec City. QMI Agency has obtained a letter that Foreign Affairs Minister John Baird and Immigration Minister Jason Kenney have sent to the speakers of the House of Commons and the Senate. Toronto Sun, 12

Spying on our own : secret files revealed
Canadian security forces kept close tabs on renowned constitutional scholar Eugene Forsey from his early days as a left-wing academic to his stint as a senator, according to newly declassified documents . . . The secret files kept on Forsey by the RCMP Security Service - the predecessor to the Canadian Security Intelligence Service (CSIS) - are public for the first time after the Star obtained them through an access-to-information request to Library and Archives Canada. Toronto Star, IN5

Naval centre one of 'Five Eyes' on the world
As you approach the Royal Canadian Navy's secretive Trinity intelligence centre near the Halifax Harbour, at least nine surveillance cameras track your movement. Protected behind two chain-link fences, both topped with barbed wire, the main Trinity facility is really a building within a building. A separate interior structure, with metal-clad walls, safeguards its secrets. Globe and Mail, A8

CYBER SECURITY / CYBERSÉCURITÉ

Beaucoup de profit à vous espionner
Tout ce que vous écrivez sur les sites de réseautage social et même en utilisant vos courriels gratuits est utilisé. Big Brother enregistre tout. Demain ou l'un de ces jours, vous risquez de recevoir de la publicité parce que vous aimez les chaussures anglaises ou le chocolat. Ou encore parce que vos amis et vos relations les aiment. Comment estce possible? Le Journal de Montreal, 50

What to do when hackers strike
If you do any shopping, banking or other business online and it hasn't happened to you yet, it probably will. In the U.S., the online retailer Zappos (which is owned by Amazon), recently sent an email to 24 million of its customers telling them that their personal information might have been compromised in a data breach. Though credit card and payment data were unaffected, the company said names, email addresses, billing and shipping information, phone numbers and other information were at risk. Edmonton Journal, C6

Hacker group targets new websites
The activist hacker group Anonymous attacked three Mexican government websites on Friday in protest at a proposed bill that seeks to toughen local laws about online file-sharing. The affected sites belong to the Interior Ministry, the Senate and the Chamber of Deputies. The homepage of the Interior Ministry remained offline by mid-afternoon. Kingston Whig-Standard, 14

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Victims of crime supported

The federal government announced more than $1.6 million in funding to support victims of crime in New Brunswick yesterday. The announcement was made by Robert Goguen, MP for Moncton-Riverview-Dieppe and Parliamentary secretary to Justice Minister Rob Nicholson, and Marie-Claude Blais, minister of justice and attorney general of New Brunswick, on behalf of Robert B. Trevors, minister of public safety and solicitor general of New Brunswick. Times & Transcript, A12

WCB hostage-taker on hunger strike, friend says
Patrick Clayton, the man convicted of taking nine hostages at the Workers' Compensation Board building in Edmonton in October 2009, is apparently on a hunger strike at the Drumheller Institution. Clayton, 40, has been held at the prison since late November, after he was sentenced to 11 years. Edmonton Journal, A4

La mort de Moïse Thériault vécue comme une «délivrance»
A travers douleur et déchirement, Gabrielle Lavallée a accueilli l'assassinat de Roch Moïse Thériault comme une «délivrance». Reste qu'elle s'interroge sur les circonstances de la mort de celui qui lui a infligé un calvaire, mettant de l'avant la thèse de la préméditation . . . «Moïse» Thériault, qui avait fait de Gabrielle Lavallée une de ses femmes au sein de sa secte, a été assassiné par un voisin de cellule à la prison de Dorchester, au Nouveau-Brunswick, le 26 février dernier. Le Soleil, 26

INTERNATIONAL / INTERNATIONAL

Londres se prépare au pire
A six mois des Jeux, une médaille devrait déjà être décernée aux organisateurs des XXXes Olympiades qui s'ouvriront à Londres le 27 juillet prochain. Les enceintes sportives sont pratiquement terminées et le budget, révisé à 14,6 milliards de dollars en 2007 (le triple de l'estimation initiale), a été respecté. Toutefois deux grands impondérables demeurent : le transport et, surtout, la sécurité des Jeux. A en croire le branle-bas de combat dans la capitale, les Londoniens se préparent au pire. La Presse, A26

The tale of an American militant
MOEED ABDUL Salam didn't descend into radical Islam for lack of other options. He grew up in a well-off Texas household, attended a pricey boarding school and graduated from one of the state's most respected universities. But the most unlikely thing about his recruitment was his family: Two generations had spent years promoting interfaith harmony and combating Muslim stereotypes in their hometown and even on national television. Chronicle-Herald, F4

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

s.16(2)(c)

Williston, Sandra

From: [redacted]
Sent: January-26-12 9:03 PM
To: [redacted]
Subject: CCRIC CF12-001 Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle

(English version previously sent)

==========
CCRIC – Bulletin cybernétique CF12-001
Date : 26 janvier 2012
==========

PUBLIC CIBLE
==========
Ce bulletin cybernétique est destiné aux professionnels et aux gestionnaires de la TI des gouvernements fédéral, provinciaux et territoriaux et des administrations municipales, ainsi que des industries à infrastructure critique et autres industries connexes.

Titre
====
Collectif d'hacktivistes Anonymous – Attaques par déni de service distribué (DSD) en rapport avec le droit d'auteur et la propriété intellectuelle.

Détails
=====
On a porté à l'attention du CCRIC une série d'attaques coordonnées par déni de service distribué (DSD) contre des cibles internationales, y compris des organisations gouvernementales et des entreprises du divertissement dont les efforts sont axés sur l'adoption de lois protégeant le droit d'auteur aux États-Unis, comme la Stop Online Piracy Act (SOPA) et la Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), ainsi que de l'Accord commercial relatif à la contrefaçon (ACRC).

Il appert qu'Anonymous, un collectif hétéroclite d'« hacktivistes », a annoncé que des attaques seraient portées en réponse à la fermeture de MegaUpload, un site d'hébergement et de partage de fichiers, et aux projets de loi sur le trafic de matériel protégé par le droit d'auteur et de marchandises contrefaites que s'apprêtent à adopter les États-Unis. Des attaques qu'ont signalé par la suite les médias visaient diverses organisations gouvernementales déjà engagées dans le processus de ratification de l'ACRC, à savoir les gouvernements d'Irlande et de Pologne.

Deux formes d'attaques DSD sont connues :
[redacted]

De l'information diffusée récemment sur le site Web Pastebin laisse entendre que des hacktivistes surveillent de près la position du Canada. Le gouvernement fédéral souhaite en effet amender la Loi sur le droit d'auteur avec son projet de loi C-11, la Loi sur la modernisation du droit d'auteur, encore à l'étude au Parlement.

[redacted]

Voici un échantillon du trafic généré par LOIC et entregistré dans les journaux d'un serveur Web :

[redacted]

Les sites ci-dessous apparaissent dans les en-têtes de référants HTTP du trafic suspect généré par LOIC. Il se peut que cette liste ne soit pas exhaustive. Évitez de visitez ces sites puisqu'ils sont suceptibles d'herberger encore à l'heure actuelle une machine zombie LOIC active ou un autre type de code malveillant.

[redacted]

Voici la liste des enregistrements de type A des sites référants au 20 janvier 2012 :

[redacted]

[redacted]

Atténuation
==========
Le CCRIC presse les organisations gouvernementales et les entreprises, qui participent de près à la modification de la Loi sur le droit d'auteur et dont les principales activités sont axées sur le matériel qu'elle protège, d'évaluer les risques d'être exposées à des attaques DSD, telles que les décrit le présent document, et de mettre en place les statégies d'atténuation nécessaires pour y faire face.

Différentes stratégies d'atténuation permettent de contrer ces attaques en fonction de leur type et de l'infrastructure de réseau ciblée. En règle générale, la meilleure défense consiste à s'y préparer à l'avance, ce que permet de faire la liste de contrôle suivante :

Préparation
****

1. Identifier les ressources matérielles les plus cruciales et les services dont elles assurent la prestation.
    - Les derniers correctifs ont-ils été installés?
    - Exécutent-elles des services inutiles comme Telnet, FTP, etc.?

2. De concert avec le fournisseur d'accès Internet (FAI), établir des procédures pour connaître l'étendue du soutien qu'il peut apporter à l'organisation lorsqu'elle fait l'objet d'une attaque DSD. Savoir s'il existe un accord sur les niveaux de services (ANS) et connaître les coûts à assumer.

3. Dresser la liste des personnes-ressources du FAI que l'on peut joindre en tout temps, ainsi que des autres moyens de communiquer avec elles.

4. Bloquer tout trafic qui présente des signes évidents d'usurpation d'identité (p. ex., les adresses IP à l'intérieur du réseau de l'organisation qui ne devraient pas être associées à du trafic entrant ou sortant). Instaurer une liste de filtrage Bogon (plage d'adresses non allouées) au périmètre du réseau.

5. Établir des procédures sur la façon de cloisonner les réseaux de l'organisation en cas d'attaque DSD. Se servir des appareils existants, comme les routeurs et les commutateurs gérés, pour s'en protéger. Dans la mesure du possible, configurer les routeurs du périmètre pour filtrer les services afin de réduire la chargeimposée aux dispositifs de sécurité, tels les pare-feu, qui analysent le trafic.

6. Désactiver tout service inutile et bloquer tout accès non autorisé vers et depuis les hôtes critiques identifiés précédemment.

7. Créer une liste blanche des adresses IP source s'il est nécessaire d'établir un trafic proritaire durant une attaque.

8. Documenter la topologie de réseau, y compris toutes les adresses IP. Tenir cette information à jour.

9. Passer en revue plan de continuité des opérations (PCO) de l'organisation et s'assurer que la haute direction et le service du contentieux comprennent bien ce qu'est une attaque DSD et les rôles et responsabilités qui leur sont dévolus.

10. Comprendre ce que constituent des conditions normales. Établir le niveau de référence du trafic sur le réseau, de la charge de travail imposée aux processeurs, de l'utilsiation des connexions et de la mémoire des hôtes essentiels en situation normale afin que les outils de surveillance du réseau entrent en œuvre lorsqu'une variation anormale se produit.

11. Reconnaître que l'organisation peut être attaquée. Solliciter la direction afin d'obtenir son approbation en vue d'élaborer et de mettre en œuvre des politiques, plans et procédures pour se défendre contre les attaques DSD. Identifier et obtenir les ressources nécessaires pour mettre en œuvre ces politiques, plans et procédures.

12. Attribuer les rôles et responsabilités. Connaître les intervenants dans la défense contre les attaques DSD et s'assurer qu'ils sont au fait de cette responsabilité. Ces personnes devraient appartenir au personnel affecté aux fonctions opérationnelles essentielles, aux opérations de TI, à la sécurité des réseaux et des TI, au service du contentieux et aux relations publiques. Tenir à jour la liste des points de contacts primaires et secondaires. Le réseau étant susceptible d'être en panne, y compris les appareils mobiles, mettre également en place d'autres mécanismes de communication.

13. Effectuer des exercices. Ce n'et plus le temps de faire l'essai des plans et des procédures lorsqu'une attaque se produit.

Identification
****

1. Savoir si l'orgaisation est une victime ciblée ou accidentelle.

2. Comprendre le déroulement logique de l'attaque.

3. Déterminer le trafic dont se sert l'attaquant en identifiant les adresses IP, les ports et les protocoles qu'il exploite.

4. Envisager de recourir à des outils d'analyse du réseau pour déterminer le type de trafic qu'exploite l'attaquant (p. ex., TcpDump, Wireshark, Snort)

5. Consulter les journaux disponibles du serveur pour comprendre la fonctionnement de l'attaque et les cibles visées.

6. Aviser le personnel concerné, notamment celui de la haute direction et du service du contentieux.

Confinement
****
1. Communiquer avec le FAI pour mettre en place un mécanisme de filtrage du trafic.

2. Bloquer le trafic le plus près possible du réseau en nuage (p. ex., avec un routeur, un pare-feu, un équilibreur de charges).

3. Changer l'adresse IP de l'hôte ciblé par l'attaque. Il s'agit là d'une solution provisoire.

4. Si l'attaque vise une application en particulier, envisager sa désactivation.

5. Identifier et corriger la vulnérabilité ou la faiblesse du système qui est exploitée. Il peut s'agir par exemple d'un service inutilisé maintenu involontairement en activité sur un dispositif destiné au public ou d'un système d'exploitation dont les correctifs n'ont pas été installés.

6. Mettre en place un mécanisme de filtrage en fonction des caractéritiques de l'attaque, par exemple le bocage des paquets IMCP Echo.

7. Limiter le trafic de certains protocoles à un nombre quelconque de paquets par seconde ou en n'autorisant l'accès des paquets qu'à certains hôtes.

Reprise des services
****
1. Confirmer que l'attaque DSD a pris fin et que les services sont de nouveau disponibles.

2. Confirmer que le niveau de performance de référence des réseaux est rétabli.

3. Au besoin, installer les correctifs et les mises à jour sur les machines touchées.

4. Dansla mesure du possible, identifier l'origine de l'attaque. Solliciter l'aide du FAI.

5. Passer en revue les registres de journalisation pour y repérer la trace des tentatives de reconnaissance. Conserver ces registres en vue d'éventuelles poursuites judiciaires.

Leçons retenues
****
Rédiger ou mettre à jour les documents suivants :

- Procédures d'opération normalisées
- Procédures d'opération d'urgence
- Plans de continuité des opérations

Consultez les références ci-dessous pour en apprendre davantage sur les activités du collectif Anonymous, l'outil LOIC servant aux attaques DSD, le projet de loi C-11 et le déni de service distribué.

Références :
http://www.us-cert.gov/current/index.html#anonymous_activities (en anglais) http://www.us-cert.gov/cas/tips/ST04-015.html (en anglais) http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html (en anglais) http://isc.incidents.org/diary/Javascript+DDoS+Tool+Analysis/12442 (en anglais) http://nakedsecurity.sophos.com/2012/01/20/anonymous-opmegaupload-ddos-attack/ (en anglais) http://www.channelregister.co.uk/2012/01/24/anon_attacks_poland_over_acta/ (en anglais) http://www.reuters.com/article/2012/01/25/ireland-web-attack-idUSL5E8CP1VU20120125 (en anglais) http://www.reuters.com/article/2012/01/23/idUS426379616120120123 (en anglais) http://www.michaelgeist.ca/ (en anglais) http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=fra&view=d (en français) http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5144516&file=4 (contenu bilingue)

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 avertir le destinataire de n'effectuer aucune activité de collecte de données hors du périmètre de son réseau selon les renseignements du présent bulletin cybernétique, notamment l'exploration, le téléchargement, le balayage, ou même une recherche Web selon tout texte du présent rapport.

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.

Centre des opérations du gouvernement/
Government Operations Centre
Courriel/email:

s.16(2)(c)

Williston, Sandra

From: [redacted]
Sent: January-26-12 2:17 PM
To: [redacted]
Subject: CCIRC CYBER FLASH CF12-001: Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property

(La version française suivra)

==========
CCIRC - Cyber Flash CF12-001
Date: 26 January 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
=====
Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property

Detail
======
CCIRC has received information about coordinated distributed denial-of-service (DDoS) attacks with multiple international targets including government and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

The loosely affiliated collective hacktivist group "Anonymous" allegedly promoted attacks in response to the shutdown of the file hosting site MegaUpload and in protest of proposed U.S. legislation concerning online trafficking of copyrighted intellectual property and counterfeit goods. Follow-on attacks reported in the media targeted various governments organizations involved in the ratification of ACTA, namely the governments of Ireland and Poland.

Two types of DDoS attacks were reported:

[redacted]

[redacted] suggests active monitoring of the Canadian position by the hacktivists. The update to Canada's Copyright Act is currently bill C-11 - Copyright Modernization Act, which is still in parliament.

[redacted]

The following is a reported sample of LOIC traffic recorded in a web server log:

The following sites have been identified in HTTP referrer headers of suspected LOIC traffic. This list may not be complete. Please do not visit any of the links as they may still host functioning LOIC or other malicious code.

The following are the A records for the referrer sites as of January, 20, 2012:

Mitigation
==========

s.16(2)(c)

CCIRC encourages government and industry organizations closely involved with the Copyright Law and copy-righted material to assess risk exposure to DDoS attack as described herein and implement mitigation strategies accordingly.

There are a number of mitigation strategies available for dealing with DDoS attacks, depending on the type of attack and the target network infrastructure. In general, the best practice defence for mitigating DDoS attacks involves advanced preparation. The following checklist may be used for this purpose:

Preparation
****

1. Identify your most critical assets and the services they provide.
    - Are they up to date with the latest patches?
    - Do they run any unnecessary services such as Telnet, FTP, etc.?

2. Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Knowledge of any Service Level Agreement (SLA) that exists and what costs may be incurred.

3. Establish 24/7 contact information for your ISP and alternate methods for communications.

4. Deny all obviously spoofed traffic (e.g., internal IP addresses that should not be coming in or going out of your network). Implement a bogon block list (unallocated address space) at the network boundary.

5. Establish procedures on how to segregate your networks in the event of a DDoS attack. Use existing network devices, such as routers and managed switches, to defend against DDoS attacks. Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.

6. Disable all unnecessary services and restrict all unauthorized access to and from all previously identified critical hosts.

7. Create a whitelist of the source IPs you must allow if you need to prioritize traffic during an attack.

8. Document your network topology including all IP addresses. Keep it up to date.

9. Review your Business Continuity Plan (BCP) and ensure senior management and legal team understand the significance of a DDoS attack, including their roles.

10. Understand "normal." Establish a baseline of network traffic, CPU usage, connection and memory utilization of critical hosts under normal conditions so that network monitoring tools will trigger on abnormal changes.

11. Acknowledge that your organization may be attacked. Seek and obtain management's approval for the development and implementation of policies, plans and procedures to defend against DDoS attacks. Identify and obtain resources to implement these plans.

12. Assign responsibility. Identify who plays a role in defending against a DDoS attack and ensure they are aware of this responsibility. This should include personnel from critical business functions, IT operations, network and IT security teams, legal advisors, and media relations staff. Ensure an up-to-date point-of-contact list with primary and alternate personnel is maintained. As the network may be unavailable, including mobile devices, ensure alternate communications mechanisms are in place.

13. Conduct exercises. The worst time to test plans and procedures is during an attack.

Identification
****

1. Determine if you are the target or a collateral victim.

2. Understand the logical flow of the attack.

3. Determine what type of traffic is being used, such as IP addresses, ports and protocols.

4. Consider using network analysis tools to determine the type of traffic being used in the attack (e.g., TcpDump, Wireshark, Snort)

5. Review any available logs to understand the attack and what is being targeted.

6. Notify appropriate personnel. This may include senior management and the legal team.

Containment
****

1. Contact your ISP provider to implement filtering.

2. Block the traffic as close to the network cloud as possible (e.g., router, firewall, load balancer)

3. Relocate the target to another IP address if a particular host is being targeted. This is a temporary solution.

4. If a particular application is being targeted, consider disabling it temporarily.

5. Identify and correct the vulnerability or weakness that is being exploited. An example of this may be an unused service that is accidently left enabled on a public-facing device or unpatched operating system.

6. Implement filtering based on the characteristics of the attack. An example may be blocking IMCP echo packets.

7. Implement rate limiting for certain protocols, allowing a certain number of packets per second for a specific protocol or to access a certain host.

Recovery
****

1. Confirm that the DDoS attack has finished and services are reachable again.

2. Confirm that your networks are back to your baseline performance.

3. If necessary, patch and update all affected machines.

4. If possible, identify the source of the attack. Enlist the help of your ISP.

5. Review logs for signs of reconnaissance. Maintain logs for possible future law enforcement requirements.

Lessons Learned
****

Create or update the following documents:

- Standard Operating Procedures
- Emergency Operating Procedures
- Business Continuity Plans

Please consult the references below for additional information on Anonymous activities, the DDoS tool LOIC, Bill C-11 and DDoS in general.

References:
http://www.us-cert.gov/current/index.html#anonymous_activities
http://www.us-cert.gov/cas/tips/ST04-015.html
http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html
http://isc.incidents.org/diary/Javascript+DDoS+Tool+Analysis/12442
http://nakedsecurity.sophos.com/2012/01/20/anonymous-opmegaupload-ddos-attack/
http://www.channelregister.co.uk/2012/01/24/anon_attacks_poland_over_acta/
http://www.reuters.com/article/2012/01/25/ireland-web-attack-idUSL5E8CP1VU20120125
http://www.reuters.com/article/2012/01/23/idUS426379616120120123
http://www.michaelgeist.ca/
http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=eng&view=d
http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5144516&file=4

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.

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:

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-26-12 8:31 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; Houston, Laura; Jones, Scott; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 26, 2012/ le 26 janvier 2012

Print Media

Software phone scam hooking Canadians
A scam where callers pretend to be Microsoft employees offering to solve computer problems now accounts for 70 per cent of all fraud complaints in Canada, reports the Canadian Anti-Fraud Centre. The fraud artists claim they are with Microsoft and offer to help people rid their computers of malicious software. Daily Gleaner, D1

Online Media

DHS disputes memo on purported railway computer breach
The Department of Homeland Security is disputing a government memo obtained by Nextgov.com that said a targeted attack on the computer network of a railway company in the Northwest disrupted train service in early December. CNET

Senators back Obama's call for cybersecurity reform
Senate Homeland Security Committee Chairman Joe Lieberman (I-Conn.) echoed President Obama's call in the State of the Union for Congress to pass comprehensive cybersecurity legislation on Tuesday evening. "The President's call for Congress to pass cybersecurity legislation underscores the pressing nature of securing the government's cyber systems

and networks — and a limited number of private sector networks that touch the lives of all Americans," Lieberman said. The Hill

Hackers attack Irish govt over new web law
Hackers attacked the websites of Ireland's departments of finance and justice on Wednesday in a protest against government plans to block websites that violate copyright laws. Officials said both websites were taken offline for a short time in the early hours of Wednesday in a denial of service attack, in which the sites were bombarded with a huge number of requests. Reuters

Understanding the threat
Many companies today make the mistake of viewing the advanced persistent threat (APT) type of attack as a single incident consisting of exploit, infection and remediation stages. However, APT attacks are now co-ordinated efforts to establish a foothold for the purposes of cyber crime, cyber espionage or emerging cyber warfare scenarios. CRN

56% of Brits don't check if public Wi-Fi is encrypted before logging on
More than half (56 percent) of Brits that use public Wi-Fi rarely check if it is encrypted before logging on, says UK2. Research conducted by the web hosting firm in conjunction with YouGov revealed more than two thirds (67 percent) did not know what VPN or Virtual Private Network means. However, 86 percent said they ensure their home Wi-Fi network is secure, indicating there is a discrepancy between ensuring safety when surfing the web from home and when on-the-go. PC Advisor

Sourcefire Uses Big Data Analytics To Stop Malware
Cyber security vendor Sourcefire's latest product uses big data analytics methods to search data to discover patterns in malware attacks and intervene to stop them. The release of FireAMP comes the same week that Cisco Systems released its 4Q11 Global Threat Report detailing how pervasive the malware threat is to organizations. Network Computing

Feds Issue Comprehensive Cloud Security Guidance
There's no silver bullet to ensuring security in the public cloud, but organizations need to take the reins and not leave security up to service providers and service arrangements, the National Institute of Standards and Technology (NIST) said in comprehensive new cloud security guidance. Information Week

ISF: consider a cyber resiliency response to protect against 'unknown unknowns'
Cyber resilience is a matter for the whole business to be involved with and not just the security team. At a presentation this week, Michael de Crespigny, CEO of the Information Security Forum (ISF), said that cyber security is not an information security issue, but a business issue. SC Magazine UK

Davos 2012: Alarming growth in cyber-attacks
Ian Powell, UK chairman and senior partner of PwC, said that the danger of cyber-attacks was little understood by many people at the top of business. "The alarming growth in cyber crime highlights the challenge that all global business leaders face. Although they might be aware of the threat they are not necessarily equipped to respond effectively," he told delegates at Davos. "After all, cyber [crime] is a global risk that knows no boundaries." The Telegraph

Microsoft researchers find new type of stealth malware
Security researchers have uncovered a new type of malware that appears to be benign as it is downloaded, potentially fooling security software, but which morphs into malicious software once it is on a user's computer. Researchers at Microsoft's Malware Protection Centre wrote about their findings this week, explaining that the code is surprising in that unlike most other similar types of malware, it doesn't attempt to download or inject an executable file into a host machine. Computing UK

Build Up Your Phone's Defenses Against Hackers
Chuck Bokath would be terrifying if he were not such a nice guy. A jovial senior engineer at the Georgia Tech Research Institute in Atlanta, Mr. Bokath can hack into your cellphone just by dialing the number. He can remotely listen to your calls, read your text messages, snap pictures with your phone's camera and track your movements around town — not to mention access the password to your online bank account. New York Times

Accused Kelihos botmaster's former employer 'angered' at revelation
A security-related company that until late December employed the Russian developer who allegedly created the Kelihos botnet said today it was "extremely disappointed and angered" at the revelation. Returnil, which sells the Virtual System Pro program, confirmed Wednesday that Andrey Sabelnikov had worked in its St. Petersburg office until Dec. 21, 2011. Network World

Apple malware became more sophisticated in 2011
Malware aimed at Macs is still insignificant compared to Windows but Apple users should to pay careful attention to the growing threat from social engineering attacks, a report has found. The Year in Mac Security by Apple security company Intego divides 2011 into two halves before and after the day, 2 May, when the fake antivirus scam Mac Defender was discovered. Tech World

Gingrich on international cyber espionage
Newt Gingrich, the current leader in the race for the Republican Party's nomination for US presidential candidate, has shared his thoughts on the matter of international cyber-espionage. In a December 9th interview with Coffee and Markets, Gingrich expressed his concern about hacking attacks, suggesting that "state-based covert activities" be treated with the same level of severity as acts of war and, further, that "we have to respond to that and create a level of pain which teaches people not to do it." Washington Post

Chinese Hackers Blamed For US Satellite Attack
A forthcoming report from a US Congressional commission reportedly blames cyber attackers for interfering with two government satellites several times over a two-year period. The intrusions on the satellite occurred four times in 2007 and 2008, according to a draft of a report from the US-China Economic and Security Review Commission obtained by Bloomberg BusinessWeek on 27 October. Tech Week Europe

Threatened by Anonymous, Symantec tells users to pull pcAnywhere's plug
Symantec this week took the highly unusual step of telling users of its pcAnywhere remote access software to disable or uninstall the software while it fixes an unknown number of bugs. Security experts said the move was unprecedented for a company of Symantec's size. Computerworld

Hackers launch fresh attacks on Israeli websites
Arab hackers claimed responsibility Wednesday for a series of attacks on prominent Israeli websites, including that of daily newspaper Haaretz. Cyber attacks against Israeli sites have been increasing since the start of the month, many of them claimed by Arab hackers. AFP

Israeli Hacker Steals 85,000 Arabs' Facebook Logins
An Israeli hacker calling himself Hannibal stole and exposed the Facebook login credentials of 85,000 Arabs earlier this week. It's the latest retaliatory strike in a politically motivated battle between Israeli and Arab hackers that's been going strong since the beginning of the month. MSNBC

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-25-12 8:17 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; Houston, Laura; Jones, Scott; Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Thomson, David; Turner.JM2 @forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 25, 2012/ le 25 janvier 2012

Print Media

Hackers target Coach website
Some visitors to Coach Inc.'s website Tuesday were directed to a hacker group's site that featured a drawing of Adolf Hitler, and the retailer said it has corrected most of the issues in the U.S. The hacker site said it targeted Coach, the largest U.S. luxury handbag maker, because it supports the Stop Online Piracy Act. Calgary Herald

Online Media

Anonymous: We Will Not Attack Facebook
Hackers' collective Anonymous clarified on Monday that it has no plans whatsoever to target Facebook on Jan 28 as reported by a section of the media. ITProPortal.com

Targeted attacks will change the economics of security
Today, European Justice Commissioner, Viviane Reding, will unveil the new European Privacy Directive, designed to safeguard personal, identifiable information that is stored by private and public sector organizations. "With the

increasingly stealthy tactics employed by cybercriminals and hacktivists, companies are going to be increasingly wary of untoward activity on servers, email and Web channels. We predict that the European directive will drive a new wave of awareness and innovation in information protection and cyber security," he added. Help Net Security

ISF launches guide to help businesses prepare for cyber attacks
The Information Security Forum (ISF), an independent information security body, has launched a report giving advice to businesses on how they can prepare their organisations for cyber threats. Cybercrime is now the third biggest crime problem experienced by UK businesses according to the 2011 PricewaterhouseCoopers (PwC) Global Economic Crime Survey. ComputerworldUK

Privacy commissioner offers parents tips for online privacy
Privacy commissioner Jennifer Stoddart has produced a video, a tip sheet for parents and a kit for teachers to help kids deal with online privacy threats. She says young people often don't think about privacy problems as they surf the net. The material is aimed at children in Grade 7 and Grade 8. The online video looks at some of the privacy pitfalls associated with the web. The tip sheet offers parents a dozen points to use when discussing the issue with their children. Stoddart produced a similar package for high school students last fall, but says she wants to lower the bar as younger and younger children jump online. Canadian Press; Ottawa Citizen; CBC News; 580 CFRA News; Toronto Star

US launched cyber attacks on other nations
The assumption that the US has the technological know-how to cripple a competing nation has always been just that: as assumption. In a recent sit-down interview, however, a former spy chief confirmed that America has already waged cyber attacks. Mike McConnell, the former director of national intelligence at the National Security Agency under George W Bush, tells Reuters this week that cyber war is more than a distant possibility. According to the current vice chairman at Booz Allen Hamilton, the US has already launched attacks on the computer networks of other nations. RT

The not-so-advanced persistent threat
Stuxnet, DuQu and the advanced persistent threat (APT) are currently dominating the headlines. Sophisticated zero-day exploits, carefully researchered and planned attacks that appear to be almost impossible to defend against, have many security professionals wondering if this is a game they can possibly win. The part that is often overlooked: These attacks target only a small number of organizations. SC Magazine

Hackers hijack US trains
Foreign hackers apparently took control of the US Northwest rail company's computers and played trains with the railway signals twice in December. Apparently the train service on the unnamed railroad "was slowed for a short while" and rail schedules were delayed about 15 minutes after the interference. Having caught a US train from New York to Florida and arrived a day and a half late we are surprised that any one noticed a 15 minute delay. The next day before rush hour, a "second event occurred" that did not affect schedules, TSA officials added. The report into the train hack seems to be its first major brush with cyber crime. The Homeland Security Department, which oversees TSA, is not sure if the rail infiltration was a targeted attack. However, it seems that the events were enough to start the TSA on a programme to educate the train companies on the perils of hacking. TechEye.net; Nextgov

Microsoft fingers alleged Kelihos botnet kingpin
Microsoft has filed a lawsuit against a Russian national who allegedly created and operated the Kelihos botnet, prior to a takedown operation in September 2011. The Register

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

Williston, Sandra

From: Bergeron, Dominic
Sent: January-25-12 1:48 PM
To: Bakri, Kareem
Subject: RE: The US "getcybersafe" equivalent Hacked

I'm pretty sure our internet provider has a mechanism in place too but unsure how efficient it is.
A bunch of sites were taken down last week including the fbi.

From: Bakri, Kareem
Sent: January-25-12 1:47 PM
To: Bergeron, Dominic
Subject: Re: The US "getcybersafe" equivalent Hacked

There are mechanisms built into both the [redacted]

Kareem Bakri
991-2945

From: Bergeron, Dominic
Sent: Wednesday, January 25, 2012 01:45 PM
To: Bakri, Kareem
Subject: RE: The US "getcybersafe" equivalent Hacked

Real question: How can we effectively protect ourselves against distributed denial of service (thousands of nodes)

From: Bakri, Kareem
Sent: January-25-12 1:27 PM
To: Bergeron, Dominic
Subject: FW: The US "getcybersafe" equivalent Hacked

Did you hear anything about this yet?

From: McCorkell, Shawn
Sent: January-25-12 12:31 PM
To: Bakri, Kareem
Subject: Fw: The US "getcybersafe" equivalent Hacked

From: Szauksztun-Zvinis, Robert
Sent: Wednesday, January 25, 2012 12:28 PM
To: Hunter, Linda; Robertson, Steve; Charette, Yves
Cc: McCorkell, Shawn; Ecker, Neil
Subject: FW: The US "getcybersafe" equivalent Hacked

FYI

Robert Szauksztun-Zvinis

Manager | Gestionnaire
Applications and Server Platforms Division | Division des applications et plates-formes du serveur
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West Ottawa ON K1A 0P8 | 269 avenue Laurier ouest Ottawa ON K1A 0P8
robert.szauksztun-zvinis@ps-sp.gc.ca
Telephone | Téléphone 613-991-7048
Facsimile | Télécopieur 613-948-8877
Government of Canada | Gouvernement du Canada

From: MacKenzie, Sara
Sent: Wednesday, January 25, 2012 10:38 AM
To: Eke, Darren; Stanfield, Charles; Hannan, Andrew; Jarrette, Amy; Charette, Yves; Szauksztun-Zvinis, Robert; Crépeault, David
Subject: Fw: The US "getcybersafe" equivalent Hacked

FYI

Yves, Robert: please forward to others as required.

From: Champoux, Martin
Sent: Wednesday, January 25, 2012 10:34 AM
To: Beaudoin, Luc S; Hatfield, Adam
Cc: Swift, Andrew; MacKenzie, Sara
Subject: RE: The US "getcybersafe" equivalent Hacked

I have already passed it on.

From: Beaudoin, Luc S
Sent: Wednesday, January 25, 2012 10:22 AM
To: Champoux, Martin; Hatfield, Adam
Subject: The US "getcybersafe" equivalent Hacked

This is to draw you attention to the CCIRC daily entry from yesterday. Could you please forward to the GetCyberSafe site team ?

5. Title : US govt security website hacked
Portal offering Internet security advice taken offline by hacktivist group Anonymous in protest of piracy crackdown
Hacktivist group Anonymous has claimed responsibility for taking down a website operated by US Federal Trade Commission (FTC) that offers Internet security advice to consumers.
The hit on OnGuardOnline.gov appears to go beyond the usual denial of service attack. The Pastebin post claiming responsibility for attack purports to show a log of the intrusion in progress, with the hacker gaining complete access to the site's back-end MySQL database and posting links to a full copy of its copied structure.
Reference: http://www.information-age.com/channels/security-and-continuity/news/1687113/us-govt-security-website-hacked.thtml

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

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-24-12 10:20 PM
To: Beaudoin, Luc
Subject: OpsIreland

Irish Government's moves to introduce copyright legislation has gotten the attention of Anonymous as they announced this evening they plan to attack Irish websites.

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

Williston, Sandra

From: Clow, Patrick
Sent: January-23-12 7:42 AM
To: Turbide, Frank; Melanson, Daryl
Subject: CyberNews

Something to consider including in Cyber News this morning.....

"After Wednesday's unprecedented unified online yelp against SOPA and PIPA, Thursday saw a new milestone: the first direct and public activist malware from Anonymous. A version of Anonymous' voluntary botnet software, known as LOIC (Low Orbit Ion Canon), was modified to make it not so voluntary, drafting unwary bystanders, journalists and even anons who don't support DDoS tactics into attacks on the U.S. Justice Department. Thursday's trickery seems not to have been central to the successful takedown of sites like justice.gov, RIAA.com and MPAA.com, but not all anons are pleased with forcing unwitting bystanders to join in a potentially illegal action.

The trick snagged those who happened to click on a shortened link on social-media services, expecting information on the ongoing #opmegaupload retaliation for the U.S. Justice Department's takedown of popular file sharing site Megaupload. Instead they were greeted by a ***Javascript version of LOIC*** *— already firing packets at targeted websites by the time their page was loaded."*

http://www.wired.com/threatlevel/2012/01/anons-rickroll-botnet/

Williston, Sandra

From: Klassen, Nathan
Sent: January-20-12 11:46 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Hi Ken and Luc,

The requested brief is attached. Comments due by 1:30 PM today in order to get this to RD before the weekend. FYI, Gregg has reviewed the draft and he is happy with it. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Williston, Sandra

From: Gregg.Murphy@ps-sp.gc.ca
Sent: January-20-12 10:54 AM
To: Klassen, Nathan
Subject: Anonymous

http://www.kctv5.com/story/16558352/anonymous-takes-down-doj-fbi-sites
http://www.firstpost.com/tech/fbi-shuts-down-megaupload-com-anonymous-shut-down-fbi-188266.html

"Federal officials confirmed it was down on Thursday evening and that the disruption was being "treated as a malicious act." " This is all I have as far as confirmation...

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

Williston, Sandra

From: Bergeron, Dominic
Sent: January-20-12 8:51 AM
To: Clow, Patrick
Subject: Re: Interesting day?

You watch traditional news??? :p

----- Original Message -----
From: Clow, Patrick
Sent: Friday, January 20, 2012 07:42 AM
To: Bergeron, Dominic
Subject: RE: Interesting day?

First story on CBC news last night.

-----Original Message-----
From: Bergeron, Dominic
Sent: January-19-12 9:48 PM
To: Clow, Patrick
Subject: Interesting day?

You've been following the news about anonymous' rampage today?

Its pretty amazing the amount of nodes these guys could get together for ddos. At least 11 sites went down including the fbi.

Makes you wonder what can be done to stop such embarrassing attacks.

Dom.

Williston, Sandra

From: Williston, Sandra
Sent: January-12-12 12:41 PM
To: Pitcher Robert; Moore, Bruce; Phlek, Vireak
Cc: Beaudoin, Luc S
Subject: RE: Comments? Top 10 threats of 2012

BotNets are still prevailant.

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: Pitcher Robert
Sent: January-12-12 12:20 PM
To: Moore, Bruce; Phlek, Vireak; Williston, Sandra
Cc: Beaudoin, Luc S
Subject: Comments? Top 10 threats of 2012

Guys,

I've been asked to put together an overview of shit we'll face in 2012. I came up with the following. Robert Dick/Gordon are to present this in the upcoming weeks. They said interface with csis and csec, but I figure we have to collective know how to avoid that idea. Anyway, here's my top 10. Anything you guys feel is too off the mark, or feel should be in, please let me know. Thanks!

- Continuation of targeted email attacks
  - Socially engineered to succeed!
- Advance malware attacks
  - Stuxnet: "…military grade software"
- Phishing attacks
  - Banking/Financial
- Social Network exploitations
  - Facebook has 800 million users. That's a lot of potential targets…
- Patch integrity
  - Keeping systems up to date!
- Cloud computing security
  - Security "outside the wire"
- Mobile/portable devices
  - IPhone/BlackBerry/Android malware
- Socially motivated/Extremely Capable
  - "Anonymous" attacks

- Software integrity
  - 0-Day exploits
- Secondary storage devices
  - Defeating perimeters by USB

Regards,
Robert Pitcher
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 949-8318
Fax/télécopieur: (613) 996-0995
Email/Courriel: Robert.Pitcher@ps-sp.gc.ca
Website/Site Internet: http://www.ps-sp.gc.ca

Williston, Sandra

From: Dincoy, Rana
Sent: January-12-12 10:30 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce; Anderson, Windy
Subject: RE: Confirming the incident write-ups for the Weekly Summary

Hi Luc, thanks for your comments and suggestions. You have a valid point about using the reports CCIRC receives to pull out some numbers to sketch out a picture of the cyber ecosystem. We in the strategic unit have talked about this previously and decided it would be appropriate to put them in a monthly product that would talk more about trends. We also have some work to do in terms of evaluating how meaningful these numbers would be for situational awareness and putting the right context around them for non-technical senior managers. We will also need some technical help with the analysis of that data. For example, in the next update of the Notification tool, an automatic counter and categorization by CI sector would be helpful.

As for the DNS Changer: I was under the impression you were in contact with US authorities on this matter and thought it was the CERT. If that's not true I'll remove it.

As requested, I will no longer copy the cyberdo in my e-mails for the Weekly Summary.

Thanks again for your comments and getting back to me so quickly... One of my challenges in writing this product is striking the balance between technical accuracy and clarity for non-technical readers... It's like the holy grail!

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

From: Beaudoin, Luc S
Sent: January-11-12 7:41 PM
To: Dincoy, Rana
Cc: Moore, Bruce; Anderson, Windy
Subject: Re: Confirming the incident write-ups for the Weekly Summary

Rana, I would appreciate if you addressed your questions to me, as stated before. Bruce and the other IH are busy doing their tactical job and should not be disrupted unless a new operational matter comes to your attention and I am not around. Strategic reports review is not their role.

There are fundamentals in these reports which are in my opinion inaccurate. These subtilties are important.

1) Item 1 is stratfort. It is public, so just say their name. They are not an "agency", they are a company. Go on wikipedia for more info.

2) Malicious email and threat actor refer usually to malware and state sponsored. Use Phishing or scam email and cyber criminals instead.

3) Don t state "potential compromise of povincial computer systems". Rather state "limited number of computer systems in Canadian Critical Infrastucture organisations potentially affected by known botnets malicious codes.

4) A website provider...replace by: a canadian internet and webhosting service provider website defaced by cyber vandals.

5) First note: typo (repeated "been" twice. Remove yellow section. State CCIRC data sources have consistently proven to be of high accuracy.

6) Not sure what US CERT has to do with DNSChanger. Remove.

7) CI finance: bank phishing does not lead to compromise. It entice users to enter PII by luring them to fake bank site (copies)

8) Comment on ISP vandalized: BEAUTIFUL !!!!

9) Stratfor: name it. [redacted] Otherwise, phishing emails have been reported so far focussed at embarassing the stratfort organisation. No malware was reported in phishing cases at this time. Stratfort posted public information and a video about the breach as well as contacted all its clients offering them 1 year privacy protection services from a 3rd party.

10) Why are we still not stating metrics like: total and average number of canadian infected hosts per day [redacted] number of canadian host still infected by ghostclick [redacted] who will loose connection to internet on the 8 Mar, number of canadian malicious sites in sandbox reports and [redacted], Arbor networks canadian ranking, trends in these values, number of reported canadian banking phishing sites reported... Why ? These are more meaningfull SA for canada.

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: Dincoy, Rana
Sent: Wednesday, January 11, 2012 11:45 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

Williston, Sandra

From: Williston, Sandra
Sent: January-06-12 9:56 AM
To: Anderson, Windy
Cc: Klassen, Nathan; [redacted]
Subject: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

CCIRC CE11-2549
File No.: 384942
RDIMS No.: 541243

Hello Windy;

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

Stratfor Global Intelligence has already notified all affected users through email, facebook and twitter. The mitigation advise to their customers was to contact their financial institution and inform them of this incident and to watch for any unauthorized activity on their accounts. In addition, they have advised that they will provide paid subscribers with identity protection coverage with a leading provider of global identity protection company at their expense for 12 months.

[redacted]

CCIRC has closed this incident and will continue to monitor.

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

Pages 226 to / à 242

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Anderson, Windy

From: Gordon, Robert
Sent: January-31-12 8:07 AM
To: Matz, Mark
Cc: Dvorkin, Corey; Dick, Robert; Hatfield, Adam; Anderson, Windy
Subject: FW: Cyber: Cyber Security, Global Trends and Defences (SDA Report)
Attachments: Cyber-Security - Global Rules, SDA 2012.pdf

FYI

Robert W. (Bob) Gordon
Special Advisor, Cyber Security / Conseiller spécial, cybersécurité
Public Safety Canada / Sécurité publique Canada
340 Laurier Avenue West / 340 avenue Laurier Quest
Ottawa, Ontario K1A 0P9 / Ottawa (Ontario) K1A 0P8
613 949-7380 Fax/Téléc.: 613 990-3287
E-Mail / Courriel: Robert.Gordon@ps-sp.gc.ca

Report: *Cyber Security: The Vexed Question of Global Rules*, is attached

http://www.darkreading.com/security/news/232500700/mcafee-and-security-defence-agenda-release-global-cyber-defense-report.html

McAfee and Security & Defence Agenda Release Global Cyber Defense Report

Fifty-seven percent of global experts believe that an arms race is taking place in cyberspace

Jan 30, 2012 | 12:11 PM |

Brussels, Washington DC - JANUARY 30, 2012 - McAfee and the Security & Defence Agenda (SDA) today revealed the findings from a report; Cyber-security: The Vexed Question of Global Rules that paints, for the first time, a global snapshot of current thinking about the cyber-threat and the measures that should be taken to defend against them, and assesses the way ahead. The SDA, the leading defense and security think-tank in Brussels, interviewed leading global security experts to ensure that findings would offer usable recommendations and actions. The report was created to identify key debate areas and trends and to help to governments and organizations understand how their cyber defense posture compares to those of other countries and organizations.

Here are some noted findings:

57% of global experts believe that an arms race is taking place in cyber space. 36% believe cybersecurity is more important than missile defense. 43% identified damage or disruption to critical infrastructure as the greatest single threat posed by cyber-attacks with wide economic consequences (up from 37% in McAfee's

2010 Critical Infrastructure Report). 45% of respondents believe that cybersecurity is as important as border security. The state of cyber-readiness of the United States, Australia, UK, China and Germany all ranked behind smaller countries such as Israel, Sweden and Finland (23 countries ranked in report).

McAfee asked the SDA, as an independent think-tank, to produce the most informed report on global cyber defense available. The SDA had in-depth interviews with some 80 world-leading policy-makers and cybersecurity experts in government, business and academia in 27 countries and anonymously surveyed 250 world leaders in 35 countries. As the only specialist security and defense think-tank in Brussels, SDA has become one of the world's leading forums for the discussion of international defense and security policies. The methodology used for rating various countries' state of cyber-readiness is that developed by Robert Lentz, President of Cyber Security Strategies and former Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance. [see here for infographic on rankings]

Top 6 Actions Cited in Report

Real-time global information sharing required Financial incentives for critical improvements in security for both private and public sectors Give more power to law enforcement to combat cross-border cyber crime Best practice-led international security standards need to be developed Diplomatic challenges facing global cyber treaties need to be addressed Public awareness campaigns that go beyond current programs to help citizens

Real-time sharing of global intelligence was a core recommendation of the report, citing the building of trust between industry stakeholders by setting up bodies to share information and best practices, like the Common Assurance Maturity Model (CAMM) and the Cloud Security Alliance (CSA). "The core problem is that the cyber criminal has greater agility, given large funding streams and no legal boundaries to sharing information, and can thus choreograph well-orchestrated attacks into systems," says Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector, McAfee. "Until we can pool our data and equip our people and machines with intelligence, we are playing chess with only half the pieces."

Experts interviewed also agreed that developments like smart phones and cloud computing mean we are seeing a whole new set of problems linked to inter-connectivity and sovereignty that require new regulations and new thinking. Last year, McAfee issued a Q3 threat report that stated that the total amount of malware targeted at Android devices jumped 76 percent from Q2 of 2010 to Q2 of last year, to become the most attacked mobile operating system.

Other key report findings from the SDA report include the following:

Need to address expected shortage of cyber workforce: More than half (56%) of the respondents highlight a coming skills shortage. Low level of preparedness for cyber attacks: China, Russia, Italy and Poland fall behind Finland, Israel, Sweden, Denmark, Estonia, France, Germany, Netherlands, UK, Spain and the United States. Cybersecurity exercises are not receiving strong participation from industry: Although almost everyone believes that exercises are important, only 20% of those surveyed in the private sector have taken part in such exercises. Risk assessment: Prioritize information protection, knowing that no one size fits all. The three key goals that need to be achieved are confidentiality, integration and availability in different doses according to the situation. Balance between security and privacy: Improve attribution capability by selectively reducing anonymity without sacrificing the privacy rights.

While many respondents believed that global treaties were an essential factor in the development of sound policy, some also suggested the establishment of cyber-confidence building measures as alternatives to global treaties, or as a stopgap measure, since treaties are seen as unverifiable, unenforceable and impractical. Stewart Barker, the former Assistant Secretary of Homeland Security under President George W. Bush, stated that

treaties "delude western countries into thinking they have some protection against tactics that have been unilaterally abandoned by other treaty signatories."

About the report: McAfee asked the Security & Defence Agenda (SDA) as an independent think-tank to produce the most extensive report on Cyber Defense. The report stack ranks the degree to which governments are prepared to withstand cyber attacks. This SDA report sets out to reflect the many different views on what cyber-security means, and how to move towards it. To build up a multi-faceted picture of opinion worldwide, SDA interviewed world leaders to highlight what they see as the key issues.

To download "The Cyber Defense Report" report please visit www.mcafee.com/

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-24-12 8:21 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; CYBERDO; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted]; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted]; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 24, 2012/ le 24 janvier 2012

Print Media

Scammer most foul
As it turns out, the computer virus scam is so widespread that the RCMP and Canadian Anti Fraud Centre (CFAC) issued a warning about it last fall. The RCMP says the increase in calls from frustrated Canadians indicates that the scam is actually working. Times & Transcript

Meeting a precursor to planned exercises
Top government and military leaders met at CFB Kingston last week to discuss the future of Canadian military and humanitarian missions. Hosted by 1 Canadian Division Headquarters, the discussion included representatives from Canada's army, navy, air force and special forces, as well as civilian officials from the Department of Foreign Affairs and International Trade, the Canadian International Development Agency and the **Ministry of Public Safety**. The seminar covered topics including the headquarters unit's principle responsibilities -- deployment of the Disaster Assistance Response Team (DART) , the evacuation of Canadian civilians from crisis areas and the deployment of Canadian military units -- as well as offshore piracy and cyber attack. Kingston Whig-Standard

Online Media

Microsoft fingers alleged Kelihos botnet culprit
Four months after taking down the Kelihos botnet, Microsoft on Monday identified the man it believes was behind the massive infection designed to deliver spam and steal data. ZDNet UK; CNET

Anonymous to attack Facebook on January 28 (video)
A new video allegedly from the hacktivist group Anonymous claims the next target is Facebook. Anonymous wants to take down Facebook with a Distributed Denial of Service (DDoS) attack. ZDNet

China-based Cyber Attack Targets DoD Access Cards
Cyber security firms have discovered a computer virus that uses servicemembers' network security cards to hack into government networks. Blasco said he suspects the cyber attack originates from China because of the Chinese characters found within the virus' coding. Military.com

Researcher traces 'Gameover' malware to maker of Zeus
The "Gameover" malware that the FBI warned users about earlier this month is a preview of the next version of the even-more-notorious Zeus money-stealing Trojan, a security researcher said today. Computerworld

Cyber defence managed service
Cyber attacks are on the increase. It seems that almost every day the media report on yet another serious security breach and that no one is immune. The consequences of a cyber attack are far reaching. Apart from the obvious damage that hacking causes to systems and networks; negative press, loss of credibility, loss of customers (and revenue) and long-term damage to brands can set an organisation back decades. The Guardian (UK)

Researchers demonstrate tragic state of SCADA security
Since the discovery of Stuxnet, we've been hearing from a variety of researchers about security vulnerabilities in SCADA computer systems. While some researchers such as Luigi Auriemma occasionally share with the public entire batches of SCADA flaws and PoC attacks for exploiting them, others get pressured by authorities and manufacturers into canceling their lectures about their discoveries. Help Net Security

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

Klassen, Nathan

From: Bendelier, Kenneth
Sent: January-24-12 7:54 AM
To: Klassen, Nathan
Subject: RE: Third BN you did

Right, thanks

-----Original Message-----
From: Klassen, Nathan
Sent: January-24-12 7:53 AM
To: Bendelier, Kenneth
Subject: Re: Third BN you did

Not sure what your questions is -- I have done far more than 3 briefing notes :). Last week I did the Israeli and Anonymous ones (stat report and Rana's weekly made up our 4 SA products that week).

I was going to also do one on the Internet blackout - but we ran out of time. Cheers,

Nate

----- Original Message -----
From: Bendelier, Kenneth
Sent: Tuesday, January 24, 2012 07:42 AM
To: Klassen, Nathan
Subject: Third BN you did

Brain fart.

Got the one on Israel and the attacks in the States. What was the third one?

Thanks

Klassen, Nathan

From: Klassen, Nathan
Sent: January-24-12 7:53 AM
To: Bendelier, Kenneth
Subject: Re: Third BN you did

Not sure what your questions is -- I have done far more than 3 briefing notes :). Last week I did the Israeli and Anonymous ones (stat report and Rana's weekly made up our 4 SA products that week).

I was going to also do one on the Internet blackout - but we ran out of time. Cheers,

Nate

----- Original Message -----
From: Bendelier, Kenneth
Sent: Tuesday, January 24, 2012 07:42 AM
To: Klassen, Nathan
Subject: Third BN you did

Brain fart.

Got the one on Israel and the attacks in the States. What was the third one?

Thanks

January 23, 2012

UNCLASSIFIED

DATE:

File No.: 385262
RDIMS No.: 550276

MEMORANDUM FOR THE DEPUTY MINISTER

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEBSITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) websites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, 2012, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of Friday, January 20, 2012, most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these websites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Gregg Murphy

UNCLASSIFIED

DATE:

File No.:
RDIMS No.: 550276

MEMORANDUM FOR THE DEPUTY MINISTER

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Gregg Murphy

Klassen, Nathan

From: Bendelier, Kenneth
Sent: January-23-12 1:26 PM
To: Dincoy, Rana; Klassen, Nathan
Subject: RE: New write-up for a new event - My comments underlined

THIS WEEK AT CCIRC

NEW EVENTS REPORTED IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted (type of authority (law enforcement?)authority that personal and credit card information of Strategic Forecasting Inc (brief description of STRATFOR) (STRATFOR)'s (delete "website", otherwise the sentence is hard to read) website report clients were posted on the Internet by a hacker group. Over [redacted] (in this case, the type of client is important – law enforcement, etc,) were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident. (and will.....)

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure (both personal and corporate..) passwords and credit card information is secure. (Delete this line about free privacy protection) STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons. (In my opinion, less comments above, this is very good)*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack. (note sure this latter line is required)

From: Dincoy, Rana
Sent: January-23-12 1:12 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: New write-up for a new event
Importance: High

What do you think of this:

THIS WEEK AT CCIRC

NEW EVENTS IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure. STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

s.16(2)(c)

Klassen, Nathan

From: Klassen, Nathan
Sent: January-23-12 1:26 PM
To: Dincoy, Rana
Cc: Bendelier, Kenneth
Subject: RE: New write-up for a new event
Attachments: THIS WEEK AT CCIRC -- Nate's comments.docx

s.16(2)(c)

Hi Rana,

Txs for the opportunity to comment. My quick thoughts are in the attached document. Sry – I did not have time to read through for editing / grammar. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Dincoy, Rana
Sent: January-23-12 1:12 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: New write-up for a new event
Importance: High

What do you think of this:

THIS WEEK AT CCIRC

NEW EVENTS IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure. STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

THIS WEEK AT CCIRC

New Events

1. **STRATFOR hacking.** CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks. CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

- ***Comment:*** *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure.* ***STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.***

Formatted: Font: +Headings (Cambria), 18 pt, Underline

Deleted: IN CANADIAN CRITICAL INFRASTRUCTURE

Formatted: Font: +Headings (Cambria), 14 pt, Italic

Deleted: *NEW EVENTS*

Formatted: Font: (Default) Times New Roman, 12 pt

Deleted: ¶
<#>¶
¶
¶

Formatted: Font: Not Bold

Formatted: Font: Italic

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.27 cm + Indent at: 1.9 cm

Deleted: *STRATFOR also offers a one-year privacy protection to clients.*

Comment [KN1]: Something on corporate emails

Formatted: Font: Italic

Deleted: ¶
STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.¶

Dincoy, Rana

From: Dincoy, Rana
Sent: January-23-12 1:12 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: New write-up for a new event s.16(2)(c)

Importance: High

What do you think of this:

THIS WEEK AT CCIRC

NEW EVENTS IN CANADIAN CRITICAL INFRASTRUCTURE

STRATFOR hacking. CCIRC learned from a trusted authority that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s website report clients were posted on the Internet by a hacker group. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure passwords and credit card information is secure. STRATFOR also offers a one-year privacy protection to clients. STRATFOR clients whose names and e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information. The release of physical addresses could also be of concern to certain clients for privacy and security reasons.*

STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information. Given STRATFOR's client base and denial of involvement by Anonymous, some experts have speculated about the true identity and motives of those responsible for this attack.

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

Dincoy, Rana

From: Dincoy, Rana
Sent: January-23-12 3:47 PM
To: Bendelier, Kenneth; Klassen, Nathan
Subject: For your review - PS-SP-#543735-v11A-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_JAN_3__2012
Attachments: PS-SP-#543735-v11A-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_JAN_3__2012.DOC.doc

Your comments have been incorporated. The only thing missing is the blurb in the back on who CCIRC is, our mandate, and reporting cyber incidents to CCIRC...

Public Safety Canada | Sécurité publique Canada

Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 14-28, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-002

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations.

This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents reported over the last two weeks. There were reports of Canadian computers being used for malicious purposes, including attacking a US State Police website. A Canadian federal department linked to the signing of the international Anti-Counterfeiting Agreement (ACTA) was targeted through a malicious e-mail. There was also a message on the Internet by hackers to e-mail or launch a cyber attack against this Department. Internationally, hackers attacked government websites in US, Poland, Ireland and the EU to protest signing of ACTA. There are also continued reports of infected computers in Canada and around the world due to the Ghostclick fraud.

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- US State Police website attack traced to Canada
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

CCIRC Products Released during the reporting period:

- Cyber Flash on cyber attacks by Anonymous related to copyrights and intellectual property (CF12-001)

Noteworthy News in the Media:

- Israeli and Palestinian hackers exchange website attacks
- Hackers around the world protest current and intended anti-piracy measures:
    - MegaUpload's shutdown prompts hacker attacks on US government and music industry websites
    - Proposed US copyright law SOPA being protested: Certain websites elect to go dark for one day in protest; Anonymous attacks US government websites such as DOJ & FBI
    - Signing of the international Anti-Counterfeiting Agreement (ACTA) prompting hacker attacks on US, Poland, Ireland and European government websites.

NEW EVENTS REPORTED IN GOVERNMENT AND OTHER CANADIAN CRITICAL INFRASTRUCTURE SECTORS

Federal Government Sector

Operation SACTA (Stop Anti-Counterfeiting Trade Agreement): An online message signed by Anonymous posted a link to a Canadian federal department website, encouraging users to join the anti-ACTA movement, and attack if necessary. This message was posted on a popular text-file sharing website often used by hackers and is presumably encouraging cyber attacks on websites.

CCIRC provided available technical details to CTEC, the federal Government's CERT, for their further investigation.

> ***Comment:*** *There are provisions in the international Anti-Counterfeiting Trade Agreement that have important implications for content sharing on the Internet. This is a multi-lateral trade agreement which Canada has signed. Canada's new proposed copy-right law, Bill C-11 (former Bill C-32), is currently in Parliament at the second reading stage. There is a great deal of opposition to this agreement around the world by the on-line community and websites of other government have recently been attacked by hackers in protest.*

File Server (FTP) Login Credentials of a Federal Department posted on the Internet. CCIRC learned that the FTP login credentials of a federal department were posted on the Internet. CCIRC advised CTEC and provided known technical details.

> ***Comment:*** *FTP login credentials are used to gain access to a file sharing server where users may upload or download files. If a threat actor used these credentials, the result could be information compromise or the use of the server as a launch point for cyber attacks.*

Non-Federal Government Sector

Canadian computers being used in cyber attacks. CCIRC has learned that a cyber attack on a US State Police website was traced to a Canadian university's computer. In addition, another Canadian university's website was found to host malicious software that could infect website visitors. There were also reports of malicious software being hosted at a website hosting service provider's server and at two other unidentified Canadian entities.

CCIRC contacted the known Canadian organizations, with mitigation advice. The RCMP was informed of items of interest. CCIRC warned the website hosting service provider that the website in question was added to various block lists, possibly resulting in reduced legitimate traffic to this website. The malicious software from the university's website has been removed and is no longer being served.

> ***Comment:*** *It is possible that cyber criminals compromised these Canadian computers to use them remotely for malicious purposes, without their owners' knowledge. Organizations that offer computers for public use, such as universities, can be particularly susceptible to such compromises.*

Some Canadian Industrial Control Systems exposed to potential cyber attacks. A trusted international partner alerted CCIRC that information that could allow remote access to certain Canadian houses and apartment buildings' heating and air conditioning systems, was posted on the Internet. CCIRC alerted those responsible for the buildings and houses, offering mitigation advice. There is no report of any cyber attack in these cases at this time.

> ***Comment:*** *Many Industrial Control Systems (ICS), such as the ones used for heating and cooling buildings, are monitored or even maintained remotely through the use of certain software. It is likely that the technicians responsible for the set-up and maintenance of the heating systems for these buildings did not take cyber security into consideration or did not know the standard practices for protecting against such exposure.*
>
> *Since the Stuxnet virus attack on an Iranian nuclear facility, there has been a heightened awareness, both domestically and internationally, of cyber security for ICS. The trusted international partner who alerted CCIRC is focussed primarily on securing ICS. CCIRC recently moderated discussion at a ICS conference in Montreal.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonating Canadian financial institutions, tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in United States and Taiwan.

Cyber criminals also attempted to solicit personal information by impersonating Service Canada and Canada Revenue Agency.

CCIRC notified the impersonated financial institutions of these fraud attempts and the Government CTEC for the federal government cases. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website compromises and publicized vulnerabilities. CCIRC discovered a small health organization's website was defaced and offered mitigation advice. CCIRC also discovered a foreign Defence Department's website was compromised and contacted the organization, as well as CCIRC's equivalent organization. There was also a list of vulnerable websites posted on the Internet, which includes a Canadian university.

There were additional website compromises in the health and non-critical infrastructure sectors. Website usernames and passwords were posted on the Internet by hackers.

> ***Comment:*** *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

Ghostclick Fraud. There were new and continued reports of infected computers in three provincial governments, three provincial health organizations, an airport authority, an energy organization, two banks, 19 Canadian universities, a national media organization and 13 telecommunications companies.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are currently websites around the world for computer users to check whether their machine is infected by the malicious software used in this fraud. These sites can be found by searching with the keywords "dns-ok".

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in. CCIRC is also working with the Canadian Internet Registration Authority (CIRA) to provide notifications to affected users.

Operation Ghostclick was worldwide fraud campaign, exposed in late 2011 by the FBI. Cyber criminals hijacked users' Internet web searches and diverted them to websites that generated advertising and sales revenues. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

> ***Comment:*** *Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. CCIRC noted that the type and size of affected organizations varied, and were spread across Canada. The number of affected telecommunications companies more than likely indicates number of infected client computers of Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*
>
> *Organizations that offer Internet access, including those that provide publically accessible wireless networks, may be particularly vulnerable. In addition to the cooperative effort underway between CCIRC and CIRA, the Canadian government has launched a website for cyber security public education..*

CCIRC PRODUCTS RELEASED:

Hacktivist attacks related to proposed anti-piracy legislation. There have been coordinated distributed denial-of-service (DDoS) attacks on websites by hacktivists, claiming to be associated with Anonymous. There were multiple international targets, which included governments (Canada, US, Poland, Ireland and EU) and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

not a redaction

In response, CCIRC issued Cyber Flash CF12-001, titled *"Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property"*. This Cyber Flash, was sent to technical and security contacts within stakeholder organizations in government and other critical infrastructure

sectors . Government and industry organizations involved with the Copyright legislation and copy-righted material were encouraged to assess their risk exposure to coordinated DDoS attacks on their networks.

NOTEWORTHY NEWS IN THE MEDIA:

Israeli and pro-Palestinian hackers exchange website attacks. Open sources reported that the websites of Israel's main stock exchange, several banks and the national airline were attacked. Pro-Palestinian hackers claimed responsibility and even claimed to have posted the login credentials for several industrial control systems in Israel on the Internet. Shortly thereafter, there were reports of suspected Israeli hackers bringing down the Saudi Stock Exchange, interfering with the Abu Dhabi Security Exchange, and publishing e-mail addresses & passwords of 30,000 Arab Facebook users.

Comment: *It is now becoming commonplace to carry real-world grievances into the cyber world. There could be an adverse impact from these attacks for Canadians and Canadian businesses that do business with the stock exchanges or banks involved. There were some media reports that some of the Israeli banks could block international access to their sites.*

Hackers around the world attack government websites to protest anti-piracy measures.

- **Retaliation for file-sharing service Mega Upload's shutdown:** Hackers, claiming to be with Anonymous, attacked the websites of the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music.

- **Signing of the international Anti-Counterfeiting Agreement (ACTA) and proposed US copyright laws:** Wikipedia shut down for one day to protest the proposed SOPA and PIPA bills. SOPA and PIPA were also cited by Anonymous as a reason for their attacks on the DOJ and FBI websites. Operation STOP ACTA by Anonymous also prompted hacker attacks on websites for US, Poland, Ireland governments as well as for the European Parliament.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

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

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Pages 268 to / à 275

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

UNCLASSIFIED

DATE: February 20, 2012

File No.:
RDIMS No.:

MEMORANDUM FOR THE DIRECTOR GENERAL

ANONYMOUS THREAT TO DOMAIN NAME SERVICE ROOT SERVERS
(Information only)

ISSUE

Internet postings claiming to have been authored by the hackivist group Anonymous indicate a potential Distributed Denial of Service (DDoS) attack against the Domain Name Service (DNS) root servers may take place on the 31st of March 2012. Under the auspices of "Operation Global Blackout", the stated objective of this DDoS attack is to "shut the Internet down".

BACKGROUND

DNS resolves human-readable domain names (e.g. google.com) into routable Internet Protocol (IP) addresses (e.g. 123.123.123.123). While DNS provides a number of supporting capabilities to the operation of the Internet, its core function is analogous to that of a telephone book. Just as the phone system cannot route a person or a business name to a particular phone number, the Internet cannot route to a domain name. Thus, when a phone call needs to be made to an "A. Smith" in Ottawa, a phone user looks this name up in a phone book and finds the phone number assigned to A. Smith. The phone system can then complete the call to the device to which the phone number for A. Smith is assigned. DNS provides a similar service to the Internet.

A **DDoS** attack is a form of cyber-attack in which multiple computers, distributed both geographically and across networks, are coordinated in such a way that their combined efforts are used for a specific objective. In general, DDoS attacks either consume all or most of the network bandwidth available to the target, or they exceed the resource capacity of the targeted device(s). The impact to the end user is that service response is very slow or, in some cases, the requested service is unavailable. There have been two previous DDoS attempts against DNS root servers, one in 2002 and the second in 2007. In both cases, the infrastructure withstood the attacks and, in both cases, lessons learned were applied to make the DNS infrastructure more resilient to DDoS attacks.

Anonymous is a loosely-coupled collective associated with collaborative online hacktivism. The group has recently focussed its efforts against regulatory efforts associated with anti-digital piracy legislation, but has also supported environmental and social justice campaigns. Cyber-attacks attributed to Anonymous have successfully exfiltrated data from targeted organizations. However, the primary attack method employed by Anonymous is DDoS. Anonymous cyber-attacks are often coordinated via various social media sites. Anonymous has made available a number of tools to support DDoS attacks such that any computer user who chooses to participate in a can do so with ease and minimal computer knowledge.

CONSIDERATIONS

The stated purpose of the proposed attack against DNS root servers is to "shut the Internet down". Given previous successful DDoS attacks attributed to Anonymous against, for example, Visa, MasterCard, PayPal HBGary, Amazon, and most recently governments around the world, including the Canadian House of Commons, it is clear that both the intent and capability of Anonymous are legitimate. There are, however, a number of mitigating factors that make the success of Operation Global Blackout doubtful.

The infrastructure itself is both high-capacity and redundant. While, logically, there are 13 root servers on the Internet, the implementation sees the load spread across over 250 physical locations. These are provided with high-capacity network connections. In addition, should a DDoS attack take place, telecommunication providers would redirect or block malicious traffic destined for the root servers in order to maintain network availability. Finally, the distributed nature of DNS makes a complete Internet blackout very unlikely. To use the phone system analogy, suppose it were possible for someone to destroy all copies of the telephone book. Many people maintain a copy of their frequently dialed phone numbers locally, such as in a contact list, on a PDA, business cards, etc. DNS works in a similar fashion where "local" DNS servers, through a process known as *caching*, maintain a record of recently requested domain names and their IP addresses. This process is repeated up the hierarchy and, unless a DDoS attack was sustained for an extended period time (days), name resolution would work in the vast majority of cases.

It can be assessed that, unless prevented through the efforts of law enforcement agencies, a DDoS attack, coordinated by Anonymous against the DNS root servers, will likely take place on 31 March, 2012. However, it is unlikely the stated objective of shutting the Internet down will be achieved. The most likely impact is that there may be temporary instances of slower performance on some network segments.

NEXT STEPS

In addition to CCIRC, law enforcement and agencies responsible for the operation of the DNS infrastructure around the world are monitoring the situation and actively developing

mitigation plans. CCIRC will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Ken Bendelier

Bendelier, Kenneth

From: Bendelier, Kenneth
Sent: February-03-12 9:08 AM
To: [redacted]
Subject: Well, if anyone is looking to understand Anonymous TT&P s.16(2)(c)

Description:
6 FEBRUARY 15 Action against Mining and Energy companies in South America.

[redacted]

Pages 280 to / à 281

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

s.16(2)(c)

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: Beaudoin, Luc S
Sent: January-24-12 1:08 PM
To: Beaudoin, Luc S
Subject: JS LOIC
Attachments: SAR-12-12-021-01 - Anonymous response to the seizure of MegaUpload2.pdf

Very interesting report by US-CERT on recent anonymous activities and the use of JS LOIC.

Distribution is GREEN (ie: OK to share with need-to-know partners but not to post publicly)

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

Bendelier, Kenneth

From: Beaudoin, Luc S
Sent: January-23-12 12:42 PM
To: [redacted]
Cc: Danaitis, Algis; 'Tiago Dejesus' (Tiago.Dejesus@rcmp-grc.gc.ca); Maurizio Rosa (Maurizio.Rosa@rcmp-grc.gc.ca); CYBERDO; Darren Sabourin (Darren.Sabourin@rcmp-grc.gc.ca); * [redacted]
Subject: Anonymous anti-ACTA threat

Ref: CE12-2590

FY Awareness.

SITUATION:

CCIRC is monitoring a recent post by the hacktisvist group "Anonymous" on pastebin referred to Operation SACTA (Stop Anti-Counterfeiting Trade Agreement)

(http://pastebin.com [redacted]

This post refers to two a Federal Department Sites:

http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=eng&view=d
http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/intellect_property.aspx?view=d

DETAILS

These sites identify the following Canadian and international stakeholders:

- Canadian Intellectual Property Office
- Industry Canada's Intellectual Property Policy Information Page
- Canadian Heritage - Copyright Policy
- World Intellectual Property Organization (WIPO) Treaties
- World Trade Organization (WTO) – TRIPS

The post is encouraging supporters to:

1) "Spread the word! (twitter, piratepad, pastebit, WWP, flyers, you name it!)"
2) "mail the s**t out of your government demanding that ACTA is to be put away."
3) "Attack if necessary."
4)"???????????"
5)"Profit."

CCIRC has already observed reports of Anti-ACTA hackers attacking other websites such as Polish Government websites.
Reference: http://www.siliconrepublic.com/strategy/item/25451-anti-acta-hackers-attack-po

CURRENT ACTION

This information was provided to GC-CTEC for their action and mitigation of federal government stakeholders. CCIRC is actively monitoring the situation.

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

Hayward, Jane

s.15(1) - Subv

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-23-12 8:22 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; CYBERDO; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 23, 2012/ le 23 janvier 2012

Print Media

Beware of "anti-virus" scams
The Canadian Anti-Fraud Centre, formerly Project Phonebusters, issued an alert last year about socalled "anti-virus scams." It notes the scam has been proliferating since March 2010, and police in Manitoba and Ontario dealt with an increasing number of such complaints in 2011. Leader-Post

Woman victimized by Spanish email scam
Dorothy Pilarski started getting calls from friends who thought she was stranded in Spain. Hackers had gotten into her email account and written to all her contacts, pretending to be Dorothy. Toronto Star

The gang that hijacked your computer - Meet the Koobface group, who are living comfortably in Russia - allegedly several million dollars richer
Five men believed to be responsible for spreading a notorious computer worm - and to have pocketed several million dollars from online schemes - are hiding in plain sight in St. Petersburg, Russia, investigators say. The group is known as

the Koobface gang. Beginning in July 2008, the Koobface gang targeted web users with invitations to watch a funny or sexy video. Those curious enough to click the link got a message to update their computer's Flash software, which begins the download of the Koobface malware. Victims' computers are drafted into a "botnet," or network of infected PCs, and are sent official-looking advertisements of fake anti-virus software. Their web searches are also hijacked and the clicks delivered to unscrupulous marketers. The security software firm Kaspersky Labs has estimated the network included 400,000 to 800,000 PCs worldwide at its height in 2010. Hamilton Spectator

The day the web went dark - U.S. anti-piracy bills spark outrage online
The Issue: Many of the Internet's most-used websites went dark on Wednesday to protest the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA), anti-piracy bills currently wending their way through U.S. Congress. The protest appeared to work with impressive efficiency - many proponents withdrew support for the bills, seen as deeply flawed. While Google's dramatic blacked-out logo was visible only to U.S. users, the self-imposed disabling of major sites such as Wikipedia affected users worldwide, including Canadians. Toronto Star; Charlottetown Guardian

Des pirates s'en prennent au FBI
La fermeture jeudi par les États-Unis du site de téléchargement Megaupload a entraîné depuis 48 heures une série de contre-attaques de pirates informatiques. Le Federal Bureau of Investigation (FBI), le ministère de la Justice et le palais présidentiel français ont tous été touchés par le mouvement Anonymous. Hier, la police néo-zélandaise a procédé à l'arrestation de quatre personnes reliées au site de partages de fichiers Megaupload. Kim Dotcom (de son vrai nom Kim Schmitz), l'ancien président et chef de la direction de Megaupload, fait partie des suspects arrêtés. Le Soleil; Victoria Times-Colonist; Toronto Star; National Post; Montreal Gazette; Le Devoir

Online Media

Contractors vie for edge in cybersecurity race
The cybersecurity arms race is ramping up. In this case, it's contractors that are eager to show off an increasingly expansive set of capabilities ready for government use. Many contractors have erected cyber-focused centers near Fort Meade — home to both the National Security Agency and the U.S. Cyber Command — but some are now going a step farther. Washington Post

Government to form new body to oversee telecom and cyber security
India plans to set up a new body that will oversee telecom and cyber security to avoid overlap between various ministries and intelligence agencies that are currently handling this issue. The Economic Times

Israel's hobbyist hackers cause a stir, but not much else
Israel's news cycle has been dominated for the past two weeks by increasingly panicky reports of an escalating cyber war between it and the Arab world. For all the media hullabaloo, Israeli specialists in the field of cyber security reject the term "cyber war" altogether when it comes to the recent high jinx. The danger, Weimann said, is of "an actual terrorist attack perpetuated by computers. Real cyber terror involves hitting control systems of airports or other infrastructure, nuclear facilities, transportation systems, hospitals, everything that is controlled by computers. The damage and the risk are huge." GlobalPost

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-21-12 11:07 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - Last Part / Dernière partie

Daily Media Summary / Revue de presse quotidienne
Last Part / Dernière partie
January 21, 2012 / le 21 janvier 2012

MINISTER / MINISTRE

I spy - Russian diplomats were feted, not expelled
Russia's Foreign Ministry weighed into the unfolding spy scandal involving a Canadian intelligence officer on Friday by denying reports that four of its diplomats at the country's embassy in Ottawa were expelled. Multiple sources within the diplomatic community say at least of two of the staffers - defence attaché Lieutenant-Colonel Dmitry Fedorchatenko and Third Secretary Konstantin Kolpakov - left the country weeks before the arrest of Sub- Lieutenant Jeffrey Delisle on charges of violating the Security of Information Act. Although not discounting the allegation of spying, those who knew the pair among foreign missions were mystified at the suggestion they were expelled. "It was well-known last fall that they were leaving. Their time was up," said one senior European diplomat, who asked not to be named. "It's all very bizarre." **Public Safety Minister Vic Toews had little to say. *"I'm not aware of why those individuals left Canada,"* said Toews, minister for Canada's intelligence service.** Hamilton Spectator, A11 (Red Deer Advocate; Charlottetown Guardian); Toronto Star; Journal de Montréal; Le Devoir (L'Acadie Nouvelle; Le Droit; La Presse); * Winnipeg Sun (Toronto Sun; Ottawa Sun); * Moncton Times and Transcript; * Globe and Mail

Harsher measures sought by province - Swan urges action on home invasions, knife crimes
Harsher penalties for thugs convicted of home invasions, carjackings and premeditated knife crimes are on Justice Minister Andrew Swan's shopping list as he and his federal and provincial counterparts meet in Charlottetown next week. Swan said Friday he will urge Ottawa to amend the Criminal Code to make home invasions and carjackings stand-alone offences to reflect the seriousness of the crimes. The Manitoba minister is also seeking to make it a federal offence to wear body armour and to fortify buildings and vehicles. **By Friday afternoon, Public Safety Minister Vic Toews had caught wind of Swan's requests. At a news conference in Ottawa, Toews implied that he supported more mandatory sentences -- although he didn't make any promises on the issue. Provincial justice ministers realize Ottawa's crime-fighting policies are working, Toews said. *"This will result in a safer Canada."* The federal minister couldn't resist a swipe at the NDP official opposition in Ottawa, which has not supported the mandatory minimums in recent federal crime bills. *"This is an NDP attorney general who is calling for more mandatory minimums,"* Toews said of Swan. *"This is certainly not in keeping with what his federal counterparts are saying."*** Winnipeg Free Press, A10; * Moncton Times and Transcript (Calgary Herald)

Border agency nets three more on most-wanted list - Immigration: Two surrendered voluntarily this week
Three more of the Canada Border Services Agency's most-wanted fugitives have been caught, with two surrendering voluntarily. **Public Safety Minister Vic Toews announced the arrests Friday.** Delson Jules turned himself in to CBSA authorities at Montreal's Pierre Elliott Trudeau Airport on Tuesday. Originally from Haiti, he was convicted in Canada of criminal harassment, uttering threats and assault. On Wednesday, Namibian national Christa Kozonguizi turned herself in to CBSA officials at the Greater Toronto Enforcement Centre. She is considered inadmissible to Canada based on "security grounds." A tip from the public led to the apprehension Wednesday of Damien Rami Butler, originally from Jamaica. The RCMP arrested him in the Greater Toronto Area and turned him over to local authorities. Butler has been convicted of a number of charges including trafficking. Meanwhile, Haitian national Jameson Seide was deported on Tuesday, the eighth man from the CBSA's most wanted list to be sent home. So far, 18 people on the CBSA's list have been located. Over 30 people on the list remain at large. Kingston Whig-Standard, 9 (Winnipeg Sun; London Free Press); Saskatoon Star-Phoenix; * Toronto Sun

Ottawa battles over jurisdiction in Rwanda case
The Federal Court of Canada, not Quebec Superior Court, has the jurisdiction to rule on Leon Mugesera's last-ditch attempt to stop his deportation from Canada, a federal government lawyer argued Friday. Mugesera, who has been in

Canada for almost 20 years but is wanted in his native Rwanda for inciting the 1994 genocide, wants Quebec Superior Court to put his deportation on hold until the United Nations Committee Against Torture can review the case. **Lisa Maziade argued Mugesera's case has been exhaustively analyzed by the public safety minister**, the Supreme Court and the Federal Court, and all have ruled the 59-year-old should leave Canada. Besides, she said, the decision of the UN commit-tee would not be binding. Edmonton Journal, A11; * Montreal Gazette; * Journal de Montréal; * La Tribune - Sherbrooke

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Naval espionage suspect fed phoney secrets – source
Authorities fed an alleged and unwitting Canadian naval spy fabricated information as part of a classic "sour milk" counter-intelligence ploy to taint the credibility of secrets the man is suspected of passing to Russia, the Ottawa Citizen has learned. "This was done by the book - sour the milk so that you confuse the other side," Michel Juneau-Katsuya, a former spy service counter-intelligence officer with sources close to the Halifax case, revealed in an interview Friday. Once naval officials suspected there was a spy in their midst, deliberately flawed information was baited and designed to eventually be discovered by its foreign recipients, casting doubt the usefulness of any other classified data related to the case. While military and RCMP investigators are still gathering details, Juneau-Katsuya said he believes Russia may have been after North Atlantic Treaty Organization secrets. Victoria Times-Colonist, A11 (Winnipeg Free Press; Vancouver Sun; Fredericton Daily Gleaner; Edmonton Journal)

Expert: Canada wise to play down spy scandal – ESPIONAGE
Foreign Affairs Minister John Baird's refusal to comment on reported expulsions of Russian Embassy personnel over an alleged spy scandal doesn't surprise one political science expert at Royal Military College and Queen's University. Christian Leuprecht says the prime suspect in the espionage case, Sub-Lt. Jeffrey Delisle, is a low-ranking individual -- and even if allegations he leaked secrets are true -- long-term surveillance would probably have kept really damaging information from falling into the wrong hands. Leuprecht noted Canada needs its relationship with Russia, especially if it hopes to coax Moscow to take a tougher line on Iran and Syria. "If you want Russia on side, we're not going to blow this out of proportion," he said. Kingston Whig-Standard, 9 (Winnipeg Sun; Toronto Sun; London Free Press; Edmonton Sun)

Canada, Russia in 'Cold War lite' - Frosty relations between countries hamper closer ties, trade: observers
Canada and Russia are waging a "Cold War lite" two decades after the fall of the Berlin Wall, experts say, following news that a Canadian naval officer was slapped with espionage charges and accused of selling top-secret information to a foreign entity. Professor Piotr Dutkiewicz, director of the Institute of European and Russian Studies at Carleton University, said the Harper government's thinking toward Russia is outmoded. "The Canadian government is stuck in a Cold-War mentality," he said. "We now have a Cold War lite." Although official diplomatic relations have proceeded steadily under the Harper government, there is a layer of frost on the relationship that is hampering closer ties and more trade, observers say. Moncton Times and Transcript, D4 (Montreal Gazette)

The spies among us - Even if Sub-Lt. Jeffrey Paul Delisle is found guilty of passing on secrets, the most sensitive details will likely stay under wraps
The allegations against Sub-Lt. Jeffrey Paul Delisle are the stuff of great spy novels. But what we know of the naval intelligence officer thus far is maddeningly mundane. The charges are grave, though few specifics of the government's case against him are known. Delisle is accused of having passed Canadian secrets to some foreign agency - reports have said Russia - starting in July 2007 and lasting through to last Friday, Jan. 13. He was arrested that day on criminal breach of trust charges and was charged on Jan. 14 with violating the federal Security of Information Act, a law brought in after the 9/11 attacks. If true, his case could become one of the most significant espionage plots in modern Canadian history. So how did a self-described "proud parent" of a teenage girl and two preteen boys get caught up in an alleged spying plot worthy of a Hollywood film? The possible reasons, as history shows us, are endless. Toronto Star, IN1

Putin's People - The Russian PM's circle supports the use of spying as a way to increase the country's international power
Russian spies haven't been this visibly active since the height of the Cold War. "Much of this goes on sub rosa and never comes to public view," said Wesley Wark, a University of Toronto security expert. "But the general view is that the post-Soviet Russian state remains wedded to a very intensive overseas intelligence collection effort. The Putin administration in particular seems extremely keen on investing in foreign intelligence, which is perhaps not very surprising, given his KGB background." (Mr. Putin is a former KGB spy, who was stationed in Dresden, East Germany, in 1985-90.) In fact, the scale of Russian spying has never really let up, despite the collapse of the Soviet Union 20 years ago. "As far as anyone can tell it has remained unchanged or even has increased since the end of the Cold War," said Prof. Wark. National Post, A16

Harkat lawyers take aim at security law - Revised certificate legislation leaves defendants in dark, team says

Lawyers for Ottawa's Mohamed Harkat have asked the Federal Court of Appeal to strike down the country's security certificate law for a second time. The Harkat case will be the first to test whether the government's revised security certificate law can withstand a challenge under the Canadian Charter of Rights and Freedoms. The previous version of the law, used to deport foreign-born terror suspects, was ruled unconstitutional by the Supreme Court in February 2007. In that ruling, Canada's high court said the security certificate process was so secretive that it denied defendants the fundamental right to meet the case against them. The government subsequently introduced a new law, which gave terror suspects the right to be represented in secret hearings by "special advocates" - defence lawyers with security clearance. Special advocates are allowed only limited contact with the accused. Harkat's legal team contends the new law still leaves defendants too much in the dark. Ottawa Citizen, D4

It's time to list Iran's Revolutionary Guard as terrorists
An opinion piece from MP Irwin Cotler states "Iran's Supreme Court has now confirmed the death sentence of Iranian-born web programmer Saeed Malekpour, a Canadian permanent resident. Malekpour was convicted of "crimes against Islam" and "spreading corruption on Earth" - which have emerged as classic trumped-up charges in the Iranian pattern of the criminalization of innocence. This case should serve as the wake-up call that the Canadian needs to sanction the IRGC and list it as a terrorist entity. The United States has already labelled it as a terrorist group, while the UN and EU have imposed various sanctions against the IRGC and its leaders. It is regrettable that Canada continues to dither with regard to listing it as a terrorist entity here in Canada. The hope is that pressure from the international community may yet convince Iran to drop the false charges in this case and free Malekpour - allowing him to return to Canada. But however this case ends, the time has come to sanction the IRGC, and list it as a terrorist entity." National Post, A18

CYBER SECURITY / CYBERSÉCURITÉ

The day the web went dark - U.S. anti-piracy bills spark outrage online
. The Issue: Many of the Internet's most-used websites went dark on Wednesday to protest the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA), anti-piracy bills currently wending their way through U.S. Congress. The protest appeared to work with impressive efficiency - many proponents withdrew support for the bills, seen as deeply flawed. While Google's dramatic blacked-out logo was visible only to U.S. users, the self-imposed disabling of major sites such as Wikipedia affected users worldwide, including Canadians. Toronto Star, IN2; Charlottetown Guardian (Red Deer Advocate; Winnipeg Free Press)

Des pirates s'en prennent au FBI
La fermeture jeudi par les États-Unis du site de téléchargement Megaupload a entraîné depuis 48 heures une série de contre-attaques de pirates informatiques. Le Federal Bureau of Investigation (FBI), le ministère de la Justice et le palais présidentiel français ont tous été touchés par le mouvement Anonymous. Hier, la police néo-zélandaise a procédé à l'arrestation de quatre personnes reliées au site de partages de fichiers Megaupload. Kim Dotcom (de son vrai nom Kim Schmitz), l'ancien président et chef de la direction de Megaupload, fait partie des suspects arrêtés. Avec 150 millions d'utilisateurs et 50 millions de téléchargements chaque jour, Megaupload trônait parmi les sites les plus achalandés. Mais son contenu - musique, films, séries télé - était jugé illégal et violait les droits d'auteur. Le Soleil, 24; Victoria Times-Colonist; Toronto Star; National Post; Montreal Gazette; Le Devoir

Megaupload et Anonymous
Megaupload était l'un des sites de partage de fichiers les plus notoires au monde avec 150 millions d'utilisateurs. Son fondateur, Kim Dotcom, avait gagné 42 millions $US l'an dernier. Pour l'industrie cinématographique, le site fonctionnait avec des fichiers piratés. Le site a été fermé jeudi et est accusé d'avoir facilité le téléchargement illégal de plusieurs millions de fichiers, violant les droits de leurs auteurs. Le groupe de pirates informatiques Anonymous se présente comme un défenseur des libertés sur Internet. Le blocage de ces sites est la dernière cyberattaque d'Anonymous, un groupe de pirates disséminés dans le monde entier et représentés par un masque blanc et noir au sourire sarcastique, qui s'en est déjà pris à l'Église de scientologie ou au ministère de la Défense syrien. Le Soleil, 25

LAW ENFORCEMENT AND POLICING BRANCH / SECTEUR DE LA POLICE ET DE L'APPLICATION DE LA LOI

Heavy-handed G20 cops may face charges - Nobody has no plans to turn his other unbroken cheek, or reconstructed nose
A man arrested by police at the turbulent G20 summit 18 months ago is calling for criminal charges against the officers in light of a new report that finds they used excessive force against him. The report by the agency that investigates complaints against police concludes Adam Nobody, who was arrested at the provincial legislature in June 2010, made

substantiated allegations. The report calls on Chief Bill Blair to lay Police Act charges against five officers. "They beat me up tremendously bad," Nobody, 28, said in an interview Friday. "I had another human being stepping on my face, grinding my face into the ground. It's appalling." The report by the Office of the Independent Police Review Director names constables Babak Andalib-Goortani, Michael Adams, Geoffrey Fardell, David Donaldson and Oliver Simpson. It concludes their behaviour hurt the reputation of the police force and was of a "serious nature." Hamilton Spectator, A10 (Red Deer Advocate; Charlottetown Guardian; Halifax Chronicle-Herald); La Voix de L'Est; * Toronto Star; * Toronto Sun; * National Post; * Globe and Mail

Dozens of female RCMP officers seek justice through class-action lawsuit
Lawyers are in the final stages of drafting documents to be filed in court as early as next week that are expected to set in motion a class-action lawsuit that threatens to further destabilize one of the most iconic institutions in the country - the Royal Canadian Mounted Police. At this point, 94 current and former female members of the force from every province have asked to join the suit that is seeking damages potentially in the tens of millions of dollars for alleged maltreatment on the job. It's expected the number of women involved in the action will eventually be well over 100. Regardless of its outcome, the lawsuit, and the vast array of ugly harassment-related charges contained within it, is likely to provoke profound changes within the walls of an organization whose reputation has been shattered in recent years. New RCMP Commissioner Bob Paulson has vowed to investigate all harassment complaints thoroughly and take a zero-tolerance attitude towards workplace abuse going forward. Globe and Mail, S1

Mafia used list to deal: source - Duchesneau recalls working with officer, describes him as one of 'safest guys'
The list of police informants stolen by a retired intelligence officer in the Montreal police force was used as a bargaining chip by mafia lawyers to get reduced sentences for their clients, according to a source close to the investigation. The source told The Gazette that retired police officer Ian Davidson, who was found dead in a Laval hotel room with his throat cut, had tried to shop the list of 2,000 informants to the mafia. He said police were able to seize the list and claimed that no informant names were compromised. Montreal Gazette, A8; Journal de Montréal; Red Deer Advocate (Charlottetown Guardian); La Presse; Toronto Sun

Des bombes artisanales découvertes - CRIME ORGANISÉ ASIATIQUE
Une dizaine de bombes de fabrication artisanale ont été découvertes par hasard, jeudi, lors d'une opération visant un réseau de stupéfiants lié au crime organisé asiatique et apparemment dirigé par un ex-associé des Hells Angels Salvatore Cazzetta. Les enquêteurs de la moralité et des stupéfiants de la région ouest de la police de Montréal s'attendaient à trouver de la drogue et au moins un locataire lorsqu'ils se sont présentés dans un duplex de la rue LaSalle, à Longueuil, jeudi soir. Mais à leur grande surprise, les limiers sont plutôt tombés sur une dizaine de bombes artisanales fabriquées avec des tuyaux, communément appelées pipebombs. Ils ont aussitôt fait évacuer l'immeuble et appelé les artificiers de la Sûreté du Québec qui ont désamorcé les engins. Journal de Montréal, 25

Defence wants to know why police weren't called
The lawyer defending a Mountie on trial in Red Deer for extortion repeatedly asked a witness on Friday, who said she was terrified of the officer, why she didn't report him to police. Jennifer Henschel, who was under cross-examination, said she didn't call the police because - he was the police. "Because he was an RCMP officer. He told me he could run people out of town," Henschel said on Friday. RCMP Const. Hoa Dong La, in a judge-alone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain, involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. La, 47, faces 15 counts altogether, including three counts of extortion, two of criminal harassment and 10 of mortgage fraud. Red Deer Advocate, A2

Judge needs more time to review material in RCMP case
Judge Nancy Orr says she needs more time to review the reams of material presented in the case of an RCMP officer here facing charges of assault and confinement. The case surrounds 37-year-old Constable Darren Doucette who was not in court. He was posted to administrative duties last year when he was charged with assaulting and confining in his police cruiser 19-year-old Donovan Fitzpatrick. Doucette was responding to a noise complaint on Main Street when four men in an apartment fled out a back door and he pursued. Fitzpatrick complained the officer used excessive force. The decision by the judge is pending Feb. 23. Charlottetown Guardian, A3

Gang war escalating, police warn - Man shot to death in Surrey Thursday was half-brother of Dhak member killed in October
One of two men gunned down in Surrey late Thursday was the half-brother of a Dhak associate shot to death there in October, The Vancouver Sun has learned. And police are bracing for more violence as the death toll rises in a bloody ongoing conflict between two rival groups of gangsters. Sgt. Bill Whelan, of the Combined Forces Special Enforcement Unit, said heads of organized crime and homicide teams met Friday to strategize about what to do in the after-math of a string of gang murders, including the execution at the Sheraton Wall Centre Tuesday of high-profile gangster Sandip (Dip) Duhre. Vancouver Sun, A13; Toronto Star; Edmonton Journal; Windsor Star

Ex-Mountie gets 3 years for child porn, sexual assault
A Vancouver man who had nearly 27,000 images of child pornography on his computer and who sexually assaulted a 14-year-old boy has been sentenced to three years, three months in jail. In December, Warren Robert Allen, 53, pleaded guilty to one count of possession of child porn for the purpose of distribution and one count of sexual assault. Allen was arrested in May 2010 during a police crackdown on child pornography that resulted in more than 200 charges being laid and 57 arrests in Canada and overseas. The mitigating factors in the case included that Allen, who served as an RCMP officer in Alberta from 1978 to 1984, has no prior criminal record and is a "very intelligent, high-functioning and high-achieving" man, said the judge. Calgary Herald, A6

RCMP issue ecstasy warning in Saskatchewan
Saskatchewan RCMP are warning residents to stay away from the street drug ecstasy following several deaths associated with the drug in neighbouring provinces. "Illegal drugs are conveyed across provincial and international borders and the public needs to be aware of the inherent dangers of ecstasy and other illegal drugs," the force says in a Friday news release. The B.C. Coroners Service has found the toxic compound paramethoxymetamphetamine (PMMA) in the victims of at least five people who died after taking ecstasy in the last six months, and other deaths are under investigation. Alberta has also seen ecstasy-related deaths in recent months. No such deaths have yet been reported in Saskatchewan, RCMP say. Saskatoon Star-Phoenix, A6

Canucks tip aussies in massive drug scheme
Four men alleged to be part of an international drug syndicate were arrested Friday in Australia after police were tipped off by Canadian border security. The Canada Border Services Agency discovered 6.1 kg of cocaine, 12.3 kg of Ecstasy and nearly two kilos of methamphetamine concealed in a shipping container full of ovens at Vancouver's port. CBSA officials alerted law enforcement in Australia, where the container was bound. Toronto Sun, 25

Dad charged
A father is facing now charges after his nine-year-old son was fatally shot by his older brother. RCMP arrested the 34-year-old Sagkeeng First Nation man on charges of unsafe storage of a firearm. His 14-year-old son got his hands on a loaded weapon and accidentally shot his nine-year-old brother Nov. 3. The boy later died in hospital. The father is scheduled to appear in court Feb. 22. Edmonton Sun, 26

Penalty killers - Police union, brass drag their feet on charges
An opinion piece states “Running out the clock. With there being no one in power who seems to care, it's a strategy that's working. It's not just the Toronto Police Association ragging the puck but the chief, the board and politicians who oversee them too. The result is police do not seem accountable. The bottom line is police, as shown by routinely not co-operating with the Special Investigations Unit, don't seem to want to be accountable. The CBC's Dave Seglins broke the story that ‘Ontario's top police complaints watchdog has concluded five officers involved in the now infamous arrest of G20 protester Adam Nobody should be charged with misconduct for using unnecessary force and for discreditable conduct.’ Good cops need bad cops gone quickly but the sand in this hour-glass is moving slow. Justice delayed is justice denied after all. Perhaps Premier Dalton McGuinty or Mayor Ford could take some action but neither are that stupid or brave.” Toronto Sun, 6

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Pickton inquiry head frustrated by slow pace
In the past week, lawyers for more than half a dozen current and former Vancouver police and RCMP officers have joined the hearings, arguing their clients' reputations have been put at stake by a report that criticized how both forces investigated missing women and Pickton. The collection of high-profile criminal lawyers all asked to cross-examine the author of that report, Peel Regional Police Deputy Chief Jennifer Evans, who conducted an external review for the commission. Evans has already been on the stand for five days, and the officers' lawyers want another week with her. Commissioner Wally Oppal, who has until June 30 to complete his report into why Pickton wasn't caught, appeared exasperated Friday as he acceded to the request. "The courts get bogged down by lengthy submissions and lengthy arguments and lengthy trials, and we're falling into the same trap here." Oppal said. Halifax Chronicle-Herald, B2

Police foresaw Pickton inquiry - Bungled investigative efforts noted in 2000
It was April 2000, the height of Robert "Willie" Pickton's killing spree. Dozens of women were already missing, and 23 more would vanish. Pickton was by then a prime police suspect. Documents disclosed recently at the Missing Women Inquiry of Commission in Vancouver offer stunning details of what police knew - or thought they knew - and what some officers didn't seem to want to know. Perhaps most telling, on April 25, 2000, RCMP officers were already discussing the possibility that bungled police efforts would lead to a public inquiry. National Post, A1

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

"Une histoire kafkaïenne", dénonce Hassan Diab
Accusé d'avoir proféré un attentat terroriste en France, dans les années 1980, Hassan Diab a parlé publiquement pour la première fois depuis son arrestation. Une vingtaine de manifestants ont voulu présenter une pétition de 650 noms au ministre de la Justice, Rob Nicholson, pour réclamer l'annulation de l'extradition de M. Diab vers la France. Selon les partisans de l'accusé, M. Diab est victime d'une méprise de la part du gouvernement français. L'"attentat de la rue Copernic" est resté gravé dans la mémoire des Français. Le groupe de manifestants réclame au passage une réforme de la loi canadienne sur l'extradition, qui devrait inclure la notion de présomption d'innocence, le droit à un procès équitable et à la divulgation de la preuve. Le Droit, 9; * Ottawa Sun; * Edmonton Journal; * Le Devoir

Whistleblowing Mexican author fears death if forced back home
A Mexican journalist fears she and her family could be killed if they are forced to leave Canada. Karla Berenice Garcia Ramirez, who sought asylum in Canada in 2008 with her husband, says threats against her life intensified after she wrote a book alleging corruption at a Mexican government ministry where she once worked. Ramirez's refugee status application was rejected in 2010. Last November, the government conducted a pre-removal risk assessment and issued a deportation order, said Lobat Sadrehashemi, one of Ramirez's lawyers. Ramirez and her husband have filed an application to remain in Canada on humanitarian grounds and are seeking a Federal Court review of the recent risk-assessment decision. Winnipeg Free Press, A22 (Vancouver Sun)

Jamaican tot found dead in suitcase
Canadian police help has been requested following the arrests in Jamaica of a Scarborough woman and her deportee husband after the remains of a two-year-old boy was found stuffed in a suitcase. Stephanie Warren, 34, a Canadian citizen, who last lived on Tuxedo Crt., and her husband, Alfanso, 32, are being detained in a Kingston jail and charges are pending, Jamaica Constabulary Force spokesman Karl Angell said on Friday. Angell said his officials have been in touch with the High Commission of Canada in Jamaica to request help from police here in probing the background of the couple, who lived in the Ellesmere and Markham Rds. area for years before returning to Jamaica. Toronto Sun, 10

Menottés à l'arrivée
Entre leur arrivée au Canada et le traitement de leur dossier, plusieurs milliers de demandeurs d'asile passent chaque année par la «case détention». Une expérience de routine pour le gouvernement canadien. Un traumatisme pour ceux qui sont emprisonnés, révèle une étude de l'Université McGill, la première du genre menée au Canada. Au moment où le gouvernement fédéral songe à systématiser la mise en détention des demandeurs d'asile et à en allonger la durée avec la loi C-4, ces résultats en inquiètent plusieurs. L'an dernier, plus de 4000 demandeurs d'asile sont passés par un centre de prévention de l'immigration, pour un séjour qui dure en moyenne 28 jours, selon l'Agence des services frontaliers du Canada (ASFC). Ces séjours ne sont pas sans laisser de traces sur la santé mentale des demandeurs d'asile. La Presse, A16

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Care and feeding of cows and inmates
An opinion piece states "In Kingston this week, in another courtroom in another courthouse far from where I was at the notorious Shafia honour-killing case, eight people went on trial for mischief. They are the holdouts from a group of 24 who were arrested in August of 2010 in protests to save the so-called 'prison farm' at the Frontenac Institution facility in this prison-heavy part of south-eastern Ontario. The judge will deliver his verdict next month. The eight had refused the chance to walk away with a charitable donation through a diversion program and demanded a trial: Essentially, they objected to the six prison farms once located at minimum-security institutions across the country (two near Kingston, and one each in New Brunswick, Manitoba, Saskatchewan and Alberta) being shut down by the federal government. The protesters failed - the Frontenac dairy herd was eventually trucked away and sold - just as those who fought to save the other farms failed." National Post, A4

INTERNATIONAL / INTERNATIONAL

Explosions rock Nigeria's Kano, at least six killed

At least six people were killed in a string of bomb blasts on Friday in Nigeria's second city Kano and the authorities imposed a curfew across the city, which has been plagued by an insurgency led by the Islamist sect Boko Haram. Kano, like other northern cities in Nigeria, has been plagued by an insurgency led by Islamist sect Boko Haram, blamed for scores of bombings and shootings against mostly government targets that are growing in scale and sophistication. Kingston Whig-Standard, 12

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

Klassen, Nathan

From: Klassen, Nathan
Sent: January-20-12 9:37 AM
To: Anderson, Windy
Cc: Bendelier, Kenneth
Subject: Weekly work plan -- January 23 to January 27 -- 2012 -- Nate Klassen

Hi Windy / Ken

Here is my tentative work plan for January 23 - 27. The review for the past week is also below. Cheers,

Nate

Weekly Work Plan (January. 23 - January. 27):

1. ***PIA***
   - ***a.*** Start working on section 6 of the PIA – the PIA is my priority for January;
   - ***b.*** Once received -- input comments from Bud, Rob, Ken, ATIP, and PS legal into the draft; and
   - c. Start briefing note for LC;

2. ***Situational Awareness***
   - a. Produce weekly stats report WRT CCIRC's products – use the new template;
   - b. Explore using publication tool for stat report / posting stat report on the portal on a monthly basis;
   - c. Provide comments on the weekly SA report;
   - d. Create decks / briefs as required by Windy / Ken; and
   - *e.* Help out on any other SA product as determined by Windy / Ken.

3. ***Other***
   - ***a.*** Continue to get up to speed WRT CCIRC

Last week in review (January. 16 – January 20):

1. ***PIA***
   - a. Start working on section 5 of the PIA – the PIA is my priority for January; -- Finished and circulated for comments
   - b. Circulate sections 1-4 of PIA to Ken / Bud / Rob / PS legal / PS ATIP for comment; and -- Finished and circulated for comments
   - c. Contact PS document management to: (1) set up CCIRC 'retention schedule; and (2) obtain Record Disposition Authority from the Librarian and Archivist of Canada – Contacted PS document management and they are in the process of providing us the required information.

2. ***Situational Awareness***
   - f. Produce weekly stats report WRT CCIRC's products -- Done
   - g. Provide comments on the weekly SA report; -- Done, provided Rana with comments
   - h. Fixed the 1 page feedback form we will circulate with our new weekly product;
   - i. Wrote two briefs – Israeli – Palestine 'cyber war' and Anonymous attacks on US Government and private sector
   - j. Set up meeting with RCMP

3. ***Other***
   - a. Continue to get up to speed WRT CCIRC;
   - b. Send training request for next fiscal year to Ken -- Done

Nathan Klassen
Canadian Cyber Incident Response Centre

Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Klassen, Nathan

From: Murphy, Gregg
Sent: January-20-12 1:09 PM
To: Klassen, Nathan
Subject: RE: Brief

Tar sands;

Anonymous also announced "Operation Green Rights/Project Tarmaggedon," against Exxon Mobil, ConocoPhillips, Canada Oil Sands, Imperial Oil, the Royal Bank of Scotland, and others. http://news.cnet.com/8301-27080_3-20078963-245/anonymous-targets-monsanto-oil-firms/

-----Original Message-----
From: Klassen, Nathan
Sent: January-20-12 1:05 PM
To: St-Louis, Danielle
Cc: Murphy, Gregg
Subject: Brief

Hi Danielle,

Today's brief for RD is attached. Ken and Luc are happy with the final product. Could you please read it over for grammar / spacing J / ect? Once done please prepare the official brief and send it over. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca <mailto:Nathan.Klassen@ps-sp.gc.ca>

Klassen, Nathan

From: Bendelier, Kenneth
Sent: January-20-12 11:58 AM
To: Klassen, Nathan; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Re: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Good.

Send.

From: Klassen, Nathan
Sent: Friday, January 20, 2012 11:45 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Hi Ken and Luc,

The requested brief is attached. Comments due by 1:30 PM today in order to get this to RD before the weekend. FYI, Gregg has reviewed the draft and he is happy with it. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Bendelier, Kenneth

From: Klassen, Nathan
Sent: January-20-12 11:46 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today
Attachments: PS-SP-#549586-R-Briefing_Note_-_HACKERS_ATTACK_UNITED_STATES_GOVERNMENT_AND_PRIVATE_SECTOR_WEB_SITES_-_to_DG_-_2012_-01-20.DOC.DRF

☺

From: Klassen, Nathan
Sent: January-20-12 11:46 AM
To: Bendelier, Kenneth; Beaudoin, Luc S
Cc: Murphy, Gregg
Subject: Briefing note -- Anonymous attacks -- Comments due by 1:30 PM today

Hi Ken and Luc,

The requested brief is attached. Comments due by 1:30 PM today in order to get this to RD before the weekend. FYI, Gregg has reviewed the draft and he is happy with it. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

Klassen, Nathan

From: Klassen, Nathan
Sent: January-20-12 1:05 PM
To: St-Louis, Danielle
Cc: Murphy, Gregg
Subject: Brief
Attachments: PS-SP-#549586-R-Briefing_Note_-_HACKERS_ATTACK_UNITED_STATES_GOVERNMENT_AND_PRIVATE_SECTOR_WEB_SITES_-_to_DG_-_2012_-01-20.DOC.DRF

Hi Danielle,

Today's brief for RD is attached. Ken and Luc are happy with the final product. Could you please read it over for grammar / spacing ☺ / ect? Once done please prepare the official brief and send it over. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

Weir, Sarah

From: Fortunato, Stephanie
Sent: January-20-12 4:31 PM
To: St-Louis, Danielle
Cc: Weir, Sarah
Subject: RE: Memo to DG: Hackers Attack United States Government and Private sector Websites

Hey!

Robert just read it, he'd like us to send it to the DM on Monday morning. There are a few changes that need to be made. First of all, after FBI in the background section, there should not be any punctuation. Also, in the 3rd paragraph under the consideration header, the word "internet" should be spelt "Internet". Please make these changes and then have the memo signed by the acting Director on Monday.

Thanks!!

Steph

From: St-Louis, Danielle
Sent: January-20-12 4:22 PM
To: Fortunato, Stephanie
Cc: Klassen, Nathan; Murphy, Gregg; Bendelier, Kenneth
Subject: Memo to DG: Hackers Attack United States Government and Private sector Websites

As discussed. please show to Robert and we will have it sent to DGO formally on Monday.
If you have any questions, please let me know. Have a nice weekend!

Thank you Steph

Danielle St-Louis
Administrative Assistant | Adjointe administrative
Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: **613-991-7738** Fax | Téléc.: 613-991-3574
E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

CCIRC is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

UNCLASSIFIED

DATE: January 20, 2012

File No.: 385245
RDIMS No.: 549586

MEMORANDUM FOR THE DIRECTOR GENERAL

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEB SITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) web sites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of, Friday, January 20th most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these web sites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, Canadian Cyber Incident Response Centre
National Cyber Security

Prepared by: Nate Klassen
Gregg Murphy

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:

File No.: 385262
RDIMS No.: 550276

MEMORANDUM FOR THE DEPUTY MINISTER

HACKERS ATTACK UNITED STATES GOVERNMENT AND PRIVATE SECTOR WEBSITES

(Information only)

ISSUE

Hackers attacked and disrupted the following United States' (U.S.) websites: Department of Justice, Federal Bureau of Investigation (FBI), Universal Music Group, Recording Industry Association of America, Motion Picture Association of America, and Warner Music Group.

BACKGROUND

Media reports that on Thursday, January 19, 2012, the U.S. Justice Department and the FBI seized the website 'Megaupload' due to Internet piracy concerns. In retaliation, and within a matter of minutes, the hacker group, Anonymous, reportedly prevented access to many important U.S. websites. As of Friday, January 20, 2012, most of these websites were back online.

CONSIDERATIONS

There are three Canadian considerations regarding this incident.

First, Canadian citizens may have unknowingly participated in the attacks against these websites. Media reports that Anonymous set up a link on the Internet that would automatically launch an attack against targeted sites if clicked (e.g. if unsuspecting Canadians clicked this link their computer would automatically participate in the attacks).

Second, Canada may become a future target for Anonymous as it is in the process of reviewing its Internet legislation in order to strengthen its copy right laws (Bill C-32). Canada has been previously targeted by Anonymous (tar sands and Occupy Wall Street).

.../2

Third, this incident demonstrates the speed and reach with which Anonymous can operate. As such, if they decide to target Canada they could quite rapidly disrupt Canadian sites.

NEXT STEPS

The Canadian Cyber Incident Response Centre is continuing to monitor the situation and will inform senior management of any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Gregg Murphy

Klassen, Nathan

From: Murphy, Gregg
Sent: January-20-12 10:54 AM
To: Klassen, Nathan
Subject: Anonymous

http://www.kctv5.com/story/16558352/anonymous-takes-down-doj-fbi-sites
http://www.firstpost.com/tech/fbi-shuts-down-megaupload-com-anonymous-shut-down-fbi-188266.html

"Federal officials confirmed it was down on Thursday evening and that the disruption was being "treated as a malicious act." " This is all I have as far as confirmation...

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-20-12 8:42 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; [redacted] Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; [redacted] Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; [redacted] Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; [redacted] Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; [redacted] Houston, Laura; Jones, Scott; [redacted] Labelle, Sébastien; Labossiere, Alain; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; [redacted] Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 20, 2012/ le 20 janvier 2012

Print Media

Le FBI ferme le site Megaupload
La justice américaine a ordonné hier la fermeture du site Megaupload.com, plateforme emblématique et controversée du téléchargement direct sur Internet, accusé de violation des droits d'auteur, s'attirant aussitôt une cyberattaque des pirates d'Anonymous. Quatre responsables du site basé à Hong Kong, dont son fondateur, Kim Dotcom, 37 ans, ont été interpellés à Auckland, en Nouvelle-Zélande, sur la base de mandats d'arrêt délivrés par les États-Unis. Le FBI (police fédérale américaine) et le ministère de la Justice américain ont estimé, dans un communiqué commun, qu'il s'agissait de l'une des plus "grandes affaires de violation de droits d'auteur jamais traitées aux États-Unis". Journal de Montréal

Hackers attack FBI, Justice Department websites after Megaupload shutdown
Minutes after the U.S. Department of Justice shut down notorious file-sharing site Megaupload.com, the department's own website was brought down in a cyber attack orchestrated by the hacker group Anonymous. "The government takes down Megaupload? 15 minutes later Anonymous takes down government & record label sites," a member of Anonymous said via Twitter. The group also disabled the sites of Universal Music, the RIAA, the U.S. Copyright Office, Broadcast

Music Inc., the FBI and the Motion Picture Association of America in what it called its "largest attack ever." By late evening, however, most sites were back online. National Post

The evasive 'Koobface gang' - Despite Facebook publicizing their names and faces, the Russian cyber criminals have yet to be brought to justice, Christopher Williams reports
Facebook took a very unusual step for a multinational web company this week, when it publicly accused five Russian men of running a multi-million-dollar scam against hundreds of thousands of its users. The "Koobface gang", as the quintet is known to Internet security experts, stand accused of infecting social network users' computers with a malicious software "worm". The global network of up to 800,000 remotely-controlled machines became a lucrative business for the gang. Other cyber criminals would pay them to bombard their victims with ads for fake antivirus software, or to hijack searches to deliver traffic to rogue pharmacy websites. Ottawa Citizen

If Wiki were wishes, trolls might surf
An opinion piece states "In the crosshairs are two bills introduced before Congress last year - the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA) - that would give content owners the legal tools with which to choke off business to sites they claim infringe on their rights. The proposed Acts are ludicrously blunt instruments that are far more likely to damage the myopic lawmakers who now support them rather than a 'free and open Internet.' Beyond this, they are virtually unenforceable, and any law that can't be enforced gets what it deserves: It gets ignored as tens of thousands of online denizens operate their various workarounds to popular acclaim." Moncton Times and Transcript

Copyright debate moving north
An opinion piece states "If you tried to use Wikipedia Wednesday and were met by a black screen with the chilling caution 'Imagine a World Without Free Knowledge,' welcome to the world of copyright debate. That debate is peaking in the U.S. Congress, where two proposed laws would force Internet providers to shut down 'pirate' sites selling illegal movies, music or books -- cutting off those sites, refusing to accept advertising from them and disabling any payment processing links. The crackdown is necessary. Free knowledge doesn't include freedom to break the law. Canada's proposed new copyright law takes a halfway approach. Internet providers would have to inform customers they have downloaded illegal material. That's a potentially effective approach, but if it doesn't work, something closer to the U.S. model will be necessary." Winnipeg Sun

Digital intruders have been warned
An editorial states "The Ontario Court of Appeal's decision on Wednesday recognizing a right to sue for damages for outrageous violations of privacy is a good example of sensible judicial innovation. It is an adaptation that reflects life in the digital age. Laws against trespass, breaking and entering, burglary, and unreasonable search and seizure - protecting bricks-and-mortar rights, one might say - remain very important, but the same principles that underlie those older rights need to be complemented, in order to deal in an analogous way with what Mr. Justice Robert Sharpe - who wrote the three-judge panel's decision - calls informational privacy. The result is a new tort - that is, the civil-lawsuit equivalent of a crime - by the name of 'intrusion upon seclusion.'" Globe and Mail

Online Media

Anonymous goes nuclear; everybody loses?
An opinion piece states "In the aftermath of Wednesday's SOPA/PIPA blackout protests, the Internet community amassed quite a bit of goodwill, flexed its muscles in a friendly, humorous, civil-disobedience kind of way, and, remarkably, even managed to change quite a few minds. Just 24 short hours later, Anonymous legions nuked that goodwill and took cyber security into thermonuclear territory. The real question now is: were they played? As I write this, #OpMegaUpload is in full effect. The Internet is seemingly coming down all around me. Global Internet traffic is fluctuating between 13 percent and 14 percent above normal, and, as you can see from the above image, global network attacks were up 24 percent. Affected sites include the White House, the FBI, the Department of Justice, multiple record label sites, the MPAA, and RIAA, and the U.S. Copyright Office." CNET

Google Expands Hacked Sites Label In Search Results
A year ago, Google began labeling hacked sites and sites with malware as sites that may compromised in the search results snippets. Yesterday, Google's Matt Cutts announced on Google+ that Google has expanded that feature. Matt said the change they just launched will "expand our [Google's] coverage of labeling search result pages." Search Engine Roundtable

Spammers target childrens' games
With adults wising up to the dangers of clicking unknown links, spammers are increasingly targeting children. Anti-virus firm Avast says it's identified more than 60 individual sites during the last month containing 'game' or 'arcade' in their URL

address, all aimed squarely at children. The most visited site was cutearcade.com, a collection of online games with dressing up and coloring games - and even Hello Kitty. Avast says its users have reported an infection at this site over 12,600 times. The malicious Trojan redirects viewers to linuxstabs.com, a known distribution point for malware. TG Daily

Facebook users targeted by transformed Carberp Trojan

A new form of the Carberp Trojan, which tricks users into committing financial fraud via e-cash vouchers, is now targeting Facebook users, according to researchers at Trusteer. The malware is used in a man-in-the-browser (MitB) attack, which exploits the trust users have with Facebook and the anonymity of e-cash vouchers, wrote Amit Klein, CTO of Trusteer, in a recent blog post about the Carberp Trojan. Klein said the Trojan replaces a Facebook page with a fake page that notifies users that their account has been "temporarily locked" and can be unlocked by providing personal information and an e-cash voucher worth approximately $25. Search Security

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

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-20-12 8:07 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 20, 2012 / le 20 janvier 2012

MINISTER / MINISTRE

Top Mountie gagged: senator
A Liberal senator is accusing the government of trying to "muzzle" the RCMP commissioner after learning of guidelines that require all meetings between the top officer and parliamentarians to be approved first by government officials. Internal emails obtained by Postmedia News show that when Senator Colin Kenny attempted to schedule a meeting recently with Commissioner Bob Paulson, Paulson replied, "I apologize for any delay, but I've become aware of some guidelines from the **Department of Public Safety** in terms of engaging with Parliamentarians and Senators and so I may have to respectfully ask you to route your request for a meeting through the Minister's Office or the Department." Kenny said in an interview Thursday that the government was improperly trying to muzzle a senior public servant and that the guidelines will have the effect of shutting down communication between parliamentarians and officials. **Julie Carmichael, a spokeswoman for Public Safety Minister Vic Toews**, said in a statement that allegations the commissioner is being muzzled are "***baseless and inaccurate***" and that it is "***standard practice across government to ensure a co-ordinated approach between departments and agencies.***" Ottawa Citizen, A1 (National Post, Starphoenix, Montreal Gazette, Calgary Herald, Vancouver Sun); Hamilton Spectator (Red Deer Advocate)

Mounties on tight leash: MPs, senators wishing to meet RCMP brass must go through Toews
The federal Conservatives are directly exerting strict communications control over the RCMP and its new top cop, documents obtained by the Star reveal. Documents released under Access to Information show top political staff of **Public Safety Minister Vic Toews** oversaw and approved the design of a new RCMP communications protocol that put the national police force on a tighter leash. As the Star first reported, that protocol requires the RCMP to flag anything that might "garner national media attention" to **Public Safety Canada**. New **Public Safety** documents show **Toews's** office had a direct hand in crafting the policy, working with the RCMP's new public affairs director - Daniel Lavoie - a former associate assistant deputy minister in **Toews'** department. Lavoie, who moved to the RCMP from **Public Safety** last summer, advised former colleagues that implementing the new protocol "will require a change of mentality" at the RCMP, even though the force was already flagging important media issues to the government. Lavoie's emails show he met with outgoing RCMP boss William Elliott as the protocol was developed. None of the emails suggests Lavoie or Elliott raised any concerns about the RCMP's independence. The documents show it was developed under the watchful eyes of **Toews's chief of staff Andrew House and communications director Michael Patton**, contrary to initial suggestions to the Star by Patton that he was unaware of a new policy. On top of that comes a new edict from **Toews's** office that requires Elliott's replacement, Commissioner Bob Paulson, to vet all his meetings with MPs and senators first through his political bosses. Paulson replied he'd since become aware of "guidelines" from the **Department of Public Safety** on his dealings with MPs and Senators. Toronto Star, A10

* **Pour un registre québécois**
«Nous préconisons le maintien du registre [des armes à feu]. Nous sommes convaincus que c'est indispensable.» Le dg de la Sûreté du Québec (SQ), Richard Deschesnes, fonde son opinion sur le fait que le registre que veut abolir le gouvernement Harper est consulté 711 fois par jour au Québec, tous corps policiers confondus. Avec 1,7 million d'armes enregistrées en province, la SQ veut savoir qui sont ceux qui les possèdent. «Prenez le cas de l'homme barricadé à Saint-Malachie, mercredi. Dans ce genre d'opération, il faut détenir cette information. C'est pourquoi nous appuyons **le ministre [de la Sécurité publique]** dans ses démarches auprès du gouvernement fédéral.» Québec tente de récupérer les données du registre que veut détruire Ottawa. Le Soleil, 3

* **Des enfants dans les centres de détention**
En moyenne, depuis 2005, au moins 430 enfants par année sont détenus dans des prisons canadiennes. Ce ne sont pourtant pas des criminels. Ce sont des demandeurs d'asile politique, qui sont détenus comme plusieurs milliers de leurs semblables, selon le pouvoir discrétionnaire d'un agent de l'Agence des services frontaliers du Canada. On dit 430

enfants, mais c'est peut-être beaucoup plus. Certains enfants ne sont pas comptabilisés dans les statistiques parce qu'ils accompagnent simplement en prison leurs parents demandeurs de statut. Bientôt, ces demandeurs de statut seront détenus pour une période d'un an ferme, sans possibilité de révision de détention, et sans accès à un tribunal, si le projet C-4 défendu par le gouvernement fédéral est adopté. Malheureusement, rien n'indique que **le ministre canadien de la Sécurité publique** fasse beaucoup mieux une fois C-4 adopté, s'inquiètent les chercheurs du CSSS de La Montagne, dans un mémoire qu'ils prévoient soumettre au Parlement sous peu. Le Devoir, A1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

La Nina could set stage for flu pandemic
Now, two U.S. scientists - Jeffrey Shaman at Columbia University and Marc Lipsitch at Harvard University's school of public health - have identified a climatic pattern that could set the stage for the emergence of a new and deadly strain of influenza. Globe and Mail, L6

*** Release data on Tamiflu**
An editorial states, "Over the past three years, Ontario has spent $26 million stockpiling Tamiflu to treat people in the event of a pandemic. During the last big scare - H1N1 in 2009 - there were shortages of the children's antiviral dose and cases of frantic parents racing between drug stores trying to fill what they believed could be a life-saving prescription. Around the world, the bill for this one drug has been in the billions as governments built up supplies..." Toronto Star, A18

*** Not prepared for emergencies**
In the wee hours of the morning, a water valve at the high school failed and most of the city's water supply spilled onto the ground, almost draining the reservoir. Millions and millions of gallons of water, flowing out into a dark and cold Arctic night in the middle of a community can make quite a mess. YellowKnifer

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Russian embassy staff expelled
The Harper government has expelled staff at Russia's embassy in the wake of charges filed against a Canadian military intelligence officer for allegedly passing secrets to a foreign power, The Globe and Mail has learned. The names of two Russian diplomats - including a defence attache - and two technical staff at the embassy have been dropped from the Department of Foreign Affairs' list of diplomatic, consular and foreign government representatives recognized by Ottawa. Globe and Mail, A1; Ottawa Citizen (Times Colonist); Toronto Star; London Free Press (Whig-Standard, Ottawa Sun, Calgary Sun, Edmonton Sun, Toronto Sun, Winnipeg Sun); * Winnipeg Sun (Edmonton Sun); * Winnipeg Free Press

Top court rejects Almalki appeal
Ottawa's Abdullah Almalki vows to continue his fight for justice after the Supreme Court of Canada rejected his bid to force the government to reveal more of its secrets. Almalki is one of three former terror suspects - all of whom were tortured in overseas prisons - suing the government for $180 million. Ottawa Citizen, A3; National Post (Windsor Star); * Hamilton Spectator; * La Presse (Le Droit)

*** The new age of local espionage has just begun**
An editorial states, "...By Monday, Halifax had become a hub - and a hubbub - of international intrigue as a 40-year-old naval intelligence officer was charged with passing along military secrets to a "foreign entity." In this instance, the latter is code for Russia. The Herald has confirmed this through its own spy network... Sub.-Lt. Jeffrey Paul Delisle worked at such a top-secret nerve centre in Halifax, dubbed Trinity. Even if the allegations against him stand up to scrutiny, we'll never know how much damage may have been done... If anything, analysts say there are more Russian spies deployed in North America now than there ever were. And the sort of tactical and strategic intelligence that can be gleaned from sites like Trinity would be of great value to a great power that still likes to play the Great Game... Expect more of the same as the shipbuilding contract gets into full swing. "Foreign entities" will be very interested in these ships' design, capabilities and components. Much of the high-end stuff will be developed out-of-province, but it will all have to be assembled here at some point. FYI, we aren't the only ones building a modern navy. So is Russia. So is China. Stealing technology is hardly beneath them, and there will always be well-placed people hanging around who are not above betraying their country." Chronicle-Herald, A9

*** PACKAGE WAS EXPLOSIVE**

A suspicious package that prompted London police to close a stretch of Southdale Rd. for almost four hours Wednesday contained an explosive device, police said. The package was found in an isolated wooded area in the southwest part of the city on Southdale near Wickerson Rd. The explosive disposal unit was called in. Police closed Southdale between Bramblewood Rd. and Wickerson from about 7:30 p.m. to 11:30 p.m. The device was destroyed and no one was injured. Police did not release details. London Free Press, A7

CYBER SECURITY / CYBERSÉCURITÉ

*** Le FBI ferme le site Megaupload**
La justice américaine a ordonné hier la fermeture du site Megaupload.com, plateforme emblématique et controversée du téléchargement direct sur Internet, accusé de violation des droits d'auteur, s'attirant aussitôt une cyberattaque des pirates d'Anonymous. Quatre responsables du site basé à Hong Kong, dont son fondateur, Kim Dotcom, 37 ans, ont été interpellés à Auckland, en Nouvelle-Zélande, sur la base de mandats d'arrêt délivrés par les États-Unis. Le FBI (police fédérale américaine) et le ministère de la Justice américain ont estimé, dans un communiqué commun, qu'il s'agissait de l'une des plus "grandes affaires de violation de droits d'auteur jamais traitées aux États-Unis". Journal de Montréal, 37; Halifax Chronicle-Herald; Toronto Sun

*** Hackers attack FBI, Justice Department websites after Megaupload shutdown**
Minutes after the U.S. Department of Justice shut down notorious file-sharing site Megaupload.com, the department's own website was brought down in a cyber attack orchestrated by the hacker group Anonymous. "The government takes down Megaupload? 15 minutes later Anonymous takes down government & record label sites," a member of Anonymous said via Twitter. The group also disabled the sites of Universal Music, the RIAA, the U.S. Copyright Office, Broadcast Music Inc., the FBI and the Motion Picture Association of America in what it called its "largest attack ever." By late evening, however, most sites were back online. National Post

*** The evasive 'Koobface gang' - Despite Facebook publicizing their names and faces, the Russian cyber criminals have yet to be brought to justice, Christopher Williams reports**
Facebook took a very unusual step for a multinational web company this week, when it publicly accused five Russian men of running a multi-million-dollar scam against hundreds of thousands of its users. The "Koobface gang", as the quintet is known to Internet security experts, stand accused of infecting social network users' computers with a malicious software "worm". The global network of up to 800,000 remotely-controlled machines became a lucrative business for the gang. Other cyber criminals would pay them to bombard their victims with ads for fake antivirus software, or to hijack searches to deliver traffic to rogue pharmacy websites. Ottawa Citizen, F9

*** If Wiki were wishes, trolls might surf**
An opinion piece states “In the crosshairs are two bills introduced before Congress last year - the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA) - that would give content owners the legal tools with which to choke off business to sites they claim infringe on their rights. The proposed Acts are ludicrously blunt instruments that are far more likely to damage the myopic lawmakers who now support them rather than a ‘free and open Internet.’ Beyond this, they are virtually unenforceable, and any law that can't be enforced gets what it deserves: It gets ignored as tens of thousands of online denizens operate their various workarounds to popular acclaim.” Moncton Times and Transcript, D6

*** Copyright debate moving north**
An opinion piece states “If you tried to use Wikipedia Wednesday and were met by a black screen with the chilling caution ‘Imagine a World Without Free Knowledge,’ welcome to the world of copyright debate. That debate is peaking in the U.S. Congress, where two proposed laws would force Internet providers to shut down ‘pirate’ sites selling illegal movies, music or books -- cutting off those sites, refusing to accept advertising from them and disabling any payment processing links. The crackdown is necessary. Free knowledge doesn't include freedom to break the law. Canada's proposed new copyright law takes a halfway approach. Internet providers would have to inform customers they have downloaded illegal material. That's a potentially effective approach, but if it doesn't work, something closer to the U.S. model will be necessary.” Winnipeg Sun, 10

*** Digital intruders have been warned**
An editorial states “The Ontario Court of Appeal's decision on Wednesday recognizing a right to sue for damages for outrageous violations of privacy is a good example of sensible judicial innovation. It is an adaptation that reflects life in the digital age. Laws against trespass, breaking and entering, burglary, and unreasonable search and seizure - protecting bricks-and-mortar rights, one might say - remain very important, but the same principles that underlie those older rights need to be complemented, in order to deal in an analogous way with what Mr. Justice Robert Sharpe - who wrote the

three-judge panel's decision - calls informational privacy. The result is a new tort - that is, the civil-lawsuit equivalent of a crime - by the name of 'intrusion upon seclusion.'" Globe and Mail, A12

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Tasers most likely to be used on 'downtrodden,' published study asserts
The use of Tasers by Canada's police forces represents a "teething new urban terrorism" that targets society's "downtrodden," says a study published this month that looked at more than two dozen deaths involving the stun guns. Those most likely to get "tased" include the poor, mentally ill and chronic drug users, according to the study, led by Temitope Oriola, who received a Governor General's Gold Medal for academic excellence upon the completion of his doctoral studies at the University of Alberta last year. Leader-Post, A7 (Edmonton Journal, Calgary Herald, The Province, Vancouver Sun)

First guns. Then food processors?
An opinion piece states, "Pierre Perron of the Canadian Firearms Program wrote "the Armi Jager AP80 rifle is a prohibited firearm and always has been." While this may be correct, I can't help but think that a larger issue might have been overlooked. The Armi Jager AP80, a prohibited variant of the AK-47, has been circulating as a non restricted firearm for well over a decade, yet there have been no incidences with this firearm that would indicate it is any more of a risk to public safety than a regular non-restricted rifle..." National Post, A9; National Post

* **Charged ex-Mountie arrested again**
A former Mountie charged with second-degree murder is back behind bars for flouting his bail conditions. Keith Gregory Wiens, 57, is accused of killing his common-law wife, Lynn Kalmring, in their home in Penticton, B.C., on Aug. 16. Edmonton Journal, A11; The Province

* **Way off target**
An opinion piece states, "The Mounties aren't too happy with me after my last column. It seems the men and women in red serge don't like it being pointed out that they have the ability to seize private property with no government oversight. Last week I wrote about the RCMP's reclassification of a .22-calibre semi-automatic rifle as a prohibited firearm because it looks like another rifle that is already banned...So while the Harper government crows about scrapping the gun registry, the RCMP, which they control, will continue to seize private property without compensation all because something looks scary to a paper pusher in Ottawa." Toronto Sun, 23 (Winnipeg Sun, London Free Press, Calgary Sun, Kingston Whig-Standard, Edmonton Sun)

* **Dirty police officers hurt ex-drug dealer, court told Thursday**
Rather than being beaten by dirty cops, an ex-drug dealer hurt himself by going "berserk" on police who had no choice but to restrain him, a defence lawyer argued as part of a cop corruption trial. Former pot dealer Christopher Quigley has testified several members of the once-illustrious Team 3 of the Toronto Police Central Field Command drug squad beat him to a bloody pulp in 1998 because he wouldn't tell them where they could find his money. The trial continues Friday. Kingston Whig-Standard, 10; Toronto Sun

* **Gangster talked of getting out shortly before shooting: Heed**
Just months before his public execution Tuesday, gangster Sandip Duhre admitted he regretted his choices and would get out of the life if he could. Duhre spoke frankly to Vancouver-Fraserview MLA Kash Heed during a chance encounter at a south Surrey restaurant in late summer, Heed recalled Wednesday. Vancouver Sun, A5

* **La «taupe du SPVM» voulait aussi vendre des renseignements à des trafiquants kurdes**
L'ex-policier Ian Davidson n'aurait pas seulement tenté de vendre sa liste ultrasecrète d'informateurs à la mafia italienne. Il aurait aussi essayé de faire affaire avec un redoutable gang de Kurdes turcs actif dans le trafic de drogue au centre-ville, croit la police. Celui que plusieurs surnomment maintenant "la taupe du SPVM" aurait engagé ces tractations devant le peu d'empressement de la mafia à répondre à son offre. La Presse, A5 (La Tribune, La Voix de l'Est); Le Soleil (Le Devoir)

* **Quatorze arrestations pour trafic de drogue**
La Sûreté du Québec (SQ) a frappé mercredi et hier un réseau impliqué dans le trafic de stupéfiants, actif sur le territoire de la MRC de Manicouagan. La frappe policière, qui découle d'une enquête qui a duré près d'un an, a conduit à neuf perquisitions et à 14 arrestations à Baie-Comeau et à Chute-aux-Outardes. Le Soleil, 20

* **Constable had woman fearing for her life**

A woman testified Thursday in Red Deer court during a Mountie's trial that she feared he had set her home on fire. The 2006 fire caused structural damage and killed a dog, cat and cockatiel. RCMP Const. Hoa Dong La, in a judge-alone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain, involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. Red Deer Advocate, A1

*** Police keeping tabs on toxic form of ecstasy**
Though it has not yet turned up in Newfoundland and Lab-rador, police in the province are keeping tabs on fatal overdoses in Western Canada linked to a form of the drug ecstasy laced with a toxic additive. Paramethoxymethamphetamine (PMMA) is not a new chemical, according to Sgt. Stephen Conohan, a provincial drugs and organized crime awareness co-ordinator with the RCMP. The Telegram, A4

*** RCMP scoring higher in Yukoners' esteem**
Seventy-eight per cent of Yukoners believe RCMP officers demonstrate professionalism at work, according to a new national survey released last week. That's a 12 per cent increase over the same survey in 2010. The annual national survey polled about 500 adult Yukoners over the phone during June and July 2011. Three-quarters of Yukoners say the RCMP is an organization with integrity, compared to 63 per cent in 2010. Whitehorse Star, 2

*** Newfoundland man pleads not guilty to charges in six-day standoff with RCMP**
A Newfoundland man charged after a six-day standoff with the RCMP in December 2010 has pleaded not guilty to all charges. Leo Crockwell barricaded himself inside a Bay Bulls, N.L., home and eventually evaded police by slipping out a side window. The Guardian, A6

*** Banishment remains tool of First Nations justice**
Back in the day, if you were a First Nations citizen who killed another member of the same band or committed a serious crime, you most likely would face banishment. Banishment back then was a nasty piece of business. You had to leave the safety of the camp and take your chances in the outside world. Fast forward 150 years, and the issue of banishment has come full circle. The media recently picked up the fact that the Samson Band in Alberta was contemplating banishment to rid the community of gang members. The four bands at Hobbema, Alta., have been in the news because of runaway gang violence. In the past several years, there have been a rash of murders, drive-by shootings and other evidence of gang activity on the reserve. Saskatoon Star-Phoenix, A9

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Vancouver police should have probed Pickton, officer says
Vancouver police should have investigated serial killer Robert Pickton rather than simply leaving him to the RCMP in a neighbouring city, the public inquiry into the case has heard. Ontario's Peel Regional Police Deputy Chief Jennifer Evans, who conducted an external review for the inquiry, contradicted the Vancouver police force's contention that Mr. Pickton was the responsibility of the Mounties in Port Coquitlam because that's where women were being killed. Deputy Chief Evans said Thursday when Vancouver police received information in 1998 and 1999 that Mr. Pickton may have been picking up sex workers in the city and killing them at his farm, they should have opened a criminal investigation. Globe and Mail, S1 (Red Deer Advocate); Leader-Post (Times Colonist)

*** City police should have pressured RCMP**
Vancouver police should have pressured the Coquitlam RCMP to aggressively investigate Robert Pick-ton in relation to the murder of dozens of missing women, an Ontario policing expert said Thursday. Peel Regional Police Deputy Chief Jennifer Evans, in her fourth day of testimony at the Missing Women Com-mission of Inquiry, insisted the VPD "should have made it a priority" to pressure the Mounties. The Province, A14

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Texas fugitive caught in province
RCMP and the Canada Border Services Agency (CBSA) have announced the arrest of a Texas fugitive.The man, identified as 46-year-old Gene Paul Hooks, was taken into custody Jan. 10 by the Canadian Border Services Agency in Shaunavon. The CBSA issued a "deportation order for serious criminality" Jan. 13. Hooks appeared in court Thursday in Regina and is scheduled to return to court in Swift Current Jan. 25. CBSA spokesman Sean Best said the deportation order won't be acted on until criminal matters have concluded. Leader-Post, A4

*** Mexican journalist in B.C. fears for life if deported**
A Mexican journalist who blew the whistle on corrupt officials in her homeland is pleading with the federal government to let her stay in Canada and says she will be persecuted if sent back. Karla GarcDia RamDirez, a mother of two children, fled to B.C. as an asylum seeker in 2008 after uncovering shady dealings in a government ministry. Red Deer Advocate, A7 (Toronto Star); Chronicle-Herald

*** Campaign shines light on human trafficking**
As many as 15,000 people become victims of human trafficking every year in Canada. That's far too many, says a Tory MP who has devoted herself to the cause. "Modern-day slavery is really manipulation of the mind," said Joy Smith before speaking to a group of University of Alberta students Thursday afternoon. Her passion to com-bat human trafficking was sparked by her son, who spent two years on the RCMP's Integrated Child Exploitation Unit. Edmonton Sun, 38

*** Justice and reconciliation are at the heart of Rwanda's recovery**
An opinion piece by Edda Mukabagwiza, Rwanda's high commissioner to Canada states, "Defence lawyers are paid to do and say whatever it takes to protect the interests of their clients. This explains why Léon Mugesera's lawyers, in a last-minute scramble to prevent their client's deportation to Rwanda, resorted to raising the spectre of torture. It amounts to a baseless and cruel slur against our country, and therefore demands a response..." Montreal Gazette, A17

*** City mother's deportation has been deferred**
The Canadian Border Services Agency (CBSA) confirmed Thursday that Hamilton mother Lucene Charles is no longer scheduled to be deported. In a statement read to The Spectator, a CBSA spokesperson said Charles has asked the agency to defer her removal from Canada. Hamilton Spectator, A5

*** "Ça passe ou ça casse"**
C'est aujourd'hui que les avocats de Léon Mugesera tenteront de prolonger le séjour du Rwandais au Canada, le temps que le comité contre la torture de l'ONU étudie le dossier et se prononce. Ce matin, à 9 h, une procédure complète sera présentée devant la Cour supérieure pour faire valoir le droit de Mugesera de s'adresser au comité contre la torture et l'obligation qu'a le gouvernement canadien de respecter les mesures provisoires jusqu'à la décision du comité. Journal de Montréal, 9

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Teen to be moved to federal prison
One of the B.C. teenagers who raped and murdered Kimberly Proctor in 2010 will be transferred from Victoria's youth detention centre to a federal penitentiary on Monday, his 18th birthday. Kruse Hendrik Wellwood lost his bid Wednesday to extend his stay at the youth facility until June 30 to allow him to complete Grade 12. B.C. Supreme Court Justice Robert Johnston agreed with the Crown that Wellwood needs intensive psychiatric and psychological treatment, available only in the federal system. National Post, A5 (The Province)

*** Forum looks at aboriginal women's plight - Manitoba MP to take issue to PM**
A Manitoba MP believes a United Nations conference this week can help his government shed some light on the issue of violence against aboriginal women. Rod Bruinooge, the Conservative MP for Winnipeg South, was at the UN in New York City this week for a three-day expert group conference of the Permanent Forum on Indigenous Issues. Research by the Native Women's Association of Canada showed more than 500 aboriginal women have been murdered or gone missing in Canada in the last four decades. Aboriginal women are 3.5 times more likely to be victims of violence than non-aboriginal women and five times more likely to be slain. The research spawned recognition of the problem and some action, including better police investigations when aboriginal women are reported missing. Winnipeg Free Press, A8

*** Egadz looks to expand sex trade registry**
A Saskatoon outreach program is looking to expand its sex-trade registry, which collects detailed information from workers in case they are found dead. Egadz, a non-profit agency that provides support for atrisk youth, has more than 100 sex trade workers on its "high-risk homicide registry," which was launched 15 years ago. The goal this year is to grow the registry to include information on more than 200 women and potentially expand to include youth at risk of running away, said Don Meikle, Egadz's director of outreach services. StarPhoenix, A6

*** B.C. cops brace for killings after murder of gangster**
Police across British Columbia's Lower Mainland are bracing for possible retaliatory killings after the brazen public execution of longtime gangster Sandip (Dip) Duhre by someone he was meeting at the Sheraton Wall Centre Tuesday night. They are looking at whether the targeted hit is linked to a series of tit-fortat slayings between rival groups over the

past 15 months that has left a trail of dead and wounded from Kelowna, B.C., to downtown Vancouver. Windsor Star, A6 (Times Colonist), Calgary Sun

*** Safe-injection sites a dilemma for Tremblay**
An opinion piece states, "...But at the moment, many of the 80,000 or so residents of the downtown borough are concerned, if not downright frightened, of what may happen to their neighbourhoods if a proposal to establish a safe-injection site in their midst is approved. A coalition of citizens groups has called for a moratorium on the project and are promising to show up at next month's meetings of their borough council and local health board to air their concerns..." Gazette, A9

*** Murder suspect's dad blames the system**
The justice system failed slaying victim Otto (Bunty) Loose if the man accused of killing him is convicted of the crime, the suspect's father said Thursday. At the time of the killing, Timmy Engel, 35, of Clares-holm was under house arrest while awaiting trial on charges stemming from a domestic incident last month. The murder charge against Timmy Engel hasn't been proven, but his father said the accusation raises serious questions about why his son wasn't remanded following the domestic charges in December. Calgary Herald, B1

*** 'Mockery of the system'**
An editorial states, "Being of Haitian origin has nothing to do with aboriginal culture in Canada, which is why rapist and killer Gregory Bromby should not have been entitled to an aboriginal parole hearing on Wednesday... Global News reports that in 2010-2011, 492 offenders who were up for parole asked for aboriginal hearings and 56 of those inmates were not aboriginal. Parole board hearings should deal strictly with the offender's crime, not his spiritual bent. A hearing concerns itself with justice, and should be conducted accordingly." Calgary Herald, A20

*** End of the line for second chances**
The real-life story of a Brampton man who was given a reprieve by a judge and turned his life around could soon be fodder for fables. And that's because Bill C10, expected to pass into law in Canada by the end of March, will make second chances a thing of the past. Instead, the bill's mandatory minimum sentences will make sure that people such as Maxwell Beech go to jail. Toronto Star, GT1

*** PM's priorities out of touch**
A letter states, "Canadians face 'tough choices,' PM says, Jan. 16. I guess we're fortunate to have a tough, level-headed economist at the helm. Obviously cuts must be made but, as we all know, some things are just too important to be left behind. I'm sure we can trust the Harper government to keep its priorities in order. Tax cuts for Big Business, support for Big Oil, the purchase of F-35s, the building of new prisons - these are the things Canadians want and need..." Toronto Star

*** Ashley Smith's mother to speak at Feb. 4 event**
The mother of a Moncton teen who died under troubling circumstances in a women's prison will be a guest speaker at a Moncton event aimed at dispelling myths about mental health. Times & Transcript, A9

*** Judge blasts appeal court**
One of Alberta's top judges has come out railing against his Court of Appeal colleagues for an apparent "tough on crime" agenda. Justice Ronald Berger, in a written judgment released Thursday, was highly critical of an earlier appeal court decision, which reiterated a three-year starting point for major sexual assaults. He said the sentencing guidelines established by the court in the Jordan Arcand case in 2010, "ignores the plethora of empirical studies that cast doubt on the efficacy of incarceration as a means of suppressing criminal conduct."
Calgary Sun, 8

*** Inmate dies months before completing sentence**
A Toronto man serving time for stabbing the mother of his former common-law wife to death died in custody Wednesday -- just six months before completing his 12-year sentence for manslaughter. Corrections officials say 60-year-old Joseph Caissie, an inmate at Joyceville Institution, was found unresponsive in his cell around 1:15 p.m. by correctional officers. Kingston Whig-Standard, 2 (Ottawa Sun)

*** Leave it to the law, and leave culture out**
An opinion piece states, "Can someone please tell me why we even have "culturally sensitive" parole hearings for cons seeking early release? To be honest, before the story broke this week about the Haiti-born killer who was granted an aboriginal culturally sensitive parole hearing in Winnipeg, I'd never even heard of this before... My question is, why do we even have these types of hearings? What does a person's culture, adopted or otherwise, have to do with a hearing that's

supposed to assess the risk of an offender and determine whether he or she should be granted parole?..." Winnipeg Sun, 5

*** NDP follows Einstein's maxim on crime issues**
The government of Manitoba has been on a spending spree on adult-jail operating expenses. Since 2004, the operating budget for jails has increased 83 per cent. While federal New Democrats harshly criticize the federal Conservatives for the tough-on-crime omnibus bill, the provincial NDP government has been quietly building more jails and hiring more prison guards to the extent that it dwarfs the Harper expenditures. Winnipeg Free Press, A11

*** Un pédophile au long cours déclaré délinquant dangereux**
Après 35 ans d'arrestations, de condamnations et de peines de prison, le tribunal s'est rendu à l'évidence, hier: rien ne peut guérir Jean-Claude Séguin de sa déviance, la pédophilie. Le cuisinier d'origine montréalaise, dont les derniers délits ont été commis à Granby, est automatiquement condamné à une peine de prison indéterminée, sans possibilité de libération conditionnelle avant au moins sept ans. La Voix de l'Est, 7

*** Policière en danger**
Laurent Minier, qui a sauvagement agressé une policière de Québec, en 2002, devrait être transféré, d'ici le mois d'avril, à la maison de transition Marcel-Caron, qui se trouve à moins d'un kilomètre de la résidence de la policière. Selon elle, la Commission nationale des libérations conditionnelles (CNLC) ne devrait jamais permettre que ce type d'agresseur soit retourné près des victimes, encore moins à un kilomètre de leur résidence de la victime parce que ça devient "carrément un cauchemar éveillé". Le Journal de Montréal, 9

*** Supreme Court to rule later on sex workers' Charter fight**
A controversial case over who can mount a Charter of Rights challenge to Canada's sex trade laws made it to the Supreme Court, bringing dozens of supporters to the court's front steps Thursday. Ottawa Citizen, C6

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Bilingui$me**
Un article d'opinion déclare, « On apprenait cette semaine que la prestation de services publics bilingues au Canada coûterait plus de deux milliards de dollars par année. Comme c'est exactement le même montant qu'a coûté le registre des armes à feu, j'ai bien peur que Stephen Harper veuille faire comme avec le registre, et élimine la langue française au pays!... » Journal de Montréal, 21

*** Feds eye MP pension reform**
MPs may soon be scrambling their golden nest eggs. Treasury Board President Tony Clement says his review of government spending to find an annual savings of $4 billion will include looking at MP pensions -- pensions the Canadian Taxpayers Federation has dubbed "platinum-plated." Kingston Whig-Standard, 9

*** Federal civil servants on edge over possible pension changes**
Finance Minister Jim Flaherty wants to be clear. The commitment he made in 2010 that the Conservative government wouldn't touch federal pensions didn't mean they would never be reviewed again. The Public Service Alliance of Canada (PSAC) was banking that public servants' paying higher contribution rates for their pensions would spare them from further changes or cuts to their pension plans. Calgary Herald, A5

OTHER / AUTRE

Double-murderer Ronald Smith asks to be spared death penalty
After almost 30 years in an isolation cell at Montana State Prison, Alberta-born double-murderer Ronald Smith - the only Canadian on death row in the United States - has formally filed his request for executive clemency to the state's parole board, submitting a 19-page appeal in which his lawyers describe the 54-year-old convict as a man who has made "great strides in his rehabilitation" and exhibits "heartfelt remorse," "a changed heart and mind" and "a potential for good." Smith, a native of Red Deer, Alta., was convicted in Montana of killing two Blackfeet Indian men - Harvey Mad Man, 24, and Thomas Running Rabbit, 20 - during a drug-and alcohol-fuelled road trip to the U.S. in August 1982. Leader-Post, A9

Prepared by Public Safety Canada Media Monitoring /

Préparé par la Surveillance des médias de Sécurité publique Canada

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-19-12 8:12 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 19, 2012 / le 19 janvier 2012

MINISTER / MINISTRE

Police need more online surveillance power, Ottawa says
Canadian law enforcement officials have never been hindered by having to abide by the country's current privacy laws, say documents revealed Wednesday, yet Ottawa remains adamant police need more online surveillance powers. Vancouver-based advocacy group OpenMedia.ca published details of an internal Canadian Association of Chiefs of Police (CACP) email message to its members who represent more than 90% of the country's police community. The message, OpenMedia says, asks CACP members to provide examples, even those with "confidential operational information," of investigations thwarted by Canada's privacy legislation. The goal of the call for case studies would appear to be to justify the federal government's proposed lawful access legislation. Responding to criticism from a Liberal Party MP during question period in the House of Commons last November, **Public Safety Minister Vic Toews** said opponents to lawful access were "***putting the rights of child pornographers and organized crime ahead of the rights of lawabiding citizens***." Despite the obvious need to respond to digital crimes, no systematic case has yet been made to justify Canada's government legislating new surveillance powers over the Internet, federal Privacy Commissioner Jennifer Stoddart said in a recent letter to **Mr. Toews**. The only case presented as justification was presented by then **Public Safety Minister** Peter Van Loan in 2009, who mentioned a kidnapping incident where police had to wait 36 hours to obtain a warrant. **Public Safety Canada** has said the legislation follows similar policies recently adopted by the United States, Australia, Germany and Sweden and "***strikes an appropriate balance between the investigative powers used to protect public safety and the necessity to safeguard the privacy of Canadians***." "***No legislation proposed by our Conservative Government will allow police to unlawfully read emails without a warrant. Claims to the contrary are baseless,***" **Public Safety spokesperson Julie Carmichael** said via email Wednesday. "***As technology evolves, many criminal activities - such as the distribution of child pornography - become much easier. We are proposing measures to bring our laws into the 21st century and provide police with the tools they need to do their job.***" "***Rather than making things easier for child pornographers and organized criminals, we call on all Canadians to support these balanced measures***," she said. National Post, FP12

Police identify pilot killed in RCMP chopper crash
Police have identified the pilot who was killed Tuesday in the crash of an RCMP helicopter as 46-year-old David Brolin. Brolin, a civilian RCMP member, was Air 5's sole occupant during a training exercise east of Cultus Lake, B.C. "***This is a very sad day for all Canadians***," **Public Safety Minister Vic Toews** said in a statement late Tuesday. "***The death of a member of our national police force is a sobering reminder of the sacrifices and bravery of the men and women who serve each day to keep our communities safe.***" London Free Press, B3 (Edmonton Sun, Kingston Whig-Standard)

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** No clear evidence Tamiflu works, researchers say**
Concerns are emerging that governments around the world may have wasted billions of dollars and even put people at risk by stockpiling Tamiflu to treat influenza. Globe and Mail, L6; Edmonton Sun

*** Non-vaccinated staff killing us, expert warns**
Thousands of Canadians die needlessly each year because health-care workers won't get flu shots, a leading expert says. London Free Press, A1

*** Protecting wetlands key in flood defence**

An opinion piece states, "Flooding was a problem not only in Manitoba this past year, but it was also a major issue in Saskatchewan. Both provinces faced enormous costs associated with lost crops, washed out roads and culverts, and in some cases, people lost their homes. In fact, flooding in Manitoba will cost taxpayers $1 billion in damages and flood-fighting efforts. This wasn't the first year Manitoba was forced to deal with water issues. We've been plagued by a number of consecutive wet years in areas throughout the province, affecting people's livelihoods and causing tremendous emotional stress and hardship for hardworking Manitobans -- those enduring the real costs of the flood. Yet, as a province, we haven't done nearly enough in terms of implementing real solutions to this recurring issue..." Winnipeg Sun, 9

*** Could La Nina predict flu pandemics?**
The weather phenomenon known as La Nina, or the appearance of waters that are cooler than normal in the eastern and central Pacific Ocean, may be responsible for more than just changes to global weather patterns. It could also play a role in worldwide flu pandemics, according to a researcher at Columbia University whose study has been published in the journal Proceedings of the National Academy of Sciences. Toronto Star, A26

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Man files human rights claim against Gatineau
A man has filed a complaint with Quebec's Human Rights Commission after he says he was singled out by the City of Gatineau for criticizing a controversial immigrant values guide. Kamal Maghri, who has lived in Canada for 11 years and works for the federal government, said he was shocked when he discovered that a city official had been investigating him. Maghri said the official was digging up details on his finances and even mentioned to other government officials that he had come to Canada just after the Sept. 11, 2001, terrorist attacks in the United States. The official also called a mosque in Gatineau to see if the caretakers knew Maghri. Ottawa Citizen, C4 (National Post)

Da? Nyet?
A letter states, "Has our Defence Ministry become so secretive that Peter MacKay doesn't dare say out loud that Canada's latest spy scandal involves Russia, when even the usually very secretive Russians are saying it (Accused Spy Would Have Had Top-Level Clearance - Jan. 18)?..." Globe and Mail, A14

Accused in spy case known as a loner
At high school in Lower Sackville, Nova Scotia, Jeffrey Paul Delisle was known as a bit of a geek, a loner who kept to himself. A clearer picture is emerging of the 40-year-old naval intelligence officer who was charged on Monday with passing government secrets to foreign interests, and who one military expert says was likely under police surveillance for months or years. Fellow students in Sackville High School's graduating class of 1990 had few recollections of the ordinary kid with the low profile now enmeshed in what could be Canada's biggest spy scandal in more than half a century. Globe and Mail, A4; National Post (Edmonton Journal, Times Colonist); Calgary Sun (London Free Press, Edmonton Sun, Ottawa Sun, Toronto Sun, Whig-Standard, Winnipeg Sun); * Whig-Standard; * Toronto Sun; * Toronto Sun; * The Record; * Chronicle-Herald; * Hamilton Spectator (Red Deer Advocate)

CYBER SECURITY / CYBERSÉCURITÉ

*** A black day for Internet privacy in Canada: expert - U.S. anti-piracy laws called heavy-handed**
Canadians would be affected if online anti-piracy laws proposed south of the border get passed by Congress, say advocates of free speech and privacy. The laws - The Stop Online Piracy Act and the PROTECT IP Act, known as SOPA and PIPA - would require Internet-service providers to block access to any site accused of posting, or linking to, copyrighted content. It also would force search engines to remove the offending sites from their databases and prevent advertisers from giving the site their business. Critics say the law would make media companies judge and jury of copyright infringement, rather than having the process resolved in court. They also say it's a blatant attack on freedom of expression. "The goal, in many ways, of SOPA is to reach beyond the borders of the United States," said Michael Geist, a University of Ottawa law professor and copyright expert. "It's Canadian sites and sites around the world that would find themselves a target for these kinds of actions." Montreal Gazette, B1

*** Day without Wikipedia just a glimpse**
If a day without Wikipedia was a bother, think bigger. In this plugged-in world, we would barely be able to cope if the entire internet went down in a city, state or country for a day or a week. And most of civilization went along until the 1990s without the internet. But now we're so intertwined socially, financially and industrially that suddenly going back to the 1980s would hit the world as hard as a natural disaster, experts say. No email, Twitter or Facebook. No buying online. No

stock trades. No just-in-time industrial shipping. No real-time tracking of diseases. It's gotten so that not just the entire internet but individual websites such as Google are considered critical infrastructure, experts said. Waterloo Region Record, A6

*** Court gives legal recourse to privacy theft victims**
Ontario's top court has created a new way for individuals to sue people who invade their private information, a new step in the legal system's attempts to come to terms with the digital age of online record-keeping and communications. Crafted by the Ontario Court of Appeal on Wednesday, the change will provide a legal avenue for those whose sexual practices, private correspondence or personal records have been snooped on for no legitimate reason. The court said information is being generated and stored at a staggering rate, but legislation has not kept pace - leaving aggrieved parties no recourse against those who violate their privacy. In his ruling, Judge Sharpe created a new legal tort - a basis for a lawsuit - called "intrusion upon seclusion." Globe and Mail, A6

*** Lock your online doors - Stopping Internet crime is a constant game of digital cat and mouse for Web heavyweight Google**
Even Google Inc. cannot guarantee your safety online. So last summer, when the company behind the world's largest search engine noticed computers all over the world were being infected with a specific type of malware (malicious software), Google went public with its discovery. Because the warning asked users to conduct a Google search to see if they were among the victims, some people derided the company for what they perceived as an attempt to promote its own service. Others claimed announcing the threat to the world would only give those responsible time to adapt. Four months later, Fabrice Jaubert, a Montreal-based software engineer who works on Google's anti-malware team, stood by the move. "We could turn the question around and ask if it would have been ethical to know someone was infected and not tell them," he said in an interview. Mr. Jaubert expects to continue playing his digital cat and mouse game "where the bad guys try to stay one step ahead of us and we come up with better, more complex algorithms to try and identify them." National Post, FP12

*** Zappos, Amazon sued over hacking**
Online retailers Zappos.com and Amazon.com are being sued in Kentucky by a Texas woman alleging that she and millions of other customers were harmed by the release of personal account information. Officials representing Zappos in Nevada and parent company Amazon in Seattle declined comment Wednesday on the lawsuit filed in U.S. District Court in Louisville, Ky. The lawsuit was filed Monday, after Zappos chief executive officer Tony Hsieh alerted employees and customers by e-mail Sunday that names, phone numbers and e-mail addresses of the shoe retailer's customer may have been accessed in a hacker attack. The company said customers' credit card and payment information weren't stolen. Zappos urged customers to reset passwords. Globe and Mail, B10

*** Internet anti-piracy bills throw lasso too widely**
An opinion piece states "If you tried to use Wikipedia yesterday and were met by a black screen with the chilling caution 'Imagine a World Without Free Knowledge,' welcome to the world of copyright debate. That debate is peaking in the U.S. Congress, where two proposed laws would force Internet providers to shut down 'pirate' sites selling illegal movies, music or books -- cutting off those sites, refusing to accept advertising from them and disabling any payment processing links. The crackdown is necessary. Free knowledge doesn't include freedom to break the law. However, the laws are a big lasso intended to corral a rogue horse. They could also catch cart horses just doing their jobs -- delivering information. Canada's proposed new copyright law takes a halfway approach. Internet providers would have to inform customers that they have downloaded illegal material. The implied threat of a criminal charge for the next offence is intended to have a 'scared straight' effect. That's a potentially effective approach, but if it doesn't work, something closer to the U.S. model will be necessary." Kingston Whig-Standard, 4 (London Free Press)

*** Brake the Internet pirates**
The following editoral, reprinted from The Wall Street Journal, states: "Wikipedia and many other websites are shutting down today to oppose a proposal in Congress on foreign Internet piracy, and the White House is seconding the protest. The covert lobbying war between Silicon Valley and most other companies in the business of intellectual property is now in the open, and this fight could define - or reinvent - copyright in the digital era. Everyone agrees, or at least claims to agree, that the illegal sale of copyrighted and trademarked products has become a worldwide, multibilliondollar industry and a legitimate and growing economic problem. Often consumers think they're buying copies or streams from legitimate retail enterprises, sometimes not. Either way, the technical term for this is theft. The Internet has been a tremendous engine for commercial and democratic exchange, but that makes it all the more important to police the abusers who hijack its architecture. SOPA merely adapts the current avenues of legal recourse for infringement and counterfeiting to new realities. Without rights that protect the creativity and innovation that bring fresh ideas and products to market, there will be far fewer ideas and products to steal." National Post, FP11

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Former officer accused of Mafia ties found dead
By the time Detective Sergeant Ian Davidson retired a year ago from the Montreal police, the 33-year veteran had built up a reputation as a meticulous analyst in the intelligence unit, responsible for handling highly sensitive information. Within months, that reputation began to unravel. The Montreal native had fallen under investigation for explosive allegations: that he tried to sell the names of secret police informants to the Mafia. The 57-year-old is believed to have committed suicide. Globe and Mail, A4; * Toronto Sun; * Toronto Star; * Le Droit (Le Soleil, La Tribune, Le Devoir); * Le Quotidien; * Journal de Montréal; * Journal de Montréal

* **A police force that does less with more**
An opinion piece states, "Police chief Marc Parent is seeking to reassure Montrealers. He said on Tuesday that a retired police detective had failed in his attempt to sell to the Mafia a top-secret list of undercover officers and other police informants. As it happens, the ex-detective died the next day. So, end of story? Hardly. It's a relief to hear that no informants lost their lives. But the larger matter - the overall performance by police against organized crime - is not reassuring at all. Montreal police appear to have been helpless to prevent the Mafia from maintaining a decades-long grip on parts of Montreal Island's economy. And when intra-Mafia politics produce high-profile murders, it's striking how seldom local police make arrests. (Do last month's arrests of five men linked to the slaying of Salvatore Montagna suggest improvement? No. The Sûreté du Québec, not the Montreal force, nailed them.)..." Montreal Gazette, A2

Mountie faces charges
A Rimbey. Alta., Mountie is on leave after being charged with assault and uttering threats in connection with at least three incidents in 2011, RCMP say. Const. Charles Lambright faces two counts of assault, one count of uttering threats and one count of breach of a court order, RCMP spokesperson Tim Taniguchi said. The charges stem from alleged incidents between Lambright and a woman he had a personal relationship with, he said. An RCMP code of conduct investigation is also underway. Starphoenix, A4 (Edmonton Journal)

Fourth special prosecutor takes Bountiful case
A new special Crown attorney has been appointed to look into allegations of sexual exploitation and other offences against minors in the polygamous community of Bountiful, B.C. Peter Wilson was appointed to represent the province in the case against religious leaders in the closed fundamentalist Mormon community, who have been accused of sexual exploitation of a young person, sexual assault and procurement in allegations dating back to the early 1980s. Wilson is the fourth special Crown attorney appointed to the case. He replaced Richard Peck, who dismissed himself earlier this month. London Free Press, B8

* **Cocaine trial tied to publisher's 1998 murder**
The cocaine conspiracy trial of a Montreal man suspected by police of being involved in the assassination of Vancouver publisher Tara Singh Hayer opened in Vancouver on Wednesday. In her opening statement, federal prosecutor Martha Devlin told the judge that the background to the drug conspiracy case began in 2005, when RCMP launched Project Expedio. The Province, A12

* **Mayor suggests expanding RCMP headquarters**
Queens District RCMP may be looking for a new home and Charlottetown Mayor Clifford Lee has a suggestion. RCMP Sgt. Andrew Blackadar said Wednesday the person who owns the building which currently houses the detachment (Maypoint Plaza) wants to sell the building. The RCMP have the space leased until May 2013. The towns of Stratford and Cornwall have already expressed interest in having the district headquarters come their way but the capital city mayor has another suggestion. The Guardian, A1

* **Profilage: le SPVM ne reçoit pas une note parfaite**
La Commission des droits de la personne et des droits de la jeunesse du Québec (CDPDJQ) déplore à nouveau le manque de collaboration de la police de Montréal dans le traitement des plaintes pour profilage racial. Le président de la Commission, Gaétan Cousineau, est heureux que le Service de police de la Ville de Montréal (SPVM) s'attaque sérieusement au problème du profilage racial et social, mais il se réserve bien d'accorder une note parfaite au nouveau plan stratégique dévoilé mardi. Le Devoir, A2

* **Mountie 'terrified' woman**
An Innisfail woman says she was terrified of the Mountie who rented a property to her about seven years ago. RCMP Const. Hoa Dong La, in a judgealone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain, involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. La, 47, faces 15 counts altogether, including three counts of extortion, two of criminal harassment and 10 of mortgage fraud. Red Deer Advocate, C1

*** Man charged with possessing 50,000 contraband cigarettes**
A 40-year-old man from Clarenville was arrested Tuesday for possession of contraband tobacco when the vehicle he was operating was stopped by the RCMP Customs and Excise Section and found to contain 50,000 contraband cigarettes. The man will appear in provincial court in March to answer to charges under the Excise Act and the Provincial Revenue Administration Act. The Telegram, A5

*** Gangster ducked earlier bullets**
Sandip "Dip" Singh Duhre, 36 - killed Tuesday in a hail of bullets at a downtown Vancouver restaurant - was a notorious gangster marked for death since 2005. Sandip, along with his brothers Balraj, 38, and Paul, 35, headed the powerful Duhre Group - whose 50 to 100 "street soldiers" have con-trolled much of the drug trade in the Fraser Valley since the 2010 arrests of rival leaders from the United Nations and Red Scorpions. The shooting comes less than a week after well-known Vancouver gangster Ranjit Singh Cheema was released from a U.S. prison. The Province, A3

*** Youth's cop car theft sentencing delayed**
Sentencing for a Moncton teen who stole a police car last fall and injured a police officer was adjourned yesterday morning so the Crown can call the Mountie to the witness stand. The 16-year-old boy appeared in Moncton youth court before Judge Irwin Lampert on Jan. 4 and pleaded guilty to a long list of charges, including obstructing Const. Kevin Tremblay by giving him a false name, stealing a police car, dangerous driving, impaired driving causing bodily harm to Tremblay and three breaches of court orders. Times & Transcript, A3 (Telegraph-Journal)

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Inquiry hears B.C. RCMP failed to 'take ownership'
An Ontario deputy police chief told the Missing Women Commission of Inquiry Wednesday that if British Columbia police leaders had "taken ownership" of the issue, "many women's lives may have been saved." Deputy Chief Jennifer Evans of Peel Regional Police concluded in her 2011 report to the inquiry that "the (Vancouver Police Department) and the RCMP initially failed to recognize the missing women issue. Leader-Post, A7 (Times Colonist)

*** Pickton claims he's innocent of murders, officer tells inquiry**
An Ontario deputy police chief who interviewed serial killer Robert Pick-ton in jail says he claims he's innocent of murdering women. "He said he didn't do anything, he maintained his innocence," Jennifer Evans, Peel Regional Police deputy chief, told the Missing Women Commission of Inquiry on Wednesday. Evans interviewed Pickton in prison as part of her review of how police con-ducted their investigations into the dozens of women who went missing from Vancouver's Downtown Eastside. The Province, A8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Lawyers doubt genocide evidence
The federal government has information that proves the Rwandan government is criminal and that fabrication of evidence about the 1994 genocide is a common occurrence sanctioned by authorities there, claim lawyers trying to stop the deportation of suspected war criminal Leon Mugesera. Starphoenix, D5

*** Waiver to cross U.S. border isn't a simple affair**
A letter to the editor states, "Mike Milne, a spokesman for U.S. Customs and Border Protection, refers to the need for a waiver to enter the U.S. if someone has a conviction for a narcotics offence. The waiver is an "Application for Advance Permission to Enter as Non-immigrant" which requires finger-prints taken by the RCMP for a Canadian record check, also sent to the FBI and the U.S. Justice Department, details of the offence, court records, family history, letters of character reference, evidence and/or a written account demonstrating rehabilitation, advance request for date(s) of entry, and fingerprints taken again (by U.S. officials)...Six hundred thousand Canadians have criminal records of possession of marijuana. Even if you don't have a criminal record in Canada any more, because of a conditional discharge or a pardon, Uncle Sam neither forgets nor forgives." Vancouver Sun, A12

*** 30 jours de prison pour un Américain arrêté au N.-B.**
Un homme âgé de 20 ans de l'Oregon a plaidé coupable à des accusations liées à son entrée illégale au Canada. Il a écopé d'une peine de 30 jours d'emprisonnement. David Allen Sankey a été arrêté vendredi par des membres du District 7 de la GRC après avoir traversé la frontière sans être passé par un poste de douane. Il a ensuite été confié à l'Agence des services frontaliers du Canada. L'Acadie Nouvelle, 6; Telegraph-Journal

*** The border**
On this issue, many of the report's recommendations mimic the ongoing work of the Canada-U.S. Regulatory Cooperation Council. That work was recently endorsed by Mr. Harper and U.S. President Barack Obama, and business and government officials on both sides of the border are hammering out the specifics of how to speed up border crossings for business by reducing duplication. The report calls for the Canada Border Services Agency to make Free and Secure Trade (FAST) lanes more widely available at the border for shippers. Globe and Mail, A6

*** New wrinkle in Mugesera case**
Ottawa has information that proves the Rwandan government is criminal and that fabrication of evidence about the 1994 genocide is a common occurrence sanctioned by the authorities, claim lawyers trying to stop the deportation of suspected war criminal Léon Mugesera. In a motion to be presented in Quebec Superior Court Friday, law firm Roy Larochelle Avocats Inc. says that documentation never before presented shows it's impossible for Mugesera to have a fair trial in Rwanda and that the judiciary is not impartial. Montréal Gazette, A6

*** Léon Mugesera case**
An editorial states, "There is much about Rwanda that Montrealers know little or nothing about because mainstream Western news media do not report it. This is why, regardless of what one thinks of the man, The Gazette's editorial "Léon Mugesera and justice in Rwanda" (Jan. 14) is out of touch with reality. Mugesera is facing deportation to Rwanda over allegations that he was in part responsible for precipitating the 1994 genocide in that country. He argues that he faces torture or summary execution there…Let's not kid ourselves into believing that deporting him to Rwanda would be legal." Montreal Gazette, A15

*** L'ONU et Mugesera...**
Un article d'opinion déclare, « Dites-moi que je rêve! En 1994, l'ONU n'a pas voulu intervenir pour empêcher le massacre de 800 000 personnes. Là, elle trouve important de demander au Canada de surseoir à l'extradition de Mugesera pour s'assurer qu'il soit bien traité dans son pays. Depuis plus de 15 ans, Mugesera a bénéficié de tous les recours juridiques de notre pays pour se faire entendre et cela ne suffit pas?... » Le Soleil, 25

*** Muslim wife fears for her life**
A Muslim wife who claims she'll be killed by her in-laws for not being able to bear children has been temporarily spared deportation to her native Bangladesh in a precedent-setting case. Mosammat Monowara Khatun, who lives in Toronto, was spared removal on Jan. 8 after a last-ditch appeal to the Federal Court of Canada stayed her deportation. London Free Press, B8 (Toronto Sun)

*** Le Canada appuie l'appel à la clémence de Ronald Smith**
Les avocats du seul Canadien condamné à mort aux États-Unis ont officiellement déposé une demande de clémence aux autorités de l'État du Montana. Leur client, Ronald Smith, maintenant âgé de 54 ans, est dans le couloir de la mort aux États-Unis depuis près de 30 ans pour les meurtres de deux hommes en 1982. Tous les appels précédents de l'homme originaire de Red Deer, en Alberta, ont été jusqu'ici rejetés. La Presse, A14 (La Voix de l'Est, L'Acadie Nouvelle); Calgary Sun; Toronto Star (Red Deer Advocate, The Guardian)

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Getting high on renewal
An editorial states, "…There has been no public clamour for a war on drugs in Canada, yet the Tories are pursuing one as part of their costly crime agenda, with measures such as legislating mandatory minimum prison terms for people caught growing a handful of pot plants. Even in the U.S., some conservatives are disowning the Reaganite policy, as the crackdown has had little impact on actual use, has proved enormously costly in fiscal and human terms and created fertile ground for drug gangs. Whether legalization is the best solution is open to debate. This newspaper has previously favoured decriminalization. But the Liberals are right to make it a political issue." Globe and Mail, A14

Killer denied day parole in aboriginal hearing
On the grounds that he is "no farther ahead" than he was when he killed 15-year-old Tara Manning, convicted murderer Gregory Bromby was denied day parole Wednesday in an aboriginal elder-assisted hearing. Although the Haitian-born Bromby is not aboriginal, he qualified for an elder-assisted hearing by demonstrating a "commitment to aboriginal spirituality." National Post, A6; * Winnipeg Sun, * Winnipeg Free Press

The legalization of pot

A letter states, "Arguments for and against the legalization of marijuana have been going on for the past decade, with weak arguments presented for maintaining the status quo... To further extrapolate that slapping a tax on marijuana would result in a black market for private dealers (as I suppose has happened in the liquor industry) is speculation gone wild. Prohibition gave rise to organized crime; illegal drug use spawned the drug cartels and countless crimes and murders. Society implicitly condones the use of marijuana. To legalize it and put it on the same footing as alcohol and tobacco is something that any progressive government should do. Discouragement of its use should follow the same programs that are now in effect for tobacco." The Gazette, A14

*** Weeding out trouble**
City officials and cops are concerned about risks posed by legal marijuana grow ops, those sanctioned by the federal government, running anonymously in Calgary communities. Despite being given the nod by Health Canada to see pot plants produced, the operations can pose the same peril seen with illegal outfits. A southwest house was shuttered Wednesday after officials from the city's safety response unit and health officials deemed it unfit for human habitation. Calgary Sun, 3

*** Getting high on the Grits' pot plank**
An editorial, "The Liberal party convention last weekend revived the old debate on whether or not we should legalize marijuana. While our prisons are jam-packed, our public finances in the red and almost everyone admits that the war on drugs is a "complete failure," the time may have come to re-open that bag of pot... Don't get me wrong. I do approve of the Conservatives' policy of being tough on crime. I just don't believe that an adult who freely decides to have six plants of marijuana in his backyard or basement and who smokes a joint or two a day is a criminal. The Conservatives do not understand that but now the Liberals do. I am quite sure that Bob Marley's spirit could inspire the Grits for their next election campaign slogan: No victim, no crime ..." Calgary Sun, 15 (Edmonton Sun, Ottawa Sun, Toronto Sun, Winnipeg Sun)

*** Move to legalize pot looks set to heat up**
An opinion piece states, "When you just can't win a war, it's a good idea to consider whether you should still be in there, fighting it. Smoking marijuana and taking other products of the cannabis plant are all illegal in this country. But many otherwise law-abiding people do it anyway, and we are now at the point where political leaders are almost embarrassed if they haven't taken a toke or two. Federal Liberal leader Bob Rae says he has smoked marijuana. So has Ontario Premier Dalton McGuinty. And U.S. President Barack Obama, when asked if he had inhaled, quipped: "Frequently ... That was the point!" It seems that everywhere, except the federal Conservative government, we're ready to shrug off our anti-dope laws..." The Record, B1

*** Hearings poorly understood**
There are many misconceptions about aboriginal parole board hearings. Among them is that offenders do not have to be aboriginal to get one. About 10 per cent of the 500 or so aboriginal hearings held every year across Canada are at the request of non-aboriginal offenders. The latest case involves Haitian-born convicted killer Gregory Bromby, who received an aboriginal parole board hearing Wednesday at Stony Mountain Institution. Another misconception? An offender won't necessarily know the elder who sits in on the hearing, nor is the elder an advocate for the offender. Winnipeg Free Press, A4

*** Man nabbed after halfway house escape**
A 38-year-old man who police say walked away from a halfway house in Nova Scotia was arrested in Charlottetown without incident Wednesday. Hartley Coleman was wanted on a Canada-wide warrant. Chronicle Herald, A3 (The Guardian)

*** Proctor killer must go to adult institution**
One of the teens who brutally raped and murdered Kimberly Proctor in March 2010 will be transferred from Victoria's youth detention centre to a federal penitentiary on Monday, his 18th birthday. On Wednesday, Kruse Hendrik Wellwood applied to B.C. Supreme Court Justice Robert Johnston to extend his stay at the youth facility until June 30 to allow him to complete his Grade 12. Times Colonist, A6

*** Barrel's a few fish shy of a load**
An opinion piece states "Cataloguing all the ways governments waste tax dollars is the journalistic equivalent of shooting fish in a barrel: It's easy and not very sporting...Now, the feds are talking about cuts, of between five and 10 per cent, to government services and programs it considers only peripherally relevant to most Canadians even as it plans to spend billions on crime, defence and heritage projects for which it either cannot or will not make a cogent case. Lawlessness is decreasing in every category of major offense almost everywhere in the country. But the Tories are determined to send more people to jail for longer just as soon as they liberate enough money from Treasury (that is, borrow enough dough from taxpayers) to build more penitentiaries. They say their share of the price tag will amount to a comparatively measly

$79 million over five years. Quebec's Minister of Public Security says, however, it expects the crime bill will cost the province more than $300 million, alone..." Moncton Times and Transcript, D6

PUBLIC SERVICE / FONCTION PUBLIQUE

MP pensions 'a ripoff on a massive scale'
The Canadian Taxpayers Federation says it's high time MPs stopped making Canadians pick up the tab for their "gold-plated" pension plan. "This is a ripoff on a massive scale," the advocacy group's federal director, Gregory Thomas, said at a news con-ference on Parliament Hill Wednesday announcing its report on parliamentarians' pensions. Treasury Board President Tony Clement said he is examining the issue of MP pensions as part of the larger government-wide spending review. He said the government's first step was to freeze MP salaries. Ottawa Citizen, A1 (Daily Gleaner)

INTERNATIONAL / INTERNATIONAL

* **Where's my copy of Good Cavekeeping?**
A copy of an al-Qaida-linked magazine was delivered to the Guantanamo detention camp for suspected terrorists, a military prosecutor revealed on Wednesday during a court discussion of mail security. The camp commander, Rear Admiral David Woods, issued orders last month tightening the screening of mail sent by lawyers to their clients at the camp that holds 171 captives on the Guantanamo Bay U.S. naval base in Cuba. Toronto Sun, 45

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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: January-18-12 12:06 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous publishes hacked Stratfor emails

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Inquirer
Complete item: http://www.theinquirer.net/inquirer/news/2139335/anonymous-publishes-hacked-stratfor-emails

Description:
HACKTIVIST GROUP Anonymous has released two sets of teaser emails retrieved from a recent attack on servers at the security intelligence firm Stratfor.

The well-known group successfully targeted the firm recently and managed to access its customers' credentials including unencrypted credit card details. It also got hold of internal emails. which it has started to publish online.

Anonymous has posted two teaser emails on Pastebin that were obtained in the hacking attack. The first is a strange set of emails containing abuse and even a marriage proposal involving Michael McCullar, senior editor of special projects at Stratfor.

E-Secure-IT
https://www.e-secure-it.com

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-18-12 9:06 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Adams, John; Allison, Catherine; Arruda, Filo; Baker, William V.; Black, Dave; Bougie, Jo-Anne; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Contant, Joanne; Crépeault, David; CSIS Media Monitoring; CYBERDO; Dauray, Michelle; De Curtis, Laura; Dicerni, Richard; Donato, Renée; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Fonberg, Robert; Forand, Liseanne; Gagnon, Genevieve; Gilbert, Monica; Hannan, Andrew; Hebert, Brigitte; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Kirvan, Myles; Leonidis, Nelly; MacKenzie, Sara; Malboeuf, Julie; McAllister, Andrew; McMillan, Lucie; Natynczyk, Walt; Nolan, Corinne; Panthaky, Jasmine; Parisi, Francesca; Patry, Line; Patton, Michael; Paulson, Robert; RCMP Emerging Trends; Rigby, Stephen; Roberts, Shane; Robinson, N.; Rosenberg, Morris; Rousseau, Johanne; Ryan, Calum; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Woolridge, Theresa; Akman, David; Ashley, Anthony; Babinsky, Antoine; Baker, Christine; Boucher, Pierre; Brinston, Elizabeth; Bruce, Shelly; Buck, Kerry; Campbell, Julie; Carmanico, Shirley; Castonguay, Francis; Chan, Kendrick; Charette, Corinne; Chenier, Maurice; Clairmont, Lynda; Couillard, Daniel; Danek, Jirka; DeJong, Michael; Desaulniers, Annie-Sylvie; Diorio, Colleen; Dupuis, Marc; Dvorkin, Corey; Fortin, Marc; Gallivan, Jim; Glauser, Mark; Glover, Barbara; Green, Martin; Hampton, Sandra; Hatfield, Adam; Hervato, Sandro; Houston, Laura; Jones, Scott; Labelle, Sébastien; Lalonde-Galea, Line; Lane, Richard; Loos, Gregory; Marcoux, Rennie; McDonald, Helen; ; Mitchell, Guy; Moffa, Toni; Montpellier, Kim; MScriven@justice.gc.ca; Oldham, Craig; Ossowski, John; Pelletier, Sandra; Pickett, Tony; Pilon, Claude; Pilon, Daniel; Piragoff, Donald; Rosen, Andrea; Routhier, Carole; Saab, Samar; Sinclair, Jill; Slatkoff, Ari; Smith, Maggie; Soper, Lesley; Stewart, Jennifer; Therrien, Daniel; Turner.JM2@forces.gc.ca; Vallerand.AL@forces.gc.ca; Wilczynski, Artur; Wong, Suki
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 18, 2012/ le 18 janvier 2012

Print Media / Médias imprimés

Cyber threats likely to increase
Any organization that believes it has shuttered all of the back door channels that hackers used to breach millions of systems last year should double check the locks in 2012, according to security experts. A cyber threat forecast by Kaspersky Lab, a Moscow Internet security firm, warns there is little doubt the cloud-based storage hack that took down Sony's PlayStation Network for more than a month will spread beyond gaming companies. The June hack of U.S.'s Citibank's database that stole information from more than 200,000 customers might not be an anomaly, the forecast said. And cyber weapons such as the Stuxnet worm that took down Iran's nuclear weapons program are expected to increase in numbers, even as hacks made in protest by so-called hacktivist organizations such as Anonymous will continue unabated. Even as the report warns everyone to gird for the attacks that are all too familiar, it also outlines emerging threats to mobile phones and energy company infrastructure. Red Deer Advocate, D7

Microsoft phone scam to blame for 70% of reports

A scam where callers pretend to be Microsoft employees offering to solve computer problems now accounts for 70 per cent of all fraud complaints in Canada, reports the Canadian Anti-Fraud Centre. The fraud artists claim they are with Microsoft and offer to help people rid their computers of malicious software. In the process, they charge as much as $400, collect credit card information and gain access to all of the personal files and contents on their victim's hard drive. According to the RCMP, the scam has been operating since February 2011. The RCMP said fraud has been elevated to new levels thanks to the emergence of the digital era. It is believed that Canadians are defrauded of between $10 billion and $30 billion annually. Ottawa Citizen, A1

Nouveaux outils de censure
L'encyclopédie collaborative en ligne Wikipedia a annoncé qu'elle suspendrait l'accès à sa version anglophone sur le Web toute la journée d'aujourd'hui pour protester contre une loi antipiratage examinée par le Congrès américain. Wikipedia, qui reçoit des millions de visites chaque jour, est considérée comme l'un des sites Web les plus populaires d'Internet. La fondation Wikipedia a fait valoir dans un communiqué que la loi «causerait du tort à Internet gratuit et libre et fournirait de nouveaux outils de censure des sites internationaux aux États-Unis». D'autres acteurs de poids d'Internet, comme Google, Facebook, Yahoo, Twitter, eBay et AOL sont contre la nouvelle législation. Plusieurs communautés en ligne, dont Reddit et Boing Boing, ont également prévu des opérations écran noir. Le Soleil, 35; Montreal Gazette

Father, son blamed for credit thefts
U.S. authorities on Tuesday unsealed criminal charges accusing a father and son team, both Russian citizens, of hacking into U.S. bank accounts and illegally snatching credit card numbers and stealing hundreds of thousands of dollars. Windsor Star, C2

Online Media / Médias en ligne

Trojan may have stolen data from Japanese space agency
Japanese space engineers have discovered a Trojan on an employee's computer and confirmed that hackers may have smuggled out login information to gain access to a cargo shuttle that carries food and equipment to the International Space Station (ISS). The compromised information may have included up to 1,000 email addresses, login details for the Japanese space agency's intranet, and NASA documents covering operation of the ISS, according to a statement from the Japanese Aerospace Exploration Agency (JAXA). On January 6th, JAXA found the virus on a terminal used by an employee who works with the H-II Transfer Vehicle (HTV), an unmanned cargo shuttle. Naked Security

Context warns of sophisticated new Trojans
Security consultancy, Context Information Security, has issued a warning regarding the sophisticated structure of financial malware, such as the Carberp Trojan, which is both difficult to detect and eliminate. Carberp targets log-in and account information, and harvests credentials for both email and social networking sites. Like its predecessors Zeus and Spyeye, Carberp operates through drive-by downloads and malicious files. Carberp remains undetected by antivirus software due to its advanced stealth, anti-debugging and rootkit techniques, composed of multiple layers of obfuscation and encryption. Context researchers have published a series of blogs that detail the process of their analyses. ARN Net

New stealthy botnet Trojan holds Facebook users hostage
A new strain of cybercrime Trojan is targeting Facebook users by taking over their machines and shaking them down for cash. Carberp, like its predecessors ZeuS and SpyEye, infects machines by tricking punters into opening PDFs and Excel documents loaded with malicious code, or attacks computers in drive-by downloads. The hidden malware is designed to steal account information, and harvest credentials for email and social-networking sites. A new configuration of the Carberp Trojan targets Facebook users to ultimately steal e-cash vouchers. Previous malware attacks on Facebook have been designed purely to slurp login info, so this latest skirmish, spotted by transaction security firm Trusteer, can be considered something of an escalation. The Carberp variant replaces any Facebook page the user navigates to with a fake page notifying the victim that their Facebook account is temporarily locked. Effectively holding Facebook users hostage, the page asks the mark for their first name, last name, email, date of birth, password and a Ukash 20 euro ($25) voucher number to verify their identity and unlock the account. Trusteer warns the cash voucher attack is in some ways worse than credit card fraud, because with e-cash it is the account-holder, not the financial institution, who assumes the liability for fraudulent transactions. The Register; Techworld

Microsoft hit by email scam
Fraudsters have attacked customers of the oft-targeted Microsoft with a phishing scam offering a £500,000 ($A739,000) financial reward. The scammers, masquerading as representatives of "Microsoft Office", offered the "financial aid award" to email recipients while requesting their personal information. The email purported to originate from an "LGHealth Email Service" in association with Microsoft. It mimicked the nature of legitimate email communication with a "confidentiality

notice" urging victims to contact the sender by reply email and destroy all copies of the original message if not the intended recipient. The scam is the latest in a series of phishing operations targeting Microsoft users. CRN

Phishing your employees in the name of security
A new open source toolkit makes it ridiculously simple to set up phishing websites and lures. The software was designed to help companies test the phishing awareness of their employees, but as with most security tools, this one could be abused by miscreants to launch malicious attacks. The Simple Phishing Toolkit includes a site scraper that can clone any web page — such as a corporate intranet or webmail login page — with a single click, and ships with an easy-to-use phishing lure creator. Sydney Morning Herald

Flaw in Facebook & Google Allows Phishing, Spam & More
Here's a nasty little Null Byte. An open redirect vulnerability was found in both Facebook and Google that could allow hackers to steal user credentials via phishing. This also potentially allows redirects to malicious sites that exploit other vulnerabilities in your OS or browser. This could even get your computer flooded with spam, and these holes have been known about for over a month. Normally, holes like this are fixed within a few hours, but Google and Facebook don't seem to care too much. Google does not offer their regular Vulnerability Reward for this kind of exploit. So, we will be going over how this exploit could be used against us and how to protect ourselves from it. Maybe this will encourage Google and Facebook to push their developers into fixing these holes as soon as possible. Business Insider

McAfee software lets scammers hijack PCs to send spam
McAfee is looking into a problem with a service in its SaaS Endpoint Protection software that appears to be allowing computers to serve as open proxies for sending spam, the company told CNET today. The problem was reported by McAfee customers on the Web who complained that their e-mails were being blocked by e-mail providers and their IP addresses were being blacklisted for sending spam. The problem appears to be in the RumorServer Service myAgtSvc.exe, McAfee Peer Distribution Service, which is part of McAfee SaaS Endpoint Protection Suite, previously known as Total Protection Service, according to the Kaamar Blog. The technology, used for delivering updates to computers without a direct Internet connection, serves as an Open Proxy on Port 6515, which effectively opens the computer up to being used by spammers to use the computer to send spam to other sites that looks like it is coming from that IP address, the blog post says. CNet; eSecurity Planet; IT Pro Portal

Phishing your employees in the name of security
A new open source toolkit makes it ridiculously simple to set up phishing websites and lures. The software was designed to help companies test the phishing awareness of their employees, but as with most security tools, this one could be abused by miscreants to launch malicious attacks. The Simple Phishing Toolkit includes a site scraper that can clone any web page — such as a corporate intranet or webmail login page — with a single click, and ships with an easy-to-use phishing lure creator. Sydney Morning Herald

Facebook "Free Mobile Recharge" scam hijacks accounts
A phishing and survey scam rolled into one is currently targeting Facebook users and ends up hijacking their accounts and making it difficult for users to get them back, warns a McAfee researcher. The victims are lured with messages seemingly posted by their friends claiming that they have received a "100rs free recharge". Following the offered link, they land to a page asking them to enter their Facebook login credentials in order to get it. The scammers then use the login credentials to access the victims' Facebook accounts, change information contained in them (including the password and the email address) and post the same message that lured in the victims in the first place. Help Net Security

Phishing E-mail Scam Attacks US-CERT
US-CERT the United States Computer Emergency Readiness Team reports that it's presently a target of an enormous phishing campaign. SCMagazine.com.au published this on January 11, 2012. It's worth noting that US-CERT coordinates security measures as well as deals with cyber assaults all over the USA. Moreover, it's run under the U.S. DHS (Department of Homeland Security). The Computer Emergency Response Team, following the latest phishing scam's appearance on January 10, 2012, issued an online security alert to all Internauts, stating that the cyber-criminals had impersonated the electronic mail addresses of US-CERT so they could target many local, state and federal governments along with private sector companies. Also an e-mail handler working at US-CERT stated that the phishing e-mail scam had been causing him trouble in receiving messages. The phishing message reportedly, has a .zip file as an attachment, which carries one malicious .eml.exe executable named "US-CERT Operation Center Reports." Captioned as "Phishing incident report," the e-mail contains one telephone number too. The sender's id displayed as soc@us-cert.gov is spoofed to make the e-mail appear from US-CERT; however, the agency points out other illegitimate ids that are also included. SPAMfighter

Malware targets smart ID cards, say researchers

Cybersecurity researchers say they've uncovered a variant of malicious software known as Sykipot that specifically targets smart identity cards used by a number of federal agencies, including the departments of Defense and Homeland Security. In a July 12 blog post, researchers from alienvault labs say the variant appears to have been compiled in March 2011. Once downloaded onto a computer via a phishing attack (in which an email containing an infected attachment or link to a malware-controlled website appears to originate from a legitimate source), the Sykipot variant uses a keylogger to steal PINs users enter to authenticate their identity, the Campbell, Calif.-based company says. Fierce Homeland Security

Israël: des pirates affirment avoir touché le site de la bourse saoudienne
Un groupe de pirates informatiques israéliens a affirmé mardi s'être introduit sur les sites des bourses de Ryad et d'Abou Dhabi, pour répliquer à des cyberattaques lancées la veille contre plusieurs sites israéliens, ont rapporté des médias israéliens. La Presse; Arutz Sheva; Financial Times

Saudis deny stock exchange website infiltrated by Israeli hackers
Saudi Arabian authorities on Wednesday denied claims that Israeli hackers had crippled the website of the oil-rich country's capital market, saying the system was operating normally. Israeli hackers claimed they brought down the websites of both the Saudi Stock Exchange (Tadawul) and the Abu Dhabi Securities Exchange (ADX) on Tuesday, in the latest episode of a continuing cyber war between hackers in Israel and other countries. The Israeli hackers, who go by the name IDF-Team, said on Tuesday they were able to paralyze the Tadawul website, while causing significant delays to the ADX exchange site. Haaretz

Facebook, Researchers Reveal Gang Behind Koobface Virus
Facebook said Tuesday that it will share the data it has collected about the group of people behind the Koobface virus that hit the social network in 2008. Koobface targeted Facebook users via fake friend messages that encouraged people to click on links that installed a malicious worm. Facebook said Tuesday that it will share the data it has collected about the group of people behind the Koobface virus that hit the social network in 2008. Koobface targeted Facebook users via fake friend messages that encouraged people to click on links that installed a malicious worm. Security researcher Dancho Danchev has also posted his analysis of the Koobface gang online. According to the research, Koobface scammers basically got sloppy. The "Koobface Mothership" was found to be in Prague, but researchers also found that daily stats were being sent via text messages to Russian telephone numbers. Ultimately, the Koobface gang was identified by the researchers as Anton Korotchenko, Alexander Koltyshev, Roman Koturbach, Syvatoslav Polinchuk, and Stanislav Avdeik. PC Magazine; The Register; redOrbit; Herald Sun; ZDNet; Forbes; The Telegraph (UK)

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

Hayward, Jane

From: Glazer, David on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-18-12 8:01 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 18, 2012 / le 18 janvier 2012

MINISTER / MINISTRE

Pilot dies in RCMP chopper crash
RCMP pilot Dave Brolin died Tuesday after a training exercise with the emergency response team turned into a real-life emergency. **"I would like to extend my heartfelt condolences and deepest sympathy to the family, friends and colleagues of Dave Brolin who lost his life today," Public Safety Minister Vic Toews said in a statement.** The Province, A3

Letters to the Editor Column
A letter states, "Brian Lilley is right on the money when he says "it's time for **(Vic) Toews** and the rest of the Harper government to wake up and fix this mess." Confiscating legally owned property without compensation is the kind of thing one would see in banana republics..." Winnipeg Sun, 8

EMERGENCY MANAGEMENT AND NATIONAL SECURITY / GESTION DES MESURES D'URGENCE ET SÉCURITÉ NATIONALE

*** It was a long dam wait**
Sakimay First Nations could receive a $21-million settlement to satisfy a longstanding flood claim, following years of negotiations with the federal and provincial governments, Chief Lynn Acoose said Tuesday. The federal government has also made an offer to settle with Cowessess First Nation, although it has not make the dollar figure public. Leader-Post, A3

*** 500 000 masques dorment chez Élections Canada**
La peur de la grippe A (H1N1) durant la pandémie, en 2009, a poussé Élections Canada à surprotéger les électeurs, si bien que près de 500 000 masques chirurgicaux et des milliers de bouteilles de désinfectants pour les mains dorment toujours dans les bureaux de l'agence gouvernementale. Selon les informations obtenues par le Journal en vertu de la Loi d'accès à l'information, Élections Canada cherche d'ailleurs à se départir de ces articles, dont la plupart sont périmés ou sur le point de l'être. Journal de Montréal, 6

NATIONAL SECURITY / SÉCURITÉ NATIONALE

*** Canada joins military satellite program**
The federal government will spend more than $337 million on military satellites designed to help soldiers in the field stay informed, and keep government information secret. Defence Minister Peter MacKay said Tuesday that by joining the $10-billion Global Wideband Satellite program, or Mercury Global, Canada will be able give soldiers in the field real-time analysis as events unfold anywhere around the globe. The federal government will spend $337.3 million to buy Canada 20 years of access to the satellite network, effective immediately, and fund the construction of one of 10 satellites planned for the network. Leader-Post, B7 (Starphoenix, Windsor Star, Times & Transcript)

CYBER SECURITY / CYBERSÉCURITÉ

*** Cyber threats likely to increase**
Any organization that believes it has shuttered all of the back door channels that hackers used to breach millions of systems last year should double check the locks in 2012, according to security experts. A cyber threat forecast by Kaspersky Lab, a Moscow Internet security firm, warns there is little doubt the cloud-based storage hack that took down Sony's PlayStation Network for more than a month will spread beyond gaming companies. The June hack of U.S.'s Citibank's database that stole information from more than 200,000 customers might not be an anomaly, the forecast said. And cyber weapons such as the Stuxnet worm that took down Iran's nuclear weapons program are expected to increase in numbers, even as hacks made in protest by so-called hacktivist organizations such as Anonymous will continue unabated. Even as the report warns everyone to gird for the attacks that are all too familiar, it also outlines emerging threats to mobile phones and energy company infrastructure. Red Deer Advocate, D7

*** Microsoft phone scam to blame for 70% of reports**
A scam where callers pretend to be Microsoft employees offering to solve computer problems now accounts for 70 per cent of all fraud complaints in Canada, reports the Canadian Anti-Fraud Centre. The fraud artists claim they are with Microsoft and offer to help people rid their computers of malicious software. In the process, they charge as much as $400, collect credit card information and gain access to all of the personal files and contents on their victim's hard drive. According to the RCMP, the scam has been operating since February 2011. The RCMP said fraud has been elevated to new levels thanks to the emergence of the digital era. It is believed that Canadians are defrauded of between $10 billion and $30 billion annually. Ottawa Citizen, A1

*** Nouveaux outils de censure**
L'encyclopédie collaborative en ligne Wikipedia a annoncé qu'elle suspendrait l'accès à sa version anglophone sur le Web toute la journée d'aujourd'hui pour protester contre une loi antipiratage examinée par le Congrès américain. Wikipedia, qui reçoit des millions de visites chaque jour, est considérée comme l'un des sites Web les plus populaires d'Internet. La fondation Wikipedia a fait valoir dans un communiqué que la loi «causerait du tort à Internet gratuit et libre et fournirait de nouveaux outils de censure des sites internationaux aux États-Unis». D'autres acteurs de poids d'Internet, comme Google, Facebook, Yahoo, Twitter, eBay et AOL sont contre la nouvelle législation. Plusieurs communautés en ligne, dont Reddit et Boing Boing, ont également prévu des opérations écran noir. Le Soleil, 35; Montreal Gazette

*** Father, son blamed for credit thefts**
U.S. authorities on Tuesday unsealed criminal charges accusing a father and son team, both Russian citizens, of hacking into U.S. bank accounts and illegally snatching credit card numbers and stealing hundreds of thousands of dollars. Windsor Star, C2

LAW ENFORCEMENT AND POLICING BRANCH / SECTEUR DE LA POLICE ET DE L'APPLICATION DE LA LOI

La commission Charbonneau devra se pencher sur la mafia
La commission d'enquête Charbonneau devrait élargir son mandat et se pencher sur l'infiltration de la mafia dans certains corps publics de la société, souhaite le Parti québécois. Journal Montreal, 2

Retired Montreal cop tried to sell secrets to Mafia
Montreal's police chief is promising swift action after reports that a retired officer allegedly tried to sell information on stoolies to the Mafia. Marc Parent said Tuesday the 33-year veteran of the force worked in the intelligence unit and was one of a handful of people who had access to a confidential list of names. The Guardian, A5 (Globe and Mail, The Record); Journal Montreal; * The Gazette (Windsor Star, Edmonton Journal); * Le Devoir; * Le Soleil; * La Presse

No public inquiry into death
There will be no public inquiry into the death of Paul (Poncho) Henderson, the Miramichi Leader Liberal Miramichi-Bay du Vin MLA Bill Fraser revealed Monday **Department of Public of Safety** officials confirmed they would not push for an inquiry. Months ago, Fraser submitted a petition bearing 2,000 signatures in the legislature calling for the provincial government to order a review of the investigation into the teen's death in 1981. Daily Gleaner, A6

Pilot of RCMP helicopter dies in crash
The pilot and sole occupant of an RCMP helicopter died Tuesday in a crash in British Columbia. He was a civilian member with "several" years of experience with the RCMP and "extensive" experience as a pilot, said Chief Supt. Wayne Rideout, the RCMP E Division's deputy criminal operations officer. Times Colonist, A2 (Leader-Post, Edmonton Journal); The Telegram; * Globe and Mail (Vancouver Sun); * Windsor Star; * Calgary Sun

Experts say spy case could be damaging
The Harper government hunkered down Tuesday in an attempt to weather an unfolding spy drama involving a naval officer who worked at one of the most sensitive and secure military intelligence centres in the country. Prime Minister Stephen Harper, Defence Minister Peter MacKay, the military and the RCMP turned aside questions on the case of Sub.-Lt. Jeffrey Paul Delisle, who's charged with communicating information to a foreign entity. Defence experts said, given where the suspect worked, the potential damage to national security was immense. The Guardian, A5 (Red Deer Advocate, Hamilton Spectator, Chronicle-Herald); * Globe and Mail; * Windsor Star (Telegraph-Journal); * Whig-Standard; * The Record; * Chronicle-Herald; * Chronicle-Herald; * Chronicle-Herald; * Journal Montreal

Bank documents questioned in trial of Mountie accused of fraud
Admissibility of a bank of evidence has been called into question in the trial of a Mountie accused of extortion, criminal harassment and fraud. RCMP Const. Hoa Dong La, in a judge-alone trial before Justice David Gates in Red Deer Court of Queen's Bench, is accused of using a variety of tactics for monetary gain involving five different properties in Innisfail and Bowden and in the rural area near Bowden Institution. He faces 15 counts altogether, including three counts of extortion, two of criminal harassment and 10 of mortgage fraud. Red Deer Advocate, A3

*** New police watchdog hits ground running**
A dinner conversation with his father years ago helped set Richard Rosenthal, the new director of B.C.'s independent police investigations office, down a path that would one day see him investigate judges and take on the Los Angeles Police Department. As the head of an office that probes police incidents that result in serious harm or death, Rosenthal will inevitably be thrust into an adversarial role with B.C.'s municipal police forces and, perhaps more dramatically, with a provincial RCMP force that's still seeing double after a string of black eyes. The Province, A4

*** Le député de Manicouagan appelle la GRC en renfort**
Ottawa doit demander à la GRC d'intervenir "de manière musclée" contre les trafiquants d'amphétamines (speed) dans les communautés innues du Québec, affirme le député fédéral de Manicouagan, Jonathan Genest-Jourdain. La Presse, A6

*** Roberval**
Neuf arrestations ont été faites à Roberval, hier, au terme de 12 perquisitions menées par la Sûreté du Québec et la Gendarmerie royale du Canada. L'opération Intérim a mobilisé 90 policiers. Les personnes ont été mises en état d'arrestation pour leur participation à un réseau organisé de trafic de stupéfiants au Lac-Saint-Jean. La Presse, A14

*** L'enquête s'est échelonnée sur plus d'un an**
L'opération de lutte antidrogue "Intérim", qui a été menée hier par la Sûreté du Québec et la Gendarmerie royale du Canada (GRC), est le fruit d'une enquête qui s'est échelonnée sur une période de plus d'un an. Le Quotidien, 6

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Affaire Pickton
Le fait que la GRC ait possédé pendant cinq ans des preuves liant Pickton à deux prostituées disparues a été présenté comme une preuve que les policiers travaillant sur l'affaire ont été incapables d'empêcher le tueur en série d'assassiner davantage de femmes. L'avocate de la GRC Cheryl Tobias a cependant indiqué qu'il n'y avait jamais eu de raison d'examiner les vêtements pour y trouver de l'ADN, puisque l'identité du suspect et celle des victimes étaient connues. Pickton n'a jamais nié son implication, mais a plutôt clamé l'autodéfense. La Presse, A14

No reason for DNA test in 1997: lawyer
Suggestions that the RCMP should have tested clothing seized from Robert Pickton in 1997 for DNA sooner are hindsight, but the facts are there was no reason for investigators working on an attempted murder case at the time to test them, a federal government lawyer told a public inquiry. Mr. Pickton's clothing and a pair of handcuffs were seized after a brutal attack on his farm in Port Coquitlam, B.C., which left a prostitute from Vancouver's Downtown Eastside near death with severe stab wounds. Globe and Mail, S2 (Red Deer Advocate)

*** RCMP made mistake refusing Pickton's offer, inquiry told**
Two RCMP officers should have followed up on an offer by serial killer Robert Pickton to let them search his farm as early as 2000, the Missing Women Inquiry heard Tuesday. Leader-Post, B10 (Edmonton Journal, Times Colonist)

*** Ontario cop at odds with RCMP lawyer**

An Ontario deputy police chief on the stand at the Missing Women Commission of Inquiry refused Tuesday to agree with an RCMP lawyer that there was no point in the Mounties accepting Robert Pick-ton's invitation to search his farm in 1999. Jennifer Evans, Peel Region-al Police deputy chief who analyzed the police probe into Pickton, produced a 2010 report that documents that cops knew for years that Pickton's farm was rife with evidence. The Province, A14

*** Gaps in policing must be bridged**
An editorial states, "Jennifer Evans, the deputy police chief in the Peel regional police in Ontario, didn't offer much that we didn't already know when she spoke at the Missing Women Commission of Inquiry this week. We already knew what she had to say. There is really only one question: Will police act on that knowledge? Evans told the inquiry that it is still possible for serial killers such as Robert Pickton and Paul Bernardo to escape detection by operating in more than one police jurisdiction..." Times Colonist, A12

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** Yank busted for kid porn**
A Minnesota man has been arrested and detained in Manitoba to face allegations he was trying to smuggle explicit child pornography into Canada. Kirk Douglas Therneau, 54, was arrested by Canada Border Services Agency investigators at the Emerson border crossing Sunday and transported to Winnipeg where his charges appeared in court Tuesday. Winnipeg Sun, 7

*** Legal aid being cut off to Roma, lawyer says**
An Ottawa refugee lawyer says Legal Aid Ontario has started to deny funding to most Roma asylum-seekers, but won't explain why. Without legal representation, Kaplan said, his Roma clients, who are illiterate and speak no English, have little chance of success before the IRB. If their claim is denied, they'll be deported back to Poland, where Kaplan said they'll face violent threats from neo-Nazis and systemic discrimination in education, employment and health services. Ottawa Citizen, C1

*** Refugee bid felled by crimes in Punjab**
A refugee claimant who settled in Montreal with his wife after leaving his long-time job with a paramilitary force in India has been ordered out of Canada for complicity in crimes against humanity during the brutal suppression of a separatist insurgency in the Punjab. National Post, A6

*** Une autre voix s'élève contre la déportation de Mugesera**
Alors que Léon Mugesera est toujours détenu au Centre de prévention de l'immigration de Laval en attendant son éventuelle déportation, une autre voix s'est élevée hier contre la décision d'Ottawa de retourner le Rwandais accusé d'incitation au génocide dans son pays d'origine pour qu'il soit jugé devant ses pairs. Le Soleil, 4

*** Send Mugesera back**
A letter states, "...The obvious thing to do, of course, is to send Léon Mugesera back to Rwanda, to be judged by the people of his own country. If the Anti-Torture Committee is worried that he will be mishandled there, let it insist on being allowed to appoint its own representatives to follow the judicial proceedings there. But this might, of course, be too much real work for said committee." The Gazette, A18

*** Seeking new life, finding gang life**
They come from a war-torn nation looking for a fresh start in Friendly Manitoba. Yet, some African immigrants have learned the kindness only extends so far, and a failure to comply with the law can mean a ticket back home. As a boy in Somalia, Yassim Ibrahim saw his father murdered. He immigrated to Winnipeg in 1999 with his mother and four siblings, and in less than 10 years, at age 23, he was the godfather of the Mad Cowz street gang. His criminal record included the attempted murder of a rival gang member. Ibrahim was deported back to Somalia. Winnipeg Free Press, A4

*** Pharma boss faces U.K. extradition for stolen drugs**
The former head of a Richmond pharmaceutical company is facing extradition to the United Kingdom after being caught allegedly possessing $9-million worth of stolen drugs in 2007. A committal hearing for Mahmood Sheraly Aziz is scheduled for B.C. Supreme Court in Vancouver next week. Aziz, who was arrested in Canada last March, is out on bail, according to the federal justice branch. Vancouver Sun, A2

*** Deportation order deferred**
Lucene Charles's removal from Canada has been deferred, according to a letter received by Charles and her supporters. On Monday, the Canadian Border Services Agency (CBSA) faxed the reprieve letter to one of her supporters. It reportedly says her deportation to the Caribbean island has been deferred until further notice. The letter was read aloud

to The Spectator by Charles and two of her supporters, including Archdeacon Rick Jones of St. Paul's Anglican Church. Hamilton Spectator, A2; Hamilton Spectator

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Stiffer ecstasy laws spark turn to new pills
New tough laws cracking down on ecstasy production in British Columbia have had the unintended consequence of opening the door to more toxic, fake ecstasy pills, a criminologist says. The synthetic drug PMMA wasn't on the radar for police or the public until last week, when the BC Coroners Service announced the "new" unregulated chemical had been linked to at least five ecstasy-related deaths in B.C. in the past six months, and a number of deaths in Alberta. Leader-Post, B7

*** Haitian-born killer granted aboriginal parole hearing**
When convicted murderer Gregory Bromby faces a Winnipeg parole board on Wednesday, the hearing will be conducted in a circle rather than across a table, the smell of burning sweetgrass, cedar or tobacco will likely fill the room due to a ceremonial process known as "smudging" and an aboriginal elder will open and close the hearing with a prayer. Bromby has requested an "aboriginal elder-assisted parole board hearing." The thing is, the Haitian-born 34-year-old is not aboriginal. National Post, A1, Edmonton Sun (Winnipeg Sun), La Voix de l'Est

*** Legal pot**
An editorial states... "In the meantime, on The Gazette's Facebook page (facebook.com/ montrealgazette), we asked readers whether they think there should be a Gazette editorial endorsing legalization. Here are some responses: 'I don't use it myself but yes, it should be legalized. Regulate and tax it as we do alcohol. When drugs are available in prison, you know you've pretty much lost the war on drugs. If marijuana is going to remain illegal then you'll have to ban alcohol, too. End the hypocrisy.'..." The Gazette, A19

*** City sex offender jailed**
A sex offender who admitted to failing to apprise authorities he'd moved was sentenced to 30 days behind bars Tuesday. Toby Peter Lloyd Forrest, 38, of 72 Regent St., Apt. 123, pleaded guilty in provincial court Tuesday failing to register as a sex offender as required by a court order between March 31, 2010, and Oct. 12, 2011, and failing to notify the sex offender registry of a change of address. Daily Gleaner, A6

*** Violent gangster may be in Manitoba: RCMP**
A violent gang member is eluding cops and could be in Manitoba. Thomas Gordon Bear was released from Saskatchewan Penitentiary on Aug. 2, on parole for a 45-month sentence. Police say he walked away from his halfway house Sept. 19. RCMP then issued a Canada-wide warrant for his arrest. Bear is a known member of the Native Syndicate, Mounties say. Winnipeg Sun, 13

*** Judge reserves decision on defence of necessity**
Justice Rommel Masse will give his decision in March on whether eight hold-out Save Our Prison Farm protesters are entitled to a defence of necessity, covering their methods in trying to prevent removal of the dairy herd from Frontenac Institution in August 2010. The eight were all charged individually with mischief by inter-f ering with the lawful use of property, during a two-day demonstration centred on the main access road into Collins Bay Penitentiary and the adjacent Frontenac Institution. Kingston Whig-Standard, 1

*** Database opens door to drug dens' pasts**
A new Ottawa company will list homes that housed former drug operations on the first registry of its kind in the country. HomeProof, set to launch next month, will provide insurance claim information, as well as the criminal pasts of houses to realtors -- for a fee. Ottawa Sun, 6

*** Warrant out for sex offender**
Vancouver police are searching for Kevin Scott Miller, wanted Canada-wide for breach of a long-term supervision order. Miller has a history of sex offences involving women and teenage girls. Police believes he is at high risk to re-offend violently and sexually. Toronto Sun, 30

*** Judge spares lifetime con lengthy prison sentence**
Joseph Davis has spent a lifetime proving he can't function in society for long before turning back to crime and ending up behind bars. But the Winnipeg drifter's grim history and bleak outlook wasn't enough to stop a Manitoba judge from giving

him one more chance to succeed. Davis, 43, was spared an indefinite prison sentence Friday after the Crown lost its battle for a rare dangerous offender designation. Winnipeg Free Press, B3

*** Hallelujah! Canadians agree it's time to legalize marijuana**
An opinion piece states, "A new poll suggests Canada may have reached the tipping point and a 66-per-cent majority favours legalizing marijuana. Hallelujah! Finally we might get a sensible public policy discussion in this country about what to do about a relatively benign substance that has been demonized and outlawed for a century yet is as readily available in schoolyards as cigarettes... Let's treat marijuana and other drugs as a health issue rather than a crime. It's cheaper, better for our communities and safer for kids. It would let police focus on real criminals, ease the burden of overloaded, backlogged courts and save a fortune in expensive legal and penal costs..." Vancouver Sun, A5

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Un fardeau de 143 milliards $**
Les divers régimes de pension des employés du gouvernement canadien les fonctionnaires, les policiers, les militaires, les juges, les députés et les sénateurs représentent un imposant boulet financier pour les contribuables canadiens: 143 milliards de dollars. Cette somme représente la totalité des engagements financiers non capitalisés du gouvernement fédéral envers les caisses de retraite de ses employés au 31 mars 2010, selon des documents obtenus par La Presse en vertu de la Loi sur l'accès à l'information. Le Nouvelliste, 18 (Le Droit)

*** Tory spending cuts are welcome news**
An editorial states, "Those concerned with the Harper government's rather liberal spending patterns -- that would be us -- were somewhat pleased with the new report coming out of the Parliamentary Budget Office that the brakes have already been applied. The credit card has been put away... Parliamentary budget chief Kevin Page has now told us that Ottawa has cut back on its spending -- very quietly, obviously -- by 3% over the first six months of the current fiscal year. If this holds true, it puts the Harper government on the right path towards its promised 5% cut to its estimated $80-billion direct program funding budget by 2013-14. Spending on operating expenditures, for example, is down 4%, and capital spending is down a whopping 15%....Unlike critics from the left, however, we do not mind the spending of money to bolster public safety -- like more than doubling the money spent on the border security agency that is now tracking down and deporting wanted criminals from foreign lands who have found sanctuary within our too-soft borders. Or spending serious dollars to build more prisons so that more violent criminals and sexual offenders get a jail cell rather than a laugh track to undeserved freedom." Kingston Whig-Standard, 4

INTERNATIONAL / INTERNATIONAL

*** Terror suspect avoids deportation**
The radical cleric Abu Qatada won his case to avoid being deported to Jordan Tuesday after judges ruled his human rights would be breached. The European Court of Human Rights said that Qatada, once described as Osama bin Laden's righthand man in Europe, could not be sent to Jordan because there was a risk he would be tried with evidence gained by torture, which would amount to a "flagrant denial of justice." However, the Strasbourg court upheld Britain's policy of attempting to deport terrorist suspects to countries that have given assurances that they will not use inhuman treatment. Ottawa Citizen, A13; National Post; Edmonton Journal

OTHER / AUTRE

*** UN gang's key cartel contact gunned down in Mexico**
A B.C. man executed in the Mexican state of Sinaloa this week was a high-ranking member of the United Nations gang who had direct contact with Mexican cartels, The Vancouver Sun has learned. Salih Abdulaziz Sahbaz, 37, spent much of the last three years in Mexico and was the key cartel contact for the notorious B.C. gang, police sources confirmed. Vancouver Sun, A4

*** Suspect charged with trying to kill Obama**
A man accused of firing shots at the White House in November has been formally charged with attempting to assassinate U.S. President Barack Obama, according to an indictment unsealed Tuesday. A preliminary psychiatric evaluation in December found Oscar Ortega-Hernandez, 21, competent to stand trial, but federal prosecutors are asking for more extensive tests to ensure he can be held legally liable. Edmonton Journal, A19

*** Canadian on death row in Iran**

Hope is fading for a Richmond Hill man, Saeed Malekpour, who has lost his final appeal against a death sentence in Iran. "The branch of the Supreme Court responsible for (his) case announced to one of his lawyers that the court reached the decision to have the death sentence carried out," says Maryam Nayeb Yazdi, a Toronto-based human rights activist. Malekpour, a 35-year-old Canadian permanent resident, was awaiting citizenship when he was arrested.
Hamilton Spectator, A8

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

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-17-12 8:00 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 17, 2012 / le 17 janvier 2012

MINISTER / MINISTRE

Naval officer accused of sharing secrets
A Royal Canadian Navy intelligence officer stands accused of sending top secret information to a foreign entity as recently as last week in one of the rarest and most closely guarded investigations to have rocked the military. Court documents filed in Halifax allege that Sub-Lieut. Jeffrey Paul Delisle, 40, broke the federal Security of Information Act and committed criminal breach of trust when he passed restricted information to a foreign agency over the span of more than four years. A **spokesperson for Public Safety Minister Vic Toews** said the **minister** had been briefed on the arrest. "***Minister Toews has been briefed and congratulates the RCMP and security agencies for their collaboration. As this matter relates to national security and is before the courts, we have no further comment,***" **Julie Carmichael** said Monday. Waterloo Region Record, A1 (Toronto Star)

Pot legalization
An editorial states, "he single concrete policy proposal to emerge from the weekend Liberal convention - a resolution urging the legalization of marijuana - is being touted as "controversial." But it shouldn't be. For the last quarter century, a majority of Canadians have supported the decriminalization of simple marijuana possession...In 2006, when asked whether the Tories would do anything to advance the issue of pot decriminalization, then justice **minister Vic Toews** responded: "***It is a very short answer, and the answer is no.***" That's a retrograde attitude. But at least the Tories are forthright about their position on the issue...In her capacity as health minister, and then **public safety minister** under Mr. Martin, Anne McLellan was particularly hawkish in her opposition to marijuana reform - for similar U.S.-centric reasons..." National Post, A12

Police can now confiscate private property!
An opinion piece states, "When Bill C-68, the gun registry bill, was being debated, opponents said the registration of firearms would lead to their eventual confiscation. Now that is happening. Just before Christmas 2011, owners of certain firearms were informed by letter that their rifles had been reclassified as prohibited weapons in Canada and that they must be turned over to police officials. **Public Safety Minister Vic Toews** was asked about this gun registry mess on the Sun News Network, and defended the current situation. "***It is not a decision that I make as a politician; it's something that the police and classification experts make***," **Toews** said...It's time for **Toews** and the rest of the Harper government to wake up and fix this mess." Whitehorse Star, 6

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

*** Blueprint for a plague**
An opinion piece states, "H5N1, a variant of avian influenza, is nasty stuff. It kills somewhere between 50% to 60% of the humans it infects. The good news, if you can call it that, is that while extremely lethal, H5N1 isn't particularly communicable. Fewer than 600 people are known to have contracted it. So if you get it, you're probably in a bad way, but the odds of getting it are long indeed..." National Post, A12

*** Sorting out banned bird flu study**
The World Health Organization says it will take a role in helping sort through an international scientific controversy over two bird flu studies that the U.S. government deemed too dangerous to publish in full. Red Deer Advocate, C3

*** Le système d'alerte de Pointe Lepreau sera mis à l'essai jeudi**

Le système d'alerte en cas d'urgence sera mis à l'essai jeudi prochain dans la région de Pointe Lepreau. La mise à l'essai sera dirigée par l'Organisation des mesures d'urgence du Nouveau-Brunswick en partenariat avec la centrale nucléaire de Pointe Lepreau et Énergie NB. L'Acadie Nouvelle, 10

*** It's not the time to reduce research**
A letter states, "Tucked away on page B6 of the Jan. 12 Times Colonist was a disturbing article reporting that 60 scientists and researchers were being "declared surplus" (fired) at Environment Canada. They are part of 776 personnel to be cut. I wonder why Environment Canada is cutting scientists when Canada is facing serious environmental challenges. The Cohen Inquiry into the failing stocks of salmon in B.C. waters showed the need to monitor and identify viruses in fish from farms and wild salmon, imported or endemic..." Times Colonist, A11

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Navy officer faces espionage charges
A member of the Royal Canadian Navy has become the first person charged under the country's post-9/11 secrets law for allegedly passing protected government information to an unknown foreign body. Sub-Lt. Jeffrey Paul Delisle, 40, was charged Monday under the Security of Information Act, which came into effect in 2001. The navy intelligence officer is charged with communicating information that may "increase the capacity of a foreign entity or a terrorist group to harm Canadian interests." Ottawa Citizen, A1 (Windsor Star, Vancouver Sun, Daily Gleaner, Calgary Herald, Winnipeg Free Press, Chronicle-Herald); Globe and Mail; Edmonton Sun (Calgary Sun, Toronto Sun, Winnipeg Sun, Ottawa Sun); * The Guardian (Hamilton Spectator); * Le Soleil (Le Droit, La Presse); * Journal de Montréal

CYBER SECURITY / CYBERSÉCURITÉ

*** Spying on cyber crime**
The end of the Cold War combined with the advent of the Internet gave rise to an unprecedented wave of electronic espionage and crime. Michel Juneau-Katsuya witnessed first-hand the rise of cyber crime as a senior manager with the Canadian Security Intelligence Service (CSIS) at the time. In 2000, Mr. Juneau-Katsuya left public service to become founding chief executive of security consulting firm Northgate Group. He recently spoke with Financial Post technology reporter Jameson Berkow about the growing digital threat and how companies should respond. The following is an edited transcription of their conversation. National Post, FP8

*** Websites going dark to fight anti-piracy bill**
In the digital world, it's the equivalent of going on strike. Tomorrow, a number of high-profile websites, including Wikipedia, Reddit, Cheezburger Network and Boing Boing, will go dark for up to a day to protest against contentious anti-piracy legislation proposed by the U.S. Congress. The pending legislation would boost the power of the Justice Department to punish foreign websites that infringe copyright. It has also pit Hollywood, which has lobbied for the legislation as a tool to protect content, against Silicon Valley, which sees it as a menace to free speech. Online lobbying efforts to kill the bill already appear to have paid off. On Saturday, the Obama administration signalled it does not support aspects of the pending legislation - the Stop Online Piracy Act - and depicted it as a threat to global innovation. The digital dust-up, however, continues with media baron and Twitter newbie Rupert Murdoch jumping into the fray decrying the Obama administration's stance with a tweet. Globe and Mail, A12

*** Hacker attacks Israeli websites**
The website for Tel Aviv's stock exchange was shut down for hours on Monday after a hacker who identified himself as a Saudi announced that a pro-Palestinian group called Nightmare had targeted the site. El Al Airline, also named by the hacker OxOmar as a target, pre-emptively closed down its own website, directing visitors to a page with a statement that it was under maintenance. In addition, problems were reported on the sites of a few small Israeli banks. Monday's incidents were the latest in a series of attacks on Israeli websites kicked off earlier this month by a hacker who snagged thousands of credit card numbers from a poorly protected site associated with online shopping. Ottawa Citizen, A11; National Post; Telegraph Journal; Le Devoir

*** Online shoe site hacked**
Online shoe retailer Zappos told customers it has been the victim of a cyber attack affecting more than 24 million customer accounts in its database. The popular retailer, owned by Amazon.com, said customers' names, email addresses, billing and shipping addresses, phone numbers and the last four digits of credit cards numbers and scrambled passwords were stolen. But it said the hackers had not been able to access servers that held customers critical credit card and other payment data. Times Colonist, B2

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Kakeeway arrested near Swift Current
Sgt. Paul Dawson says it was "good police work" on Saturday that led to RCMP in Swift Current arresting a Winnipeg man wanted for murder in his hometown. Leader-Post, A3

What you said ...
Q. Does Canada need a national DNA databank for missing people? Yes 53% No 47%...The mother of an Edmonton Edmon man who vanished more than three years ago is helping push a bill into Parliament that could create a national DNA bank for missing people...That DNA bank would collect and store samples of the missing, or their relatives, and allow investigators to cross-reference DNA with remains. London Free Press, B4 (Kingston Whig-Standard)

*** Mountie investigated**
A seven-year RCMP veteran, currently posted with the Combined Forces Special Enforcement Unit, is being investigated for impaired driving following a crash on Highway 1 late Sunday. The single-vehicle crash involving the off-duty female Mountie happened at 10: 45 p.m. on Highway 1, eastbound in the area of the 160th Street overpass. The Province, A8

*** RCMP won't pay vet bills for shot dog**
Nancy Stevenson was devastated last summer when her beloved dog was shot twice by a police officer in front of her Shediac home. However, Stevenson is left owing more than $5,000 from veterinarian bills. She has sought reimbursement from the RCMP, but was informed on Friday that they have denied her claim. She complained to police and the RCMP investigated, but Cst. Chantal Farrah, spokesperson for the RCMP's J Division in Fredericton, said yesterday that the investigation revealed that there was no negligence on the part of the officer. Times & Transcript, A3

*** Investigation finds police shooting justified**
A lengthy investigation into a March 2011 shootout that left a 24-year-old man dead and a Fort McMurray RCMP officer wounded has found police acted in self-defence. Edmonton Journal, A4 (Calgary Herald)

*** Un policier du SPVM aurait tenté de vendre de l'information secrète à la mafia**
Un policier du Service de police de la Ville de Montréal (SPVM) aurait tenté de vendre des informations confidentielles concernant les informateurs de la police au crime organisé. Selon ce qu'a rapporté Radio-Canada hier, le policier en cause était un sergent-détective au service des renseignements criminels. Il a pris sa retraite en janvier de l'année dernière après une trentaine d'années de service au sein du SPVM. La Voix de l'Est, 22 (Le Soleil, La Tribune); Journal de Montréal; Journal de Montréal

*** Council beefs up services, approves charters**
Red Deerians will see some differences when it comes to major services approved under the 2012 operating budget. The snow and ice removal budget was beefed up by just over $572,000, boosting the total amount to $2.9 million. Policing and crime prevention were also forefront on the minds of civic leaders. The RCMP's member fee agreement with the city, which pays for about 128 officers, rose by $617,000. A funding request of just over $92,500 was approved to pay for a provincial government shortfall of three Mounties. The RCMP requested a number of new positions - two community peace officers, a criminal analyst position, a court liaison officer position, video capture technician/training and development facilitator, and four RCMP officers (three school resource officers, and one additional officer dedicated to the Mental Health project)... Red Deer Advocate, A3

*** Mountie on trial for fraud**
The first witnesses take the stand today in the trial of an RCMP officer charged with criminal harassment, extortion and mortgage fraud. Const. Hoa Dong La, 47, currently on paid leave, is being tried before Justice David Gates in Red Deer Court of Queen's Bench on 15 counts relating to tenants and properties located in Innisfail and Bowden. At the request of his lawyers, Ian McKay and Heather Ferg, La was allowed to sit with his wife in the public gallery rather than in the box normally reserved for the accused. La served with the RCMP Innisfail detachment before transferring to Calgary to work in the Immigrant and Passport Section. Red Deer Advocate, A1

*** Six pounds of pot seized in Labrador bust**
The RCMP street level drug enforcement team seized a quantity of marijuana recently as part of an investigation into the movement and distribution of illegal drugs into central Labrador and the isolated communities along the Labrador coast. According to police, this investigation resulted in the arrest of a man from Happy Valley-Goose Bay on Jan. 13 and the the seizure of approximately six pounds of marijuana. No charges have been laid. The Telegram, A3

*** New Nanaimo RCMP unit reports major drug bust**
A special unit of the Nanaimo RCMP recently created to target powder drugs is being credited with one of the largest drug busts ever seen in the area. A vehicle stop Friday led to the execution of a search warrant on a Strickland Street home and turned up more than eight pounds of cocaine, crack cocaine, heroin and crystal meth, police said. The RCMP's White Team also found $50,000 in Canadian currency. Times Colonist, A4

*** Ripou**
Un article d'opinion déclare, « Ce que les policiers redoutent plus que le crime organisé c'est qu'un des leurs les trahit. Quand un irréductible policier des enquêtes ou du renseignement décide de changer de camp, les conséquences peuvent en être dramatiques...Merci aux policiers honnêtes qui le pourchassent. On aimerait tous que nos policiers soient parfaits, mais malheureusement certains font exception." Journal de Montréal, 3

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Pickton, Bernardo probes plagued by same failings
The same systemic problems that allowed sex killer Paul Bernardo to rape and murder women undetected in Ontario in the late 1980s and early 1990s contributed to the failure of the Vancouver police and RCMP to catch serial killer Robert Pickton, a public inquiry heard Monday. Deputy Chief Jennifer Evans of Ontario's Peel Regional Police was asked to review the Pickton file for the inquiry, writing a critical report that concluded investigations by both the Vancouver police and the RCMP were plagued by poor communication and a lack of leadership. Globe and Mail, S3 (Waterloo Region Record, Chronicle-Herald, Red Deer Advocate); Leader-Post (The Province, Calgary Herald, Times Colonist); * Vancouver Sun; * Times & Transcript

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Mexican journalist fights deportation
Mexican journalist Karla Berenice Garcia Ramirez, her husband and her two young Canadian-born daughters, are fighting deportation from Canada - and, as they see it, for their lives. She and her husband fled to Canada from Mexico in 2008 after she and her family received death threats that had escalated from less threatening intimidation starting in 2003, the apparent result of her efforts to uncover corruption at a government ministry. She was working at the ministry at the time, but had previously been employed as a journalist. Globe and Mail, S2

*** Tofino man grounded by U.S. border rigidity**
Even the judge rolled his eyes, gave Adrian Dorst a suspended sentence when the then 24year-old got busted for having marijuana resin in a decorative pipe way back in 1967. But American authorities were dead serious when they discovered the Tofino man's 45-year-old conviction last week. They refused to let him fly through the U.S., costing the well-known nature photographer a $1,250 airline ticket and a "dream trip" to the cloud forest village of Mindo, Ecuador. Times Colonist, A3

*** Mugesera reste détenu**
Le présumé criminel de guerre rwandais, Léon Mugesera, qui fait l'objet une ordonnance d'expulsion vers son pays d'origine, devra demeurer détenu en attendant son renvoi prévu pour vendredi, a décidé hier après-midi la Commission de l'immigration et du statut de réfugié (CISR). Le gouvernement conservateur estime toutefois qu'il sera bien traité et qu'il doit être expulsé du Canada. Le gouvernement rwandais a également assuré Ottawa que Mugesera sera traité humainement. Journal de Montréal, 12; Le Soleil; The Guardian; Le Devoir (Le Droit); Globe and Mail; Montreal Gazette; London Free Press (Toronto Sun, Kingston Whig-Standard); Vancouver Sun

*** MP protests border toll 'gouge'**
Differences in the currency exchange rate are costing travellers millions of dollars at Windsor's two border crossings, says MP Brian Masse (NDP - Windsor West). Despite a currency exchange that has been close to par the past couple of years, the loonie is undervalued compared to the U.S. dollar at the Ambassador Bridge and Windsor-Detroit tunnel. Windsor Star, A3

*** Refugees may look south**
For years, Canada has had one of the most generous immigration policies in the world, welcoming tens of thousands of asylum applicants who claim to be fleeing persecution in their homelands. But Canada's Conservative government has begun rolling up the welcome mat, increasing efforts to track down and deport thousands of asylum-seekers whose

applications have been denied. The clampdown is likely to be felt not just across Canada, but in the United States. Vancouver Sun, B4

*** 7,5 kg de cocaïne déjà en janvier**
L'année 2012 n'est vieille que de deux semaines et, déjà, les employés de l'Agence des services frontaliers du Canada (ASFC) ont effectué deux importantes saisies de cocaïne à l'aéroport Montréal-Trudeau. Au total, 7,5 kg de cette drogue ont été interceptés, pour une valeur de 340 000 $. Journal de Montréal, 5

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

It's a perilous - and political - road from 'evidence' to policy
An opinion piece states, "Too much is being made of Liberals voting 77% in favour, at this past weekend's convention, to legalize marijuana. It is an excellent idea, and the resolution ticks all the correct boxes by way of justifying it: marijuana's widespread and safe use, revenue savings and generation through taxation, and the fact it would make Canadians safer from criminal violence... But as Mr. Rae illustrated with his comments on marijuana, the road from evidence to policy will always be long, perilous and political. To pretend otherwise is to insult Canadians' intelligence." National Post, A15; * Red Deer Advocate, * L'Acadie Nouvelle

Dorval man says daughter's killer needs to stay in jail
Almost 18 years after finding his daughter, Tara Manning, fatally stabbed inside their Dorval home, Michael Manning is flying to Winnipeg to try to persuade the Parole Board of Canada to keep her killer behind bars. Manning said he wants to tell the parole board on Wednesday that Gregory Bromby, 34, is not ready for parole and should not be permitted to live in a halfway house. Gazette, A4

Killer abandons plan to seek early parole
A man convicted of killing his distant cousin in London 15 years ago has abandoned his application for early parole. Lang Nguyen, 47, was supposed to begin his so-called "faint hope clause" hearing this week. Middlesex Crown Attorney Geoff Beasley confirmed that the case would not be going forward. Nguyen, convicted of first-degree murder, won his chance to apply for parole almost a year ago. London Free Press, A7

You don't know Carjacking
An opinion piece states, "The number of auto thefts in Winnipeg may be down, but carjackings a steady pace last year. The Winnipeg Sun has learned there were 44 carjackings in Winnipeg in 2011. That's up slightly from the 43 recorded the previous year, according to the Winnipeg Police Service. And it's about twice as many carjackings as Winnipeg used to experience before government made after-market immobilizers mandatory for high-risk vehicles... The problem with car thefts and carjackings is we don't do enough to target the offender. We force victims and would-be victims to install after-market immobilizers in their vehicles. But we treat the actual criminals who steal the cars with kid gloves." Winnipeg Sun, 5

*** Prison farm protesters get day in court**
Eight holdout protesters, charged in the summer of 2010 over their attempts to stop the final dismantling of Frontenac Institution's farm program, began their trial Monday in Kingston's Ontario Court of Justice on charges of mischief by interfering with the lawful use of property. Kingston Whig-Standard, 1

*** Vancouver crime rate shows drop**
Crime is going down in Vancouver, police statistics indicate. Vancouver Mayor Gregor Robertson said the statistics indicate a decrease in crime over the past five years and that the VPD's crime strategy is working. The Province, A11

*** Crime Stoppers appeals to students for help, tips**
New Brunswick Crime Stoppers and the Government of New Brunswick have joined forces to make schools and communities safer with a new Crime Stoppers program for students. The program offers high school and college students a confidential and anonymous medium to report crimes without fear of reprisal or retaliation. Times & Transcript, A6

*** Tough love**
A letter states, "...The fact is drug prohibition supporters are responsible for the adulterated drugs presently killing our children. All this is eerily similar to the adulterated alcohol that caused death and blinding in the '30s. Prohibitionists seem to be callous people who would sooner send moral messages with the law to save souls than to repeal drug prohibition and save lives. In a free country, there should be no such thing as a crime against the state." Calgary Herald, A9

*** Fossilized thinking**
A letter states, "Much like Ronald Reagan's Just Say No policy of the 1980s, Dave Reesor's idea of harsh minimum penalties for drug producers belongs in a museum. Claiming that illegal organizations produce and distribute illegal drugs for anything but profit is an opinion-biased argument. Using the case study of the United States as an example for failed drug policy, it is clear that harsher prohibition has not affected the consumer demand for drugs in any way... How many more deaths will happen before our elected officials open their eyes to the true dangers of drug prohibition?" Calgary Herald, A9

*** Pas un danger?**
Un article d'opinion déclare, « Depuis l'énoncé de la sentence de Guy Turcotte, je suis totalement outré... Supposer qu'il puisse exister des circonstances atténuantes, en l'occurrence la folie, pour justifier un tel geste est aberrant et inacceptable... La société dans laquelle je veux vivre ne doit en aucun cas cautionner un tel comportement. Il ne faut d'aucune façon laisser à quiconque l'impression qu'il peut commettre un tel crime et pouvoir s'en tirer. Guy Turcotte ne doit pas recouvrer sa liberté avant longtemps, point final... » La Presse, A16

*** Murderer back in jail for violating his parole**
A man convicted of second-degree murder is headed back to prison after violating his parole. Christopher Alexander Falconer, 29, pleaded guilty Monday in Pictou provincial court to charges of possession of a prohibited weapon and possession of marijuana. He was sentenced to three months and one month, respectively, to be served concurrently. Chronicle Herald, A6

INTERNATIONAL / INTERNATIONAL

*** Tempest in a pee-pot**
NATO soldiers can shoot Taliban terrorists. They can bomb them from the air. They can fire missiles at them from remote-controlled drones. But they can't pee on their dead bodies. Edmonton Sun, 15 (Toronto Sun, Calgary Sun, Whig-Standard, Winnipeg Sun, Ottawa Sun)

*** The world must intervene in Syria**
A letter by Maher Arar states, "The signs are clear: Bashar al-Assad is in a state of desperation, and his latest speech in front of Syrian parliament proves it: having played most of the cards at his disposal in attempting to crush the Syrian uprising (including the murder of peaceful protesters), he is now playing his final card, the "patriotism" card, by insisting that the turmoil taking place in Syria is the result of a "foreign conspiracy." He has promised that he will resort to an "iron-first" approach to deal with the "terrorists" (i.e. peaceful protesters). If anything, this ad hominem attack shows how truly bankrupt his regime has become, to be so completely unable to offer any meaningful solutions to a nation that so badly wants freedom and political change..." Ottawa Citizen, A13

*** UN chief urges action on Syria**
UN chief Ban Ki-moon on Monday urged the Security Council to act on Syria as President Bashar al-Assad came under new pressure with defections and signs of increasing co-operation among his foes. Ottawa Citizen, A11

OTHER / AUTRE

Canada loses an Afghan ally
One of Canada's best Afghan friends was assassinated in Kandahar last Thursday. Haji Fazluddin Agha, the governor of Panjwaii district, was killed when his car was struck by a vehicle driven by a suicide bomber on a road funded and paved with Canadian help and protection. Two of Agha's sons, two policemen and a civilian, also died in the blast. A charismatic bear of a man with a booming voice and a lush black beard, Agha was a deeply pious Muslim. He detested Islamist zealots and was a fierce opponent of the Taliban and al-Qaeda. Ottawa Citizen, A6 (Windsor Star, Vancouver Sun, Calgary Herald)

*** Naval crew helps recover submarine packed with cocaine from sea floor**
Last fall, Canadian navy crews assisted in the recovery of a scuttled Caribbean submarine packed with more than 6,700 kilograms of cocaine, according to a weekend release by the Royal Canadian Navy. The submarine is a "self-propelled semisubmersible," a category of custom-built drug-smuggling vessels that have emerged over the past 10 years, largely in the hands of Colombian drug cartels. National Post, A5

Bonvie, Jeff

From: Bonvie, Jeff
Sent: January-16-12 3:48 PM
To: Abramczyk, Jill; Virdee, Harjit Singh
Subject: Cyber Info
Attachments: PS-SP-#438312-v1-NCSD_GLOSSARY_OF_COMMON_CYBER_SECURITY_TERMS.DOC

Hello Jill and Harjit,

Nice to meet you both; sorry I was kind of a verbal machine gun. As discussed here is some cyber information which may (I hope) be of use.

@ Jeff To Do: Introduce you to Bud – this I will do via separate email, likely tomorrow.

NCSD's existing glossary of terms (see attached file 438312): Please note that we took from existing work where we thought it was a good fit. We didn't use any one single source (this is noted via the footnotes). In rare cases we wrote it ourselves when we either couldn't find, or were not happy with what we did find in the existing work.
The GCPEDIA Cyber Lexicon Reference: http://www.gcpedia.gc.ca/wiki/Cyber_Security_Lexicon
Backgrounder on Cyber: This we can plan for the near future, some related ongoing discussion here about our internal learning events. More to follow…
Interesting Cyber Related Links (more here than you would likely have time to read):

General News Sites:
http://www.wired.com/threatlevel/
http://www.wired.com/dangerroom/
http://www.net-security.org/
http://www.darkreading.com/index
http://www.pcworld.com/businesscenter/index/security.html
http://arstechnica.com/tech-policy/
http://slashdot.org (not security specific, just technical but often w/ posts re: security issues)
http://www.csoonline.com/

Blogs:
http://krebsonsecurity.com/ (Journalist / Researcher)
http://www.schneier.com/ (Security expert, on Security and Technology – oddly on Squids too)
http://blog.trendmicro.com/ (AV Company)
http://threatpost.com/en_us (AV Company)
http://www.symantec.com/connect/symantec-blogs/messagelabs-intelligence (AV Company)
http://blogs.technet.com/b/staysafe/ (Microsoft)
http://blogs.rsa.com/ (Security Gurus)

Popular / Frequently Referenced Material:
Defending a New Domain by William J Lynn - http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
CSIS Report, Securing Cyberspace for the 44th Presidency - http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
H. Clinton's speech on Internet Rights and Wrongs - http://www.state.gov/secretary/rm/2011/02/156619.htm
Munich Security Conference William Hague - http://www.securityconference.de/Hague-William.704.0.html?&L=1
SecDev / Munk Centre Research Reports
(Ghost Net Report) http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network
(*Shadows in the Cloud* Report) http://www.infowar-monitor.net/2010/04/shadows-in-the-cloud-an-investigation-into-cyber-espionage-2-0/
(*Koobface Report) http://www.infowar-monitor.net/reports/iwm-koobface.pdf (PDF)*

A Sample of Interesting / Popular Attacks, Hacks & Haxors
Anonymous vs HBGary
http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars
Albert Gonzalez (Massive Credit Card theft and was working for the FEDS)
http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html
General Article on Stuxnet (1 of 1598745015484545 articles on Stuxnet)
http://www.infoworld.com/t/malware/more-evidence-arises-stuxnet-was-created-attack-iran-306
RSA Attack
http://arstechnica.com/security/news/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated.ars

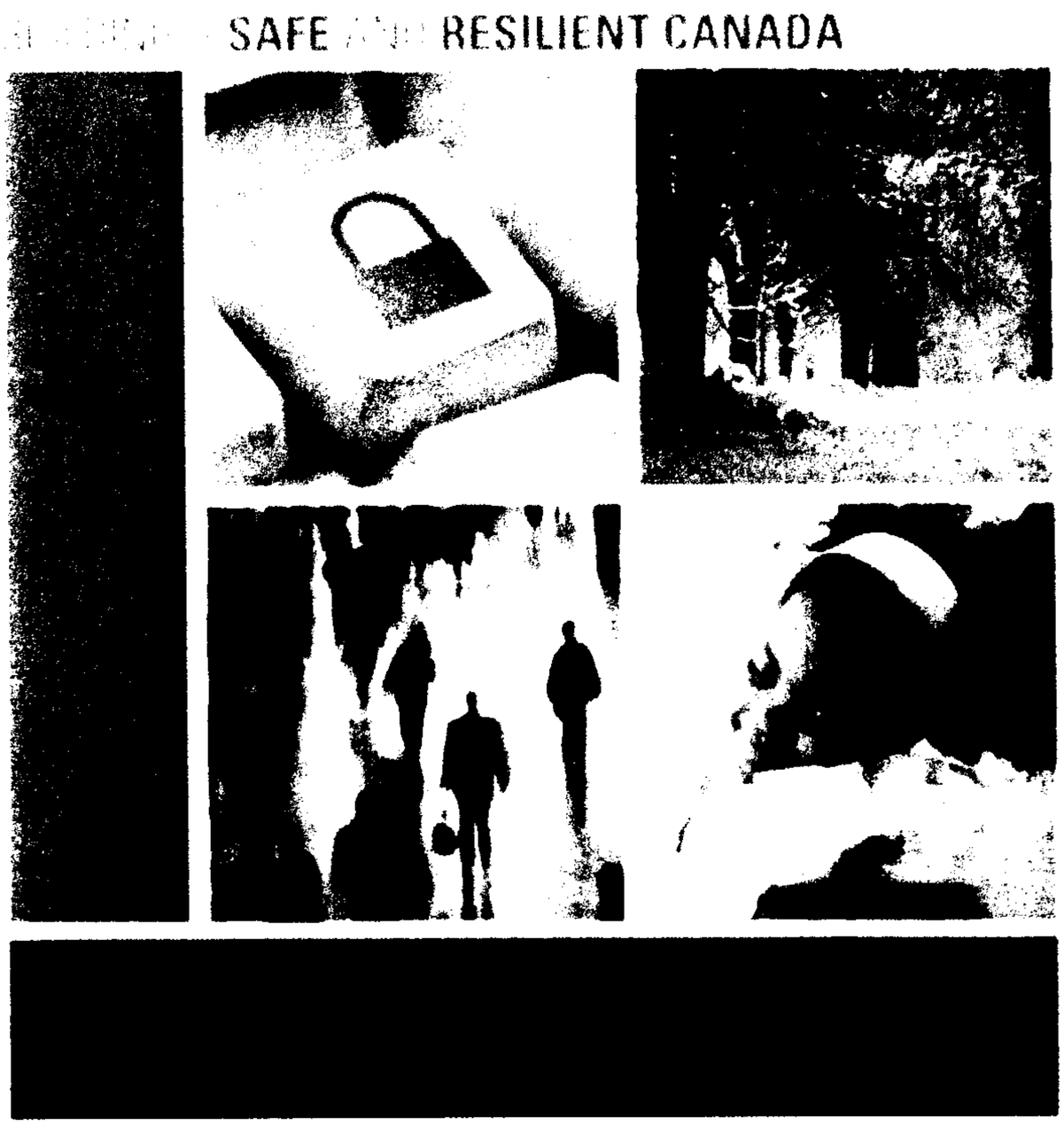
International Strategies (some of these are out of date):
Australia (PDF)
UK (It was here somewhere…)
US (PDF)
Dutch (PDF)
German (PDF)
French (PDF)

Hope this is of use!

Cheers,

Jeff
Advisor / Conseiller
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 OP8
613-990-9380
Jeff.Bonvie@ps-sp.gc.ca

Public Safety Canada | Sécurité publique Canada



NATIONAL CYBER SECURITY DIRECTORATE
GLOSSARY OF COMMON CYBER SECURITY TERMS

JUNE 17 2011
RDIMS #438312
Version 1.1

Canada

00354

National Cyber Security Directorate
Glossary of Common Cyber Terminology

A

Anti-virus software (AVS) - software that defends against viruses, trojans, worms and spyware. Anti-virus software uses a scanner to identify programs that are or may be malicious. Scanners can detect: known viruses; previously unknown viruses; and suspicious files. [1]

B

Backdoor – a backdoor in a computer system is a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection.[2]

Beaconing – is a process whereby a system (typically a victim) sends a contact message to another system (usually an intruder's control system). [2] This process is done to notify to an intruder that a system is active and remains infected.

Bot – a program covertly installed on a user's machine to allow an unauthorized user to remotely control the targeted system through a communication channel. These channels allow the remote attacker to control a large number of compromised computers in a botnet, which can then be used to launch coordinated attacks. Attackers can use bots to perform a variety of tasks, such as setting up denial of service attacks against an organization's website, distributing spam, spyware and adware, phishing attacks, propagating malicious code, and harvesting confidential information.[1]

Botnet – a collection of compromised machines running malicious applications without the knowledge of the operator via a command and control infrastructure.[2]

Brute Force Attack - attack on a system that employs an exhaustive search of a set of keys, passwords or other data. [1]

C

Computer Emergency Response Team (CERT) – a group which is responsible for responding to computer related security incidents outside of typical information technology support roles.

Cloud Computing – the ability to access all required software, data and resources via a computer network instead of the traditional model where these are stored locally on a users computer.

Compromise – the disclosure of information or data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosures, modification, destruction, or loss of an object may have occurred. [2]

Computer Network Attack (CNA) – actions take trough the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks of the computers and networks themselves. [2]

Computer Network Defence (CND) – actions taken through the use of computer networks to protect monitor, analyze, detect and respond to unauthorized activity within a department or organization's information systems and computer networks. [2]

Computer Network Exploitation (CNE) – enabling operations and intelligence collection acapabilit8ies conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. [2]

Computer Network Operations (CNO)– comprise computer network attack, computer network defence and related computer network exploitation enabling operations. [2]

Computer Security Incident Response Team (CSIRT) – See CERT.

Command and Control (CNC) Server – a system (often also compromised) which is used to control all of the infected computers in a distributed botnet.

Cryptography – the discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [1] The conversion of the information into this new protected form is referred to as encryption. The conversion of information back to its original form is decryption.

D

Decryption – decoding of a message which has been encrypted (see cryptography)

Denial of Service (DoS) Attack – a type of cyber attack aimed at overwhelming or otherwise disrupting the ability of the target system to receive information and interact with any other system.

Deep Packet Inspection – the detailed analysis of a data packet in order to determine if the contents of the packet contain malicious or otherwise unwanted data.

Distributed Denial of Service (DDOS) Attack – a denial of service attack which utilizes a series of computer systems which are in the form of a distributed network. In a DDOS attack, more than one system is attacking the target. Often DDOS attacks utilize botnets.

Digital Forensics - generally considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. [1]

E

Encryption – converting information from one form to another to hide its content (see cryptography)

Exploit - is a defined way to breach the security of an IT system through a vulnerability. [1]

Exfiltration – the unauthorized removal of data or files from a system by an intruder.[2]

F

Firewall - a firewall is a type of security barrier placed between network environments. It may be a dedicated device, or a composite of several components and techniques. It has the properties so that all traffic from one network environment to another, and vice versa, traverses through the firewall and only authorized traffic, as defined by the local security policy, is allowed to pass. [1]

G

H

Hacktivist – a computer attacker who undertakes malicious activity for political or other motivations related to a particular issue or position.

Honeypot - a decoy Information System used to deceive, distract, and divert an attacker and to encourage the attacker to spend time on bogus information.[1]

I

Industrial Control Systems (ICS) – the broad grouping of software and hardware that is used to control infrastructure such as those found in factories and power generation stations including supervisory control and data acquisition systems and programmable logic controllers.

Information Technology Security (ITS) - safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.[1]

Internet Engineering Task Force (IETF) - the group responsible for proposing and developing technical Internet standards.[1]

Internet Governance Forum (IGF) – a UN created forum which brings states, NGOs and other stakeholders to discuss public policy issues related to key elements of international governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

Internet Corporation for Assigned Names and Numbers (ICANN) – a non-profit organization dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

Intrusion Detection System (IDS) - technical system that is used to identify that an intrusion has been attempted, is occurring or has occurred, and possibly to respond to intrusions in IT systems and networks.[1]

Intrusion Prevention System (IPS) - a variant on intrusion detection systems that are specifically designed to provide an active response capability.[1]

[redacted]

[redacted]

Keystroke Logger – software or hardware designed to capture a users keystrokes on a compromised system. The keystrokes are stored or transmitted so that they maybe used to collect valued information.

[redacted]

[redacted]

Malware - malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

Metadata - data that describes the structure and workings of an organizations use of information, and the systems it uses to manage that data.

[redacted]

Network Administration - day to day operation and management of network processes and users.

[redacted]

[redacted]

Packet - a formatted block of information carried by a computer network. When data is formatted into a packet, the network can transmit longer messages more efficiently and reliably than unformatted bytes.

Patch - a small piece of software designed to update or fix problems with a computer program. This includes fixing bugs, reducing vulnerabilities, replacing graphics and improving the usability or performance.

Peer to Peer (P2P) Network - relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating power in a low number of servers. These networks are often used for sharing content files containing audio and video data.

Phishing - an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing, a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card

numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.

Proxy - a process that accepts requests for some service and passes them on to the real server.

Q

R

Ransomware - software that denies you access to your files until you pay a ransom.[1]

Rootkit - a set of software tools intended to conceal running process, files, or system data, thereby helping the intruder to maintain access to a system without detection. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules.[2]

S

Supervisory Control and Data Acquisition (SCADA) - an industrial measurement and control system consisting of a central master station, one or more field data gathering control units, and a collection of standard or custom software used to monitor and control electromechanical devices in industrial processes such as refineries, electrical power generation or flood control.[2]

Spear Phishing - the use of spoof emails to persuade people within an organisation to reveal their usernames or passwords. Unlike phishing, which involves mass mailing, spear phishing is small-scale and well-targeted.[1]

Security Token - a set of security relevant data that is protected by integrity and data origin authentication from a source which is not considered a security authority.[1]

SPAM - junk or unsolicited e-mail sent by a third party. An annoyance to users and administrators, spam is also a serious security concern as it can be used to deliver Trojans, viruses, and phishing attempts.[1]

Sniffers - computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network.[1]

Social Engineering - the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. For example, phishing is a type of social engineering technique.[2]

Spoofing - a situation in which one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage.[2]

Spyware - software that enables advertisers or hackers to gather information without the user's permission. Spyware programs are not viruses, since they do not spread to other computers, but they can have undesirable effects. Once installed, spyware tracks the infected computer's activity and reports it to others, such as advertisers. Spyware also consumes memory and processing capacity, which may slow or crash the infected computer.[1]

T

Trojan - a malicious program that is disguised as or embedded within legitimate software. The term is derived from the gift the ancient Greeks presented to the citizens of Troy during the Trojan War, as a ruse to infiltrate and sack the city.[2]

U

V

Virtual Private Network (VPN) - a private communications network usually used within a company, or by several different companies or organisations to communicate over a wider network. VPN message traffic can be carried over a public networking infrastructure (i.e. the Internet) on top of standard protocols, or over a service provider's network with a defined Service Level Agreement between the VPN customer and the VPN service provider. VPN communications are typically encrypted or encoded using SSL to protect the traffic from other users on the public network carrying the VPN.[2]

Virus - a computer program that can spread by making copies of itself. Computer viruses spread from one computer to another, by making copies of themselves, usually without the knowledge of the user. Viruses can have harmful effects, ranging from displaying irritating messages to stealing data or giving other users control over the infected computer. A virus program has to run before it can infect a computer, generally doing so by attaching itself to other programs or hide in code that is executed automatically when a user opens certain types of files.[1]

Vulnerability - a flaw or weakness in the design or implementation of an information system or its environment that could be intentionally or unintentionally exploited to adversely effect an organization's assets or operations.[2]

W

Worm - a self-replicating computer program. It uses a network to send copies of itself to other systems and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.[1]

X

Y

Z

Zero Day Exploit - a zero-day exploit makes use of unrecorded vulnerabilities in a host or network that evade anti-virus and anti-spyware systems. The exploit is generally used to insert malicious code.[2]

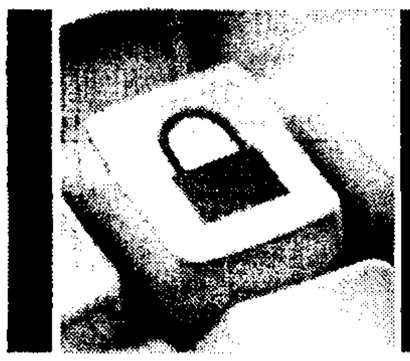
Zombie - a computer that is remotely controlled and used for malicious purposes, without the legitimate user's knowledge. A virus or Trojan can infect a computer and open a "back door" that gives other users access. As soon as this happens, the virus sends a message back to the virus writer, who can now control the computer remotely via the Internet. The computer is now a zombie doing the bidding of others, although the user is unaware. Collectively, such computers are called a "botnet."[1]

SOURCES

[1] Cyber Security Lexicon from GCPEDIA, http://www.gcpedia.gc.ca/wiki/Cyber_Security_Lexicon
[2] Department of National Defence, Defence Intelligence Cyber Glossary.

Note: Entries without source reference have been created by NCSD. Entries which are referenced to an external source may be subsets of the complete entry found in the reference.

Public Safety Canada | Sécurité publique Canada



Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 14-28, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-002

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations.

This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents reported over the last two weeks. There were reports of Canadian computers being used for malicious purposes, including attacking a US State Police website. A Canadian federal department linked to the signing of the international Anti-Counterfeiting Agreement (ACTA) was targeted through a malicious e-mail. There was also a message on the Internet by hackers to e-mail or launch a cyber attack against this Department. Internationally, hackers attacked government websites in US, Poland, Ireland and the EU to protest signing of ACTA. There are also continued reports of infected computers in Canada and around the world due to the Ghostclick fraud.

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- US State Police website attack traced to Canada
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

CCIRC Products Released during the reporting period:

- Cyber Flash on cyber attacks by Anonymous related to copyrights and intellectual property (CF12-001)

Noteworthy News in the Media:

- Israeli and Palestinian hackers exchange website attacks
- Hackers around the world protest current and intended anti-piracy measures:
    - MegaUpload's shutdown prompts hacker attacks on US government and music industry websites
    - Proposed US copyright law SOPA being protested: Certain websites elect to go dark for one day in protest; Anonymous attacks US government websites such as DOJ & FBI
    - Signing of the international Anti-Counterfeiting Agreement (ACTA) prompting hacker attacks on US, Poland, Ireland and European government websites.

NEW EVENTS REPORTED IN GOVERNMENT AND OTHER CANADIAN CRITICAL INFRASTRUCTURE SECTORS

Federal Government Sector

Operation SACTA (Stop Anti-Counterfeiting Trade Agreement): An online message signed by Anonymous posted a link to a Canadian federal department website, encouraging users to join the anti-ACTA movement, and attack if necessary. This message was posted on a popular text-file sharing website often used by hackers and is presumably encouraging cyber attacks on websites.

CCIRC provided available technical details to CTEC, the federal Government's CERT, for their further investigation.

> ***Comment:*** *There are provisions in the international Anti-Counterfeiting Trade Agreement that have important implications for content sharing on the Internet. This is a multi-lateral trade agreement which Canada has signed. Canada's new proposed copy-right law, Bill C-11 (former Bill C-32), is currently in Parliament at the second reading stage. There is a great deal of opposition to this agreement around the world by the on-line community and websites of other government have recently been attacked by hackers in protest.*

File Server (FTP) Login Credentials of a Federal Department posted on the Internet. CCIRC learned that the FTP login credentials of a federal department were posted on the Internet. CCIRC advised CTEC and provided known technical details.

> ***Comment:*** *FTP login credentials are used to gain access to a file sharing server where users may upload or download files. If a threat actor used these credentials, the result could be information compromise or the use of the server as a launch point for cyber attacks.*

Non-Federal Government Sector

Canadian computers being used in cyber attacks. CCIRC has learned that a cyber attack on a US State Police website was traced to a Canadian university's computer. In addition, another Canadian university's website was found to host malicious software that could infect website visitors. There were also reports of malicious software being hosted at a website hosting service provider's server and at two other unidentified Canadian entities.

CCIRC contacted the known Canadian organizations, with mitigation advice. The RCMP was informed of items of interest. CCIRC warned the website hosting service provider that the website in question was added to various block lists, possibly resulting in reduced legitimate traffic to this website. The malicious software from the university's website has been removed and is no longer being served.

> ***Comment:*** *It is possible that cyber criminals compromised these Canadian computers to use them remotely for malicious purposes, without their owners' knowledge. Organizations that offer computers for public use, such as universities, can be particularly susceptible to such compromises.*

Some Canadian Industrial Control Systems exposed to potential cyber attacks. A trusted international partner alerted CCIRC that information that could allow remote access to certain Canadian houses and apartment buildings' heating and air conditioning systems, was posted on the Internet. CCIRC alerted those responsible for the buildings and houses, offering mitigation advice. There is no report of any cyber attack in these cases at this time.

> ***Comment:*** *Many Industrial Control Systems (ICS), such as the ones used for heating and cooling buildings, are monitored or even maintained remotely through the use of certain software. It is likely that the technicians responsible for the set-up and maintenance of the heating systems for these buildings did not take cyber security into consideration or did not know the standard practices for protecting against such exposure.*
>
> *Since the Stuxnet virus attack on an Iranian nuclear facility, there has been a heightened awareness, both domestically and internationally, of cyber security for ICS. The trusted international partner who alerted CCIRC is focussed primarily on securing ICS. CCIRC recently moderated discussion at a ICS conference in Montreal.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonating Canadian financial institutions, tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in United States and Taiwan.

Cyber criminals also attempted to solicit personal information by impersonating Service Canada and Canada Revenue Agency.

CCIRC notified the impersonated financial institutions of these fraud attempts and the Government CTEC for the federal government cases. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website compromises and publicized vulnerabilities. CCIRC discovered a small health organization's website was defaced and offered mitigation advice. CCIRC also discovered a foreign Defence Department's website was compromised and contacted the organization, as well as CCIRC's equivalent organization. There was also a list of vulnerable websites posted on the Internet, which includes a Canadian university.

There were additional website compromises in the health and non-critical infrastructure sectors. Website usernames and passwords were posted on the Internet by hackers.

> ***Comment:*** *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

Ghostclick Fraud. There were new and continued reports of infected computers in three provincial governments, three provincial health organizations, an airport authority, an energy organization, two banks, 19 Canadian universities, a national media organization and 13 telecommunications companies.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are currently websites around the world for computer users to check whether their machine is infected by the malicious software used in this fraud. These sites can be found by searching with the keywords "dns-ok".

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in. CCIRC is also working with the Canadian Internet Registration Authority (CIRA) to provide notifications to affected users.

Operation Ghostclick was worldwide fraud campaign, exposed in late 2011 by the FBI. Cyber criminals hijacked users' Internet web searches and diverted them to websites that generated advertising and sales revenues. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

> ***Comment:*** *Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. CCIRC noted that the type and size of affected organizations varied, and were spread across Canada. The number of affected telecommunications companies more than likely indicates number of infected client computers of Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*
>
> *Organizations that offer Internet access, including those that provide publically accessible wireless networks, may be particularly vulnerable. In addition to the cooperative effort underway between CCIRC and CIRA, the Canadian government has launched a website for cyber security public education..*

CCIRC PRODUCTS RELEASED:

Hacktivist attacks related to proposed anti-piracy legislation. There have been coordinated distributed denial-of-service (DDoS) attacks on websites by hacktivists, claiming to be associated with Anonymous. There were multiple international targets, which included governments (Canada, US, Poland, Ireland and EU) and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

In response, CCIRC issued Cyber Flash CF12-001, titled *"Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property"*. This Cyber Flash, was sent to technical and security contacts within stakeholder organizations in government and other critical infrastructure

sectors . Government and industry organizations involved with the Copyright legislation and copy-righted material were encouraged to assess their risk exposure to coordinated DDoS attacks on their networks.

NOTEWORTHY NEWS IN THE MEDIA:

Israeli and pro-Palestinian hackers exchange website attacks. Open sources reported that the websites of Israel's main stock exchange, several banks and the national airline were attacked. Pro-Palestinian hackers claimed responsibility and even claimed to have posted the login credentials for several industrial control systems in Israel on the Internet. Shortly thereafter, there were reports of suspected Israeli hackers bringing down the Saudi Stock Exchange, interfering with the Abu Dhabi Security Exchange, and publishing e-mail addresses & passwords of 30,000 Arab Facebook users.

Comment: *It is now becoming commonplace to carry real-world grievances into the cyber world. There could be an adverse impact from these attacks for Canadians and Canadian businesses that do business with the stock exchanges or banks involved. There were some media reports that some of the Israeli banks could block international access to their sites.*

Hackers around the world attack government websites to protest anti-piracy measures.

- **Retaliation for file-sharing service Mega Upload's shutdown:** Hackers, claiming to be with Anonymous, attacked the websites of the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music.

- **Signing of the international Anti-Counterfeiting Agreement (ACTA) and proposed US copyright laws:** Wikipedia shut down for one day to protest the proposed SOPA and PIPA bills. SOPA and PIPA were also cited by Anonymous as a reason for their attacks on the DOJ and FBI websites. Operation STOP ACTA by Anonymous also prompted hacker attacks on websites for US, Poland, Ireland governments as well as for the European Parliament.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

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

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-13-12 8:47 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 13, 2012/ le 13 janvier 2012

Print Media

Hackers fry Putin's website
Calls for Russian Prime Minister Vladimir Putin to resign and drop his presidential bid flooded his campaign website within minutes of its launch on Thursday, prompting administrators to limit public access. Putin's spokesman and campaign official Dmitry Peskov said the website fell victim to a hacker attack in its early hours and some of the anti-Putin messages were spam. He denied any messages were blacklisted. Edmonton Sun, 20

Online Media

Cybercrime is a growing threat for government and public sector organisations
Cybercrime is a growing threat for government and public sector organisations, after 14 percent admitted they have been the victim of a web-based scam. According to research by Pricewaterhouse Coppers, more than a quarter (28 percent) believe they are likely to suffer a cybercrime attack in the next 12 months while 40 percent admit they think the risk of cybercrime to be on the rise. PC Advisor

Microsoft Planning Real-Time Feed of Valuable Threat Data
Microsoft has had a great deal of success taking down botnets in recent years. A fringe benefit of those takedowns is that Microsoft gets to collect oodles of very valuable data. Now, Microsoft is preparing to offer that threat intelligence as a real-time feed that partners can use to evaluate threats and develop better defenses. PC World

Cyber insurance offers IT peace of mind -- or maybe not
If your company were hit with a cyber attack today, would it be able to foot the bill? The entire bill, including costs from regulatory fines, potential lawsuits, damage to your organization's brand, and hardware and software repair, recovery and protection? Computerworld

Fighting cyber threats with malware not ideal
Countries are increasingly taking up the option of fending off cyber threats with homebrewed malware but while this might prove effective, security insiders noted this might bring technical and ethical issues and, ultimately, not the best method to curb online threats. ZDNet

'Gaza hackers' target Israel fire service website
Hackers claiming to be from the Gaza Strip defaced the website of the Israel Fire and Rescue services, posting a message saying "Death to Israel," a spokesman told AFP on Friday. Fire service spokesman Yoram Levy said that attackers who identified themselves as the "Gaza Hackers Team" struck its website late on Thursday and posted a picture of Israel's Deputy Foreign Minister Danny Ayalon with footprints over his face. AFP

Anonymous targets Israel as it joins war between hackers
Anonymous has posted what appear to be login details for Israeli SCADA industrial-control systems, a cyber attack that marks the politically minded group's entrance into the heated battle between Israeli and Saudi Arabian hackers that has already exposed thousands of credit card numbers and personal details. MSNBC

Stratfor back online after cyber-attack steals credit card data
Global intelligence analysis firm Stratfor has relaunched its website after hackers brought down its servers and stole thousands of credit card numbers and other personal information belonging to its customers. China Post

Security trumps secrecy in cyber fight, prosecutor says
A top federal prosecutor has a message for companies: If you've been hacked, tell us. Speaking at a cyber security conference in New York on Thursday, Manhattan U.S. Attorney Preet Bharara said companies should trust in the discretion of prosecutors and the FBI and come forward with information about a security breach, rather than keep it an internal secret. Reuters

GAO: DHS floods critical industries with irrelevant cybersecurity advice
The Department of Homeland security has responded so enthusiastically and uncritically to Presidential orders that it keep companies in the "critical infrastructure" informed of cybersecurity threats and techniques that it is, instead, drowning those companies in information that is often repetitive or misdirected, according to a new report from Government Accountability Office (GAO). IT World

Cyber Crime Threat Is Top Worry of Manhattan U.S. Attorney Preet Bharara
Preet Bharara, the top federal prosecutor in Manhattan whose office has sent terrorists and inside traders to prison, told an audience that the threat of Internet-related attacks is his biggest worry. Bloomberg

Cyber attacks now fourth biggest threat to global stability, says World Economic Forum
A report from the World Economic Forum (WEF) shows cyber attacks on governments and businesses are considered to be one of the top five risks in the world. The report, Global Risks for 2012, examined 50 global risks in the areas of the economy and the environment and in geopolitics, society and technology, and was based on interviews with more than 460 experts from industry, government and specialist areas. Daily Mail

Cyber-Crimes Pose 'Existential' Threat, FBI Warns
Despite the increased frequency and severity of online crime and espionage in 2011, many American corporations and consumers are still not taking the threat seriously, the FBI's top cyber official said Thursday. Huffington Post

Phishing pays off for email security providers
Big financial institutions and other companies are finally succeeding in reducing the volume of emails sent by malicious actors who disguise messages so that they appear to come from a trusted brand, a key technique both for cyber criminals and international spies. Financial Times

Cyber defense effort is mixed, study finds
A Pentagon pilot program that uses classified National Security Agency data to protect the computer networks of defense contractors has had some success but also has failed to meet some expectations, according to a study commissioned by the Defense Department. Washington Post

Malicious Software Attacks Security Cards Used by Pentagon
Chinese hackers have deployed a new cyber weapon that is aimed at the Defense Department, the Department of Homeland Security, the State Department and potentially a number of other United States government agencies and businesses, security researchers say. New York Times

World Economic Forum puts cyber attacks in top five biggest global risks for 2012
Cyber attacks are one of the top five global risks likely to impact the planet over the coming year, according to the latest annual report from the World Economic Forum (WEF). The international organisation interviewed more than 460 experts from industry, government, academia and civil society to compile its seventh Global Risks report. V3.co.uk

Chinese attacks target US government agencies and smartcards
Evidence has been revealed that attacks are being made against US government agencies, using a new strain of the Sykipot malware to compromise smartcards. According to Security Information and Event Management (SIEM) vendor AlienVault, the attacks originate from China and target agencies including the US Department of Defense. SC Magazine

Anderson, Windy

From: Hatfield, Adam
Sent: January-13-12 8:39 PM
To: Anderson, Windy; Cameron, Bud; Bendelier, Kenneth; Klassen, Nathan; Beaudoin, Luc S
Subject: Fw: New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks - Canada Ranks High
Attachments: Cyber_Power_Index_Findings_and_Methodology.pdf; Cyber_Power_Index.xls

FYI for the SA/results reporting angle.

Adam

From: Dvorkin, Corey
Sent: Friday, January 13, 2012 03:23 PM
To: * NCSD-340 Laurier
Cc: Stanfield, Charles; Stanfield, Charles; Champoux, Martin
Subject: FW: New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks - Canada Ranks High

Report is attached, as is an interactive spreadsheet.

Canada scores #5 globally, coming 4/19 in legal frameworks, and 5/19 countries for each of econ/social; technical infrastructure and industry applications.

Lots here to digest.

From: Castonguay LCol JF@VCDS DG Cyber@Ottawa-Hull
Sent: Friday, 13, January, 2012 14:20 PM
To: Sixsmith SL@ADM(Pol) D Pol Dev@Ottawa-Hull; Anishchenko A@ADM(Pol) D Strat A@Ottawa-Hull; Yarker LCol DR@SJS Operations@Ottawa-Hull; Kendall Maj PJ@VCDS DG Cyber@Ottawa-Hull; Messier Maj RM@VCDS DG Cyber@Ottawa-Hull; Renneberg MWO MA@VCDS DG Cyber@Ottawa-Hull; Couture Maj EB@CANOSCOM OS J3@Ottawa-Hull; Leblanc JPSS@RMC ECE@Kingston
Subject: FW: New Index Ranks Ability of G20 Nations to Withstand Cyber Attacks - Canada Ranks High

FYI.

MCLEAN, Va., Jan 12, 2012 (BUSINESS WIRE) -- A new benchmarking study of 19 of the world's 20 leading economies found that the United Kingdom and the United States lead Group of 20 (G20) countries in their ability to withstand cyber attacks and to deploy the digital infrastructure necessary for a productive and secure economy. The index also found that several major economies--Argentina, Indonesia, Russia and Saudi Arabia--do not have cybersecurity plans and do not appear to be developing them.

The index is at www.cyberhub.com

Overall, the top five countries exhibiting cyber power, as measured by the index-- the UK; the US; Australia; Germany; and Canada --illustrate that developed Western countries are

leading the way into the digital era. The top five performers also rate highly across the board, ranking in the top seven in all four categories.

The Cyber Power Index, developed by the Economist Intelligence Unit and sponsored by Booz Allen Hamilton, measures both the success of digital adoption and cyber security, and the degree to which the economic and regulatory environment in G20 nations promote national cyber power.

The Index allows visitors to compare the cyber power rankings of the G20 countries on a scale of 0-100 with 100 being most favorable. Each country's ranking is a weighted mean of scores from four categories: Legal and Regulatory Environment; Economic and Social Context; Technology Infrastructure; and Industry Application. Each category features at least four underlying indicators, many of which are composed of sub-indicators. The European Union, the newest member of the G20, was not included in the study.

"The Cyber Power Index identifies those countries that understand what it takes to operate in a digital era...and those that don't," said Booz Allen Hamilton Vice Chairman Mike McConnell. "Many define a nation's cyber power simply like other domains such as land, air or space. While cyber is a domain, a nation's capabilities must be measured by more than their military might alone. The countries able to master the uses and security requirements of emerging technologies and societal shifts brought on by the cyber revolution will emerge as the cyber powers and the winners of the 21st century."

Overall, the top five countries exhibiting cyber power, as measured by the index--the UK; the US; Australia; Germany; and Canada--illustrate that developed Western countries are leading the way into the digital era. The top five performers also rate highly across the board, ranking in the top seven in all four categories. The G20's last member, the EU, was not analyzed.

The leading emerging market countries, Brazil, Russia, India and China (the BRICs), have some room for improvement; out of the 19 economies, they rank 10th, 14th, 17th, and 13th, respectively. There is also a wide discrepancy between the top and the bottom of the index. The UK, the top performer, scores around three times the amount of points on a scale of 0 to 100 as the worst performer, Saudi Arabia. Among other conclusions from the data:

-- Cyber power relies on a solid foundation that includes technical skills for security and effective use of the cyber environment, high educational attainment levels, open trade policies, and an innovative business environment. The US has the most supportive economic and social context for fostering cyber power according to the index. This is driven by high tertiary education enrollment, research and development (R&D) investment, and an open trade environment. Asia's rising influence is also apparent in this category, as China leads the trade indicator, while Japan and South Korea fill the number one and two positions, respectively, in technical skills.

-- The gap in cyber capability between the U.S. and other countries is closing. While the U.S. has a broad and deep cyber power base, other nations such as South Korea and Japan are aggressively adopting greater levels of bandwidth and communications stability.

-- Big does not always mean powerful. China has a large population and a powerful military. As a result the nation is often considered to be a cyber power. In reality, the Cyber Index found that the country's true level of cyber power is in reality quite modest. Going forward, other countries are expected to be added to the Index, which could show the power of small countries such as Estonia. In contrast to China, Estonia is relatively tiny and hosts a modest military, yet that country's well known ability to integrate advanced technology into its society could make a telling comparison.

-- Germany's comprehensive cyber policies are a key to its success. Germany leads the legal and regulatory framework category with a near perfect score (99.3 out of 100), followed by other Western countries that also performed well in the overall index. Germany is one of only five countries (the others being the UK; the US; France; and Japan) to have both a comprehensive national cyber plan and a comprehensive cybersecurity plan.

-- Prioritisation of ICT access is higher in the developed world. There is still a clear divide between developed countries and emerging markets as measured by access to internet, mobile phones, and WiFi. The UK, US, and Germany lead

Information Communications Technology (ICT) access, while Mexico, Indonesia, India, China, and South Africa have the lowest access scores. An exception is South Korea, which is fifth, despite having strong government policy towards improving access.

-- The G20 countries have made limited technological progress within key industries. Australia is the top performer within the industry application category, which measures the ability of different industries (energy, health, transportation, government, and e-commerce) to leverage ICT developments, including security advancements. As an indication of uneven technological development across industries, Australia ranks first in the category overall, but only scores well within the electronic health indicator.

Page 374

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 375 to / à 536

are withheld pursuant to section

sont retenues en vertu de l'article

19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Klassen, Nathan

From: Klassen, Nathan
Sent: January-12-12 1:14 PM
To: Cameron, Bud
Subject: RE: Confirming the incident write-ups for the Weekly Summary

Txs Bud – [redacted] Cheers,

Nate
Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Cameron, Bud
Sent: January-12-12 10:07 AM
To: Klassen, Nathan
Subject: FW: Confirming the incident write-ups for the Weekly Summary

Note the suggestions for stats at the end.
Bud

From: Dincoy, Rana
Sent: January-12-12 10:03 AM
To: Bendelier, Kenneth
Cc: Cameron, Bud
Subject: FW: Confirming the incident write-ups for the Weekly Summary

FYI – I intend to respond to this e-mail. Some good suggestions (though harshly delivered in some cases!), some others that may be technically more accurate but completely obscure the meaning for senior managers....

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

From: Beaudoin, Luc S
Sent: January-11-12 7:41 PM
To: Dincoy, Rana
Cc: Moore, Bruce; Anderson, Windy
Subject: Re: Confirming the incident write-ups for the Weekly Summary

Rana, I would appreciate if you addressed your questions to me, as stated before. Bruce and the other IH are busy doing their tactical job and should not be disrupted unless a new operational matter comes to your attention and I am not around. Strategic reports review is not their role.

There are fundamentals in these reports which are in my opinion inaccurate. These subtilties are important.

1) Item 1 is stratfort. It is public, so just say their name. They are not an "agency", they are a company. Go on wikipedia

for more info.

2) Malicious email and threat actor refer usually to malware and state sponsored. Use Phishing or scam email and cyber criminals instead.

3) Don t state "potential compromise of povincial computer systems". Rather state "limited number of computer systems in Canadian Critical Infrastucture organisations potentially affected by known botnets malicious codes.

4) A website provider...replace by: a canadian internet and webhosting service provider website defaced by cyber vandals.

5) First note: typo (repeated "been" twice. Remove yellow section. State CCIRC data sources have consistently proven to be of high accuracy.

6) Not sure what US CERT has to do with DNSChanger. Remove.

7) CI finance: bank phishing does not lead to compromise. It entice users to enter PII by luring them to fake bank site (copies)

8) Comment on ISP vandalized: BEAUTIFUL !!!!

9) Stratfor: name it. [redacted] Mention the concern remains that these be used in targeted attacks by (yes) threat actors. Otherwise, phishing emails have been reported so far focussed at embarassing the stratfort organisation. No malware was reported in phishing cases at this time. Stratfort posted public information and a video about the breach as well as contacted all its clients offering them 1 year privacy protection services from a 3rd party.

10) Why are we still not stating metrics like: total and average number of canadian infected hosts per day [redacted], number of canadian host still infected by ghostclick [redacted] who will loose connection to internet on the 8 Mar, number of canadian malicious sites in sandbox reports and [redacted], Arbor networks canadian ranking, trends in these values, number of reported canadian banking phishing sites reported... Why ? These are more meaningfull SA for canada.

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: Dincoy, Rana
Sent: Wednesday, January 11, 2012 11:45 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

Dincoy, Rana

From: Dincoy, Rana
Sent: January-12-12 10:38 AM
To: Bendelier, Kenneth
Cc: Cameron, Bud
Subject: FW: Confirming the incident write-ups for the Weekly Summary

Sent this out before getting your message. You can certainly expand on it with the measures question...

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

From: Dincoy, Rana
Sent: January-12-12 10:30 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce; Anderson, Windy
Subject: RE: Confirming the incident write-ups for the Weekly Summary

Hi Luc, thanks for your comments and suggestions. You have a valid point about using the reports CCIRC receives to pull out some numbers to sketch out a picture of the cyber ecosystem. We in the strategic unit have talked about this previously and decided it would be appropriate to put them in a monthly product that would talk more about trends. We also have some work to do in terms of evaluating how meaningful these numbers would be for situational awareness and putting the right context around them for non-technical senior managers. We will also need some technical help with the analysis of that data. For example, in the next update of the Notification tool, an automatic counter and categorization by CI sector would be helpful.

As for the DNS Changer: I was under the impression you were in contact with US authorities on this matter and thought it was the CERT. If that's not true I'll remove it.

As requested, I will no longer copy the cyberdo in my e-mails for the Weekly Summary.

Thanks again for your comments and getting back to me so quickly... One of my challenges in writing this product is striking the balance between technical accuracy and clarity for non-technical readers... It's like the holy grail!

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

From: Beaudoin, Luc S
Sent: January-11-12 7:41 PM
To: Dincoy, Rana
Cc: Moore, Bruce; Anderson, Windy
Subject: Re: Confirming the incident write-ups for the Weekly Summary

Rana, I would appreciate if you addressed your questions to me, as stated before. Bruce and the other IH are busy doing their tactical job and should not be disrupted unless a new operational matter comes to your attention and I am not around. Strategic reports review is not their role.

There are fundamentals in these reports which are in my opinion inaccurate. These subtilties are important.

1) Item 1 is stratfort. It is public, so just say their name. They are not an "agency", they are a company. Go on wikipedia for more info.

2) Malicious email and threat actor refer usually to malware and state sponsored. Use Phishing or scam email and cyber criminals instead.

3) Don t state "potential compromise of povincial computer systems". Rather state "limited number of computer systems in Canadian Critical Infrastucture organisations potentially affected by known botnets malicious codes.

4) A website provider...replace by: a canadian internet and webhosting service provider website defaced by cyber vandals.

5) First note: typo (repeated "been" twice. Remove yellow section. State CCIRC data sources have consistently proven to be of high accuracy.

6) Not sure what US CERT has to do with DNSChanger. Remove.

7) CI finance: bank phishing does not lead to compromise. It entice users to enter PII by luring them to fake bank site (copies)

8) Comment on ISP vandalized: BEAUTIFUL !!!!

9) Stratfor: name it. [redacted]. Mention the concern remains that these be used in targeted attacks by (yes) threat actors. Otherwise, phishing emails have been reported so far focussed at embarassing the stratfort organisation. No malware was reported in phishing cases at this time. Stratfort posted public information and a video about the breach as well as contacted all its clients offering them 1 year privacy protection services from a 3rd party.

10) Why are we still not stating metrics like: total and average number of canadian infected hosts per day [redacted] number of canadian host still infected by ghostclick [redacted] who will loose connection to internet on the 8 Mar, number of canadian malicious sites in sandbox reports and [redacted], Arbor networks canadian ranking, trends in these values, number of reported canadian banking phishing sites reported... Why ? These are more meaningfull SA for canada.

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: Dincoy, Rana
Sent: Wednesday, January 11, 2012 11:45 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

Anderson, Windy

From: Labelle, Sébastien
Sent: January-12-12 11:18 AM
To: Hatfield, Adam; Anderson, Windy
Subject: FW: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

As discussed yesterday. Sorry for the delay.

Sébastien Labelle
Director of National Cyber Security Engagement and Partnerships /
Directeur national de la Mobilisation et des partenariats pour la cyber sécurité
National Cyber Security Directorate / Direction générale de la Cyber sécurité nationale
Public Safety Canada / Sécurité publique Canada
Room / pièce 11C079, 340 Laurier, Ottawa, ON,
tel 613-990-2655 ; fax 613-990-3287; mob 613-614-5263
sebastien.labelle@ps-sp.gc.ca

From: Dick, Robert
Sent: January-10-12 8:46 AM
To: Matz, Mark
Cc: Gordon, Robert; Hatfield, Adam; Labelle, Sébastien
Subject: Fw: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Note article on Israeli official's categorization of cyber identiy theft as an act of terrorism. In the Israeli context, situating something in that realm rather than crime could have especially interesting ramifications, if it's true.

From: PSMediaCentre/CentredesmediasdeSP
Sent: Tuesday, January 10, 2012 08:36 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Baker, William V.; Black, Dave <dave.black@rcmp-grc.gc.ca>; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, [redacted]; Crépeault, David; CSIS Media Monitoring [redacted] CYBERDO; De Curtis, Laura; Dunn, John <JDunn@justice.gc.ca>; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica <Monica.Gilbert@ic.gc.ca>; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line <Line.Patry@ic.gc.ca>; Patton, Michael; RCMP Emerging Trends <emerging.trends@rcmp-grc.gc.ca>; Roberts, Shane; Robinson, N.; Salas, Anik <ASalas@justice.gc.ca>; Slade, Nancy <Nancy.Slade@ic.gc.ca>; Spendlove, Jim; Stanfield, Charles; Stewart, Christena <Christena.Stewart@ps-sp.gc.ca>; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl <Cheryl.Wadasinghe@ps-sp.gc.ca>; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 10, 2012/ le 10 janvier 2012

Print Media

Canning the spam
The federal government can't move soon enough on its spam reporting centre, dubbed the "Freezer," which is designed to crack down on the millions of unwanted messages clogging Canadians' cellphones, inboxes and social network accounts. Times Colonist, A10

Online Media

Obama defence plan details heightened global cyber danger
US president Barack Obama has spoken of the drastically heightened cyber threat facing nations around the world, as he announced major changes to the American defence strategy. As he appeared at the Pentagon last week to unveil the new defence strategy, Obama promised to focus closely on improving the technological capabilities of the US armed forces. "We will ensure that our military is agile, flexible and ready for the full range of contingencies," he said. PC Advisor UK

Cyber tension follows hacker attack on Israeli credit card users
Last week, a hacker published credit card information belonging to about 20,000 Israelis on the Internet, along with the personal details of hundreds of thousands more. Israeli credit card companies swiftly canceled the cards and pledged to reimburse customers for damages caused by fraudulent use. Los Angeles Times

Venezuela's Chavez Backs Diplomat Who Was Expelled by US
Venezuelan President Hugo Chavez Monday night backed the South American country's consul general in Miami, who was expelled by U.S. authorities over the weekend and was linked to an alleged plot to launch a cyber attack against the U.S. government. Wall Street Journal

Israeli Official Threatens Retaliation After Cyber Attack
A top Israeli official said over the weekend that cyberattacks are akin to terrorism and threatened aggressive action against those who recently posted online personal information belonging to Israelis. PC Magazine; CNN; SC Magazine

US authorities probe Indian govt spy unit for email hacking
US authorities are investigating allegations that an Indian government spy unit hacked into emails of an official US commission that monitors economic and security relations between the United States and China, including cyber-security issues. Reuters; Forbes

SEC Push May Yield New Disclosures of Cyber Attacks on Companies
China-based hackers rifled the computers of DuPont Co. (DD) at least twice in 2009 and 2010, hunting the technological secrets that made the company one of the world's most successful chemical makers. It's not something investors would have learned from DuPont's regulatory filings, or from those of other companies victimized by hackers. Bloomberg

'Anonymous' hacktivists expose the intelligence gap
Over Christmas a busy, secretive group were at work, with their own views on who had been naughty and nice. However it was not Santa's elves, but the amorphous "Anonymous" collective making the decisions. This group of hackers released a vast trove of email addresses, passwords and credit card information belonging to subscribers of the US intelligence company Stratfor – and the hangover has carried on into the new year, with the release of MoD and Nato officials' details. The Guardian

Top UK security officials exposed in hack attack
Hundreds of sensitive email addresses for UK security officials were among details stolen in a major hacking attack, it has emerged. The hackers scooped the email addresses and other information during a Christmas attack on security consultancy Stratfor, but the type of UK officials breached has only just come to light. PC Pro

Google patches Chrome, beefs up malicious file blocking tech
Google last week patched Chrome 16 and improved the download warnings in the impending Chrome 17. Last Thursday, Google updated Chrome 16 with a security update that quashed three bugs, all rated "high," the company's second-most-dire threat rating. PC Advisor

Zeus returns: FBI warns of 'Gameover' ID-theft malware
A new variant of the notorious Zeus identity-theft Trojan is making the rounds and the Federal Bureau of Investigations (FBI) says it is capable of defeating common methods of user authentication employed by financial institutions. ZDNet

Anti-spam plan lacks teeth: Prof
If you still find your e-mail in-box inundated daily with unwanted messages from faraway royalty offering you free money or companies claiming they'll send you pharmaceuticals at a fraction of their price, you were likely pleased with the federal government's announcement of anti-spam legislation. Canoe

Do you know your cyberthreats?

The watchdogs at the Government Accountability Office this week issued a report that takes a look at what information, or guidance as they call it, is available to help government agencies and public sector companies bulk up their cybersecurity efforts. PC Advisor

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-11-12 8:38 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
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, 2012/ le 11 janvier 2012

Print Media

Privacy watchdog to probe UVic in security breach
An investigation by B.C.'s Office of the Information and Privacy Commissioner will determine whether the University of Victoria contravened accepted standards by keeping sensitive, unencrypted information about more than 11,700 employees on a mobile device. A weekend break-in at the administration services building saw the theft of laptops, handheld electronics, storage devices, cheques and a small amount of cash. The data stolen included names, payroll information and social insurance numbers of UVic employees dating back to Jan. 1, 2010. Times Colonist, A1

Computer virus scam goes viral
It's a consumer scam that reached epidemic proportions in Canada last year. You get a call from someone who says your computer is at risk of crashing because of a virus or malicious software. The caller may suggest he or she works for Microsoft and is aware of issues with your Windows operating system. Toronto Star, B1

Online Media

Energy Department to analyze power grid cyber threats
U.S. Energy Secretary Steven Chu has unveiled an initiative that seeks to further protect the power grid from cyber attacks. The Electric Sector Cybersecurity Risk Management Maturity project, a federal program to find and contain gaps in the cyber security defenses protecting the nation's electric grid, will be headed by the Department of Energy (DOE), with assistance from the Department of Homeland Security (DHS) and the private sector. SC Magazine

U.S. ousts Venezuelan consul for plotting cyberattack on U.S. nukes
Diplomats accredited to foreign governments can't be arrested, prosecuted and imprisoned by the country that hosts the embassy in which they work. It sounds like an idiotic rule when you look at the number of traffic and parking tickets UN diplomatic cars pick up in New York, but it's the only way governments can keep non-suicidal negotiators on staff who can be sent to talk to a potentially hostile governments with a reasonable chance of coming back with all their body parts attached in the traditional way. IT World

Anonymous hackers attack anti-piracy groups
Cyber-activists attacked the websites of Finnish anti-piracy groups after a local internet service provider was forced to block access to a popular file-sharing website, officials said. Antti Kotilainen, a spokesman for the Copyright Information and Anti-Piracy Centre (CIAPC), told AFP that websites run by his organisation and the International Federation of the Phonographic Industry (IFPI) had been "down since Monday". New Zealand Herald

Cyber Attacks May Be Revealed to Investors as SEC Rules Push Disclosures

China-based hackers rifled the computers of DuPont Co. at least twice in 2009 and 2010, hunting the technological secrets that made the company one of the world's most successful chemical makers. It's not something investors would have learned from DuPont's regulatory filings, or from those of other companies victimized by hackers. MSN

Obama defence plan details heightened global cyber danger
US president Barack Obama has spoken of the drastically heightened cyber threat facing nations around the world, as he announced major changes to the American defence strategy. As he appeared at the Pentagon last week to unveil the new defence strategy, Obama promised to focus closely on improving the technological capabilities of the US armed forces. Computerworld

Adobe plugs 6 critical holes in Reader
Adobe on Tuesday patched six vulnerabilities in the newest version of its popular Reader PDF viewer, making good on a late-2011 promise when it shipped an emergency update for an older edition. Computerworld

US probing hacking allegation against Indian spies
American law enforcement agencies are probing an allegation that Indian military intelligence (MI) spied on a US-China Economic and Security Review Commission member's email. The move comes after hackers posted letters and documents allegedly stolen from Indian servers in November last year. India Today

DHS asks America to run more computer virus scans
"Cyber fit" is a watchword of the President Obama's counterterrorism bureacurats, as the Department of Homeland Security (DHS) suggested this morning that Americans adopt greater online security as a New Year's Resolution. Washington Examiner

Who are the go-to cybersecurity help groups?
There are a ton of groups out there that offer cybersecurity help and guidance, the trick, it seems is finding the right one for your organization. The Government Accountability Office this week issued a report on just that notion saying: "Given the plethora of guidance available, individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture. Network World

Microsoft issues seven security patches, BEAST fix included
Microsoft on Tuesday released seven security fixes, including one cited as "critical," to correct eight vulnerabilities. None of the patches addressed major, ongoing attacks, but several were notable because Microsoft identified them as fixes that address issues that are easy to implement and capable of executing malware remotely. SC Magazine

Google patches Chrome, beefs up malicious file blocking tech
Google last week patched Chrome 16 and improved the download warnings in the impending Chrome 17. Last Thursday, Google updated Chrome 16 with a security update that quashed three bugs, all rated "high," the company's second-most-dire threat rating. PC Advisor UK

s.15(1) - Subv

s.16(2)(c)

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-10-12 8:37 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 10, 2012/ le 10 janvier 2012

Print Media

Canning the spam
The federal government can't move soon enough on its spam reporting centre, dubbed the "Freezer," which is designed to crack down on the millions of unwanted messages clogging Canadians' cellphones, inboxes and social network accounts. Times Colonist, A10

Online Media

Obama defence plan details heightened global cyber danger
US president Barack Obama has spoken of the drastically heightened cyber threat facing nations around the world, as he announced major changes to the American defence strategy. As he appeared at the Pentagon last week to unveil the new defence strategy, Obama promised to focus closely on improving the technological capabilities of the US armed forces. "We will ensure that our military is agile, flexible and ready for the full range of contingencies," he said. PC Advisor UK

Cyber tension follows hacker attack on Israeli credit card users
Last week, a hacker published credit card information belonging to about 20,000 Israelis on the Internet, along with the personal details of hundreds of thousands more. Israeli credit card companies swiftly canceled the cards and pledged to reimburse customers for damages caused by fraudulent use. Los Angeles Times

Venezuela's Chavez Backs Diplomat Who Was Expelled by US
Venezuelan President Hugo Chavez Monday night backed the South American country's consul general in Miami, who was expelled by U.S. authorities over the weekend and was linked to an alleged plot to launch a cyber attack against the U.S. government. Wall Street Journal

Israeli Official Threatens Retaliation After Cyber Attack
A top Israeli official said over the weekend that cyberattacks are akin to terrorism and threatened aggressive action against those who recently posted online personal information belonging to Israelis. PC Magazine; CNN; SC Magazine

US authorities probe Indian govt spy unit for email hacking
US authorities are investigating allegations that an Indian government spy unit hacked into emails of an official US commission that monitors economic and security relations between the United States and China, including cyber-security issues. Reuters; Forbes

SEC Push May Yield New Disclosures of Cyber Attacks on Companies

China-based hackers rifled the computers of DuPont Co. (DD) at least twice in 2009 and 2010, hunting the technological secrets that made the company one of the world's most successful chemical makers. It's not something investors would have learned from DuPont's regulatory filings, or from those of other companies victimized by hackers. Bloomberg

'Anonymous' hacktivists expose the intelligence gap
Over Christmas a busy, secretive group were at work, with their own views on who had been naughty and nice. However it was not Santa's elves, but the amorphous "Anonymous" collective making the decisions. This group of hackers released a vast trove of email addresses, passwords and credit card information belonging to subscribers of the US intelligence company Stratfor – and the hangover has carried on into the new year, with the release of MoD and Nato officials' details. The Guardian

Top UK security officials exposed in hack attack
Hundreds of sensitive email addresses for UK security officials were among details stolen in a major hacking attack, it has emerged. The hackers scooped the email addresses and other information during a Christmas attack on security consultancy Stratfor, but the type of UK officials breached has only just come to light. PC Pro

Google patches Chrome, beefs up malicious file blocking tech
Google last week patched Chrome 16 and improved the download warnings in the impending Chrome 17. Last Thursday, Google updated Chrome 16 with a security update that quashed three bugs, all rated "high," the company's second-most-dire threat rating. PC Advisor

Zeus returns: FBI warns of 'Gameover' ID-theft malware
A new variant of the notorious Zeus identity-theft Trojan is making the rounds and the Federal Bureau of Investigations (FBI) says it is capable of defeating common methods of user authentication employed by financial institutions. ZDNet

Anti-spam plan lacks teeth: Prof
If you still find your e-mail in-box inundated daily with unwanted messages from faraway royalty offering you free money or companies claiming they'll send you pharmaceuticals at a fraction of their price, you were likely pleased with the federal government's announcement of anti-spam legislation. Canoe

Do you know your cyberthreats?
The watchdogs at the Government Accountability Office this week issued a report that takes a look at what information, or guidance as they call it, is available to help government agencies and public sector companies bulk up their cybersecurity efforts. PC Advisor

Dincoy, Rana

From: Dincoy, Rana
Sent: January-11-12 11:46 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: Confirming the incident write-ups for the Weekly Summary

Hi Luc,

Can you please confirm the below? I've spoken with Bruce to obtain clarification where I needed it (Bruce please let me know if something isn't right).

I want to make sure particularly that I am not overstating things in my "Comments" section. I'd appreciate your feedback by tomorrow morning... Thanks! Rana

For the Week of 31 Dec 2011 – 6 Jan 2012

Issued: 12 Jan 2012

HIGHLIGHTS:

Notable Incidents:

- Client information for a private US intelligence agency posted on the Internet by Anonymous – clients include Canadians
- Malicious e-mails from threat actors impersonating Canadian banks, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems of provincial government, financial, transportation, and education sector organizations
- A website hosting service provider's website vandalized by hackers

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 31 DECEMBER 2011 THROUGH 6 JANUARY 2012:

Canadian Critical Infrastructure:

Provincial Government, Transportation and Education: Computers of two provinces' departments of education, an airport authority and four universities may have been compromised by certain common malicious software. There were also reports of compromised computers as a result of the worldwide internet fraud "Ghostclick", which the FBI exposed in late 2011.

CCIRC notified contacts in those organizations of these potential compromises and offered mitigation advice. Impact of the compromises is unknown but could potentially include data theft or remote use of these computers to commit malicious acts on the Internet. In the "Ghostclick" fraud, computer users were unknowingly re-directed to certain webpages, which financially benefited the fraudsters.

Comment: Open source computer infection reports indicate which organizations appear to be infected with certain commonly found malicious software. However, only the affected organization can confirm whether their computers have been truly been infected and the impact. **While there hasn't been any such confirmation in this situation, CCIRC believes it likely that there were compromises.**

CCIRC continues to notify stakeholder organizations that were impacted by the worldwide Ghostclick fraud and is in contact with US CERT.

Financial Sector. Threat actors impersonating prominent Canadian banks tried to compromise computer users' machines by persuading them to click on malicious links in an e-mail. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious links led to websites hosted in United States, France and Spain.

Telecommunication Sector. CCIRC observed that a website operated by an internet hosting service provider was vandalized by hackers. The impact is unknown.

Comment: Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website that can be vandalized by hackers is also vulnerable to being used to compromise the computers of that website's visitors.

International:

Anonymous, the famed hacker group, released personal and credit card information of a private US intelligence company's clients, on the Internet. These include Canadian clients. CCIRC notified the Canadian stakeholders and offered mitigation advice. CCIRC continues to analyze the situation.

Comment: The personal information released includes names and e-mail addresses, which can be used for a variety of malicious purposes by any threat actor. This can include sending malicious e-mails to those clients to compromise their computers or using the credit card information for financial gain. The release of physical addresses could be of concern to certain clients for privacy and security reasons.

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

Public Safety Canada | Sécurité publique Canada

CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

WEEKLY CYBERSECURITY REPORT FOR CIOs

CCIRC CYBER AWARNESS PRODUCT: 12-S-001
WEEK OF JANUARY 3, 2012

s.16(2)(c)

Purpose

To inform security and information technology executives in government and critical infrastructure sectors about cyber events and notable news seen by the Canadian Cyber Incident Response Centre.

Overview

There was no new nation-wide cyber security incident this week. The major event of the week was the hacking of STRATFOR, a private US intelligence company, where clients' online credentials and credit card information was leaked. [redacted] were affected. CCIRC continued to receive reports on common computer infections that benefit cyber criminals and fraud attempts to access Canadians' bank accounts or credit. There are also continued reports of Ghostclick fraud victims in Canada.

Highlights

New Events reported to CCIRC:

- Client information for STRATFOR, a private US intelligence company, posted on the Internet by a hacker group – clients include Canadian federal and provincial employees
- Infection reports in computer systems of provincial government, financial, transportation, and education sector organizations
- Fraudsters impersonating Canadian banks, enticing Internet users to reveal personal information and financial credentials
- An Internet and webhosting service provider's website vandalized by hackers

Updates:

- Ghostclick fraud notifications continue – 19,000 hosts in Canada remain infected

CCIRC Products Released this week: None

Noteworthy News:

- Hackers impersonating U.S. Computer Emergency Response Team (US-CERT) targeting U.S. federal, state, and local governments, as well as many US private sector organizations
- Symantec's Norton AntiVirus source code exposed by hackers

Canada

NEW EVENTS REPORTED IN CANADIAN CRITICAL INFRASTRUCTURE

Federal Government Sector

(content to be supplied by CTEC)

Non-Federal Government Sector

STRATFOR hacking. CCIRC learned from law enforcement that personal and credit card information of Strategic Forecasting Inc (STRATFOR)'s report clients were posted on the Internet by a hacker group. STRATFOR is a US intelligence company. [redacted] were affected. Hackers claimed to be part of Anonymous, but Anonymous denied this claim and denounced the attack. Credit card information stolen was used to make donations to charity, but these transactions have since been reversed by the credit card issuing banks.

CCIRC has provided incident details and mitigation advice to contacts at the Canadian Government CERT, provincial governments and Canadian Internet Service Providers. CCIRC remains in contact with Canadian law enforcement about this incident and will reach out to its stakeholders if they have been affected.

Comment: *Organizations whose employees subscribe to STRATFOR's website reports should implement measures to ensure employee password and credit card information is secure. Employees whose names and corporate e-mail addresses have been leaked may also be targeted by malicious actors via e-mail to steal information or credentials. The release of physical addresses could also be of concern to certain clients for privacy and security reasons. STRATFOR has been criticized by some experts for not using standard protection measures for the credit card information.*

Credential stealing malicious software infections. CCIRC received reports indicating computers of two provinces' departments of education and two banks were infected with common malicious software (Torpig/Mebroot). This malicious software is typically used by cyber criminals to discover financial/banking credentials of computer users and is quite common. **CCIRC** reached out to contacts in those organizations and offered mitigation advice.

Comment: *The organizations in question were unaware they were infected until they were notified by CCIRC. It is critical the affected organizations remedy the situation as soon possible because the presence of these infections likely means the organization's anti-virus protection has been compromised and software patching may be disabled. This may have exposed the organization to other types of undetected malicious software. Organizations whose networks are open to the public or who regularly interact with the public online may be more susceptible to these types of common infections. It is recognized that on-going checking of infection reports and clean-up of these infections can be resource intensive.*

Fraud attempts in Financial Sector. CCIRC received reports from law enforcement that fraudsters impersonating prominent Canadian banks and a credit card company tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown how many computer users provided their credential to these fraudsters. The links in these e-mails led to websites hosted in United States, France and Spain.

CCIRC notified the financial institutions of these fraud attempts. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website vandalized. CCIRC observed that a website operated by an Internet and webhosting service provider in Manitoba was vandalized by hackers. CCIRC notified the service provider, who then applied a software patch and remedied the situation.

Comment: *Organizations should monitor their websites and be vigilant against website defacements. Website vandalism can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to vandalism may also be used to compromise the computers of that website's visitors.*

UPDATES:

Ghostclick Fraud. There were new reports of infected computers in a provincial government, an airport authority and four Canadian universities attributed to Operation Ghostclick. This worldwide fraud campaign, exposed in late 2011 by the FBI, hijacked Internet web searches and diverted users from legitimate websites to websites that generated advertising and sales revenue for a criminal cyber ring. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to monitor the situation. As new reports come in, CCIRC will continue to reach out to affected partner organizations.

Comment: *According to reports received, CCIRC estimates there are still about 19,000 hosts in Canada where mitigation measures haven't been taken. These computers could lose their connection to the Internet on March 8, 2012, if their owners/operators do not take mitigation measures. Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. It should be noted many of the reported infections are on computers of ordinary Canadians that connect to the Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*

NOTEWORTHY NEWS IN THE MEDIA:

Fraudsters posing as U.S. Cybersecurity organization. A number of U.S. officials as well as certain private sector organizations are receiving e-mails from fraudsters impersonating the U.S. Computer Emergency Readiness Team (US CERT). The true US CERT has issued a public alert about this phishing campaign. The impact of this event is unknown.

Comment: *Organizations should be vigilant with all incoming e-mails, even from supposedly trusted sources. Fraudulent e-mails like this are often used by fraudsters to install viruses when opened, or they entice users to enter their personal information for a seemingly legitimate purpose. This type of incident not only damages the US CERT's credibility with its stakeholders but also could suggest someone is targeting a sizable IT security community's information. Technical*

analysis of these e-mails by US CERT continues and pertinent information will likely be shared with international partners like CCIRC.

Symantec's Norton Antivirus source code exposed by hackers. A hacker group called "the Lords of Dharmaraja" claimed to have stolen Symantec source code and documentation from the servers of Indian intelligence agencies. Symantec publicly confirmed that a segment of its source code was accessed from a third party. Symantec stated "there are no indications that customer information was impacted or exposed at this time".

Comment: *Symantec's Norton Antivirus code is commonly used around the world to protect computer systems. The stolen source code is said to be for an older version of the Antivirus software, so organizations are advised to ensure their antivirus protections are up to date.*

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

s.16(2)(c)

Grigsby, Alexandre

From: Grigsby, Alexandre
Sent: January-10-12 2:48 PM
To: 'Vivasvat.Dadwal@international.gc.ca'
Cc: Heather.Dryden@ic.gc.ca; 'Dvorkin, Corey'
Subject: RE: Tech gets its day in Congress as SOPA fight continues

That's why you avoid picking fights with the Internets

From: Vivasvat.Dadwal@international.gc.ca [mailto:Vivasvat.Dadwal@international.gc.ca]
Sent: January-10-12 12:39 PM
To: Loris.Mirella@international.gc.ca
Cc: Sean.Clark@international.gc.ca; Grigsby, Alexandre; Heather.Dryden@ic.gc.ca; Jonathan.Solomon@international.gc.ca; Lynn.McDonald@international.gc.ca; Nicholas.Gordon@international.gc.ca
Subject: RE: Tech gets its day in Congress as SOPA fight continues

And to add to that, check the link out:
Stay On Top of the Fight Against SOPA/PIPA with These Tools: [redacted]

They have developed tools to monitor the situation!

From: Dadwal, Vivasvat -TMI
Sent: January 10, 2012 12:33 PM
To: Mirella, Loris -TMI; [redacted]
Cc: Clark, Sean -WSHDC -TD
Subject: RE: Tech gets its day in Congress as SOPA fight continues

This was in TIME magazine a couple of days ago...don't think it would ever happen, but interesting to think about it anyhow.

SOPA: What if Google, Facebook and Twitter Went Offline in Protest?

By Graeme McMillan

Can you imagine a world without Google or Facebook? If plans to protest the potential passing of the Stop Online Piracy Act (SOPA) come to fruition, you won't need to; those sites, along with many other well-known online destinations, will go temporarily offline as a taste of what we could expect from a post-SOPA Internet.

Companies including Google, Facebook, Twitter, PayPal, Yahoo! and Wikipedia are said to be discussing a coordinated blackout of services to demonstrate the potential effect SOPA would have on the Internet, something already being called a "nuclear option" of protesting. The rumors surrounding the potential blackout were only strengthened by Markham Erickson, executive director of trade association NetCoalition, who told FoxNews that "a number of companies have had discussions about [blacking out services]" last week.

According to Erickson, the companies are well aware of how serious an act such a blackout would be:

> This type of thing doesn't happen because companies typically don't want to put their users in that position. The difference is that these bills so fundamentally change the way the Internet works. People need to understand the effect this special-interest legislation will have on those who use the Internet.

The idea of an Internet blackout should seem familiar to anyone who's been paying attention to the debate so far. In addition to a blackout already carried out by Mozilla, hacking group Anonymous proposed the same thing a couple of weeks ago, suggesting that sites replace their front pages with a statement protesting SOPA. That suggestion itself came a week after Jimmy Wales had asked Wikipedia users about the possibility of blacking out that site in protest of the bill.

(**MORE:** 'Anonymous' Blacks Out the Internet in Response to SOPA Debate)

As a way of drawing attention to the topic, it's something that will definitely work. Just Google alone going dark would cause havoc online, but the idea of it happening at the same time as Facebook, Twitter et al. follow suit seems almost unimaginable.

The question then becomes how to translate the inevitable confusion and outrage from those who don't know what SOPA is into activism. The key, I assume, lies in the execution of the blackout: Will the sites that voluntarily go down be entirely unavailable or will they follow the Anonymous-proposed model of replacing the front page with a statement explaining what is going on, why and how users can best become involved in the discussion? If the sites do go *entirely* dark, is the hope that the resulting outrage will be enough to fuel news stories about the reason behind the decision? And that users will not transfer their frustration to the sites themselves, as opposed to the bill they're protesting?

The fact that Facebook and Twitter are both said to be considering taking part in the blackout is simultaneously heartening and worrying. The former because, well, they're standing up for what they collectively believe in — and that's a good thing. But the latter because the lack of availability for social media on the proposed blackout day feels like it's giving up the best chance to harness the frustration and energy people will feel about the temporary loss of the Internet as they know it, and a great possibility to focus and direct that energy into productive activism against SOPA. Then again, it may take losing Facebook and Twitter to really drive home how dramatically SOPA could affect the Internet.

All of this may come to nothing, of course. The companies may decide not to black out their sites and find other ways to protest SOPA. That could be for the best; collectively closing down the most trafficked sites on the Internet to prove a point will certainly garner a lot of attention, but the effects it'll have beyond that (and the reactions it'll cause as a result) are difficult to predict and could easily end up causing a backlash against the sites responsible at a time when they least want it. But still ... just try to imagine an Internet without Google, Facebook or Yahoo. Even for a day. Almost makes you want it to happen, just to make people realize how reliant we are on the Internet as we know it now, doesn't it?

MORE: Sorry, Folks: Game Publishers Didn't 'Drop' SOPA Support

Graeme McMillan is a reporter at TIME. *Find him on Twitter at @Graemem or on Facebook at Facebook/Graeme.McMillan. You can also continue the discussion on* TIME's *Facebook page and on Twitter at @TIME.*

Related Topics: *Anonymous, mozilla, paypal, SOPA, Stop Online Piracy Act, wikipedia, Yahoo, Companies, Facebook, Google, Reviews & Features, Social Unrest, Twitter*

Read more: http://techland.time.com/2012/01/05/sopa-what-if-google-facebook-and-twitter-went-offline-in-protest/#ixzz1j4sNzEBa

---

From: Mirella, Loris -TMI s.16(2)(c)
Sent: January 10, 2012 12:28 PM
To: [redacted]
Cc: Clark, Sean -WSHDC -TD
Subject: Tech gets its day in Congress as SOPA fight continues

Tech gets its day in Congress as SOPA fight continues

By Stacey Higginbotham Jan. 9, 2012, 1:10pm PT 2 Comments
http://gigaom.com/2012/01/09/tech-gets-its-day-in-congress-as-sopa-fight-continues/

Representative Darrell Issa (R-Calif.) has called a hearing that will bring more voices from the technology industry to Washington, D.C. to discuss how legislation such as the Stop Online Piracy Act (SOPA) would affect the Internet. On Jan. 18, industry representatives that include Brad Burnham from Union Square Ventures; Lanham Napier, the CEO of Rackspace Hosting; and Alexis Ohanian, co-founder of Reddit.com, will testify before Congress.

At the previous SOPA hearing, the tech industry was represented by a single Google executive, while the five other participants testifying were from the content industry. Issa's upcoming hearing, however, is not about SOPA directly. Issa – who is pushing his own version of an IP protection bill dubbed the Online Protection and Enforcement of Digital Trade, or OPEN, Act – is holding his hearing on how Congress can help protect IP without breaking the Internet. Perhaps it can also lead to legislation that actually solves the problem of piracy a bit better as well. From his release:

> House Committee on Oversight and Government Reform Chairman Darrell Issa (R-CA) today announced that the Full Committee will hold a hearing on January 18 to examine the potential impact of Domain Name Service (DNS) and search engine blocking on American cyber-security, jobs and the Internet community. In light of policy proposals affecting the way taxpayers access the Internet, the hearing will also explore federal government strategies to protect American intellectual property without adversely affecting economic growth. The Committee will hear testimony from top cyber-security experts and technology job creators.

This news comes amid some wins and losses around SOPA overall. Despite wrongly fingering Rep. Paul Ryan (R-Wis.) as a co-sponsor of the SOPA bill, Reddit users appear to have forced the Wisconsin Congressman to take a stand against the legislation, while a look at the TV operations of news organizations whose parent companies are in support of SOPA show that those organizations are not covering the issue in depth for their viewers (but they are doing so online). As we wait for the next official SOPA markup hearing later this month (the last attempt to push the legislation out of committee was delayed over the Congressional recess), Issa's hearing will be a chance for the tech community to make its points. Hopefully, someone in the House Judiciary Committee committee that's holding the SOPA markups will be listening.

Loris Mirella
Intellectual Property Trade Policy Division (TMI) | Direction de la politique commerciale sur la propriété intellectuelle (TMI)
111 promenade Sussex Drive loris.mirella@international.gc.ca
Tel. | Tél. 613-996-8312
Facsimile | Télécopieur 613-944-0066
Foreign Affairs and International Trade Canada | Affaires étrangères et Commerce international Canada

Government of Canada | Gouvernement du Canada 125 promenade Sussex Drive, Ottawa, ON K1A 0G2

Klassen, Nathan

From: Klassen, Nathan
Sent: January-06-12 10:04 AM
To: Williston, Sandra
Subject: RE: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

Looks great!

From: Williston, Sandra
Sent: January-06-12 9:56 AM
To: Anderson, Windy
Cc: Klassen, Nathan; [redacted]
Subject: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

CCIRC CE11-2549
File No.: 384942
RDIMS No.: 541243

Hello Windy;

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

Stratfor Global Intelligence has already notified all affected users through email, facebook and twitter. The mitigation advise to their customers was to contact their financial institution and inform them of this incident and to watch for any unauthorized activity on their accounts. In addition, they have advised that they will provide paid subscribers with identity protection coverage with a leading provider of global identity protection company at their expense for 12 months.

CCIRC has completed notifications to Federal and Provincial STRATFOR clients through their respective IT Security departments. The final count of affected users is [redacted] users in 9 Provinces. CCIRC provided further mitigation advise to affected Government employees to be on the outlook for targeted email attacks and social engineering which may result from this compromise.

CCIRC has closed this incident and will continue to monitor.

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

Klassen, Nathan

From: Williston, Sandra
Sent: January-06-12 9:56 AM
To: Anderson, Windy
Cc: Klassen, Nathan; [redacted]
Subject: CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

s.16(2)(c)

CCIRC CE11-2549
File No.: 384942
RDIMS No.: 541243

Hello Windy;

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

Stratfor Global Intelligence has already notified all affected users through email, facebook and twitter. The mitigation advise to their customers was to contact their financial institution and inform them of this incident and to watch for any unauthorized activity on their accounts. In addition, they have advised that they will provide paid subscribers with identity protection coverage with a leading provider of global identity protection company at their expense for 12 months.

CCIRC has completed notifications to Federal and Provincial STRATFOR clients through their respective IT Security departments. The final count of affected users is [redacted] users in 9 Provinces. CCIRC provided further mitigation advise to affected Government employees to be on the outlook for targeted email attacks and social engineering which may result from this compromise.

CCIRC has closed this incident and will continue to monitor.

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

January 5

UNCLASSIFIED

DATE:

File No.: 384942
RDIMS No.: 541243

MEMORANDUM FOR THE DIRECTOR GENERAL

CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

(Information only)

ISSUE

Thirty four Federal Government workers and an unknown number of Provincial, Municipal, and Critical Infrastructure users have been affected by the hacking of a private international intelligence agency.

BACKGROUND

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

CONSIDERATIONS

There are financial, workplace security, and privacy considerations regarding this incident.

First, there is a financial risk to all impacted individuals as the credit card information posted online contained the full 16 digit number, expiry date, and Card Verification Value number (i.e. everything needed to make purchases).

Second, compromised individuals could be victims of specific and targeted attacks, such as malicious emails, social engineering, and attempts to compromise workplace security.

Third, impacted individuals privacy could be compromised as work/ home telephone numbers and work/home addresses were released. Given the fact that 860,000 login credentials have been compromised, there is also a strong likelihood that additional downstream privacy risks exist for impacted individuals as a significant percentage of the population uses the same password for many internet sites and work.

NEXT STEPS

There are three main actions CCIRC is taking to address this situation.

First, CCIRC is working with RCMP to identify Federal Government users registered with STRATFOR. Identified users will be notified through CTEC.

Second, CCIRC is performing further analysis in order to identify and notify any Provincial, Municipal and Critical Infrastructure users who have been affected.

Third, CCIRC plans to recommend that affected users change all internet account passwords that use elements from their compromised password; monitor their credit card transactions and; contact their bank regarding the credit card breach.

We will inform you of any significant developments. Should you require additional information, please do not hesitate to contact me at 991-7055.

Windy Anderson
Director, CCIRC
National Cyber Security

Prepared by: Nate Klassen
Sandra Williston

Page 569

is a duplicate

est un duplicata

Page 570

is a duplicate

est un duplicata

Page 571

is a duplicate

est un duplicata

Page 572

is a duplicate

est un duplicata

Page 573

is a duplicate

est un duplicata

Page 574

is a duplicate

est un duplicata

Key Ethical and Legal Trends in the Next Decade and Implications for Cyber Security Policy

Draft - Not for Distribution

David Fewer

5 January, 2012

Table of Contents

Executive Summary

Analysis

Issue #! - The Decline of Privacy

Issue #2 - Hacktivism

Issue #3 - The Surveilled State

Issue #4 - The Hacktivist State

Conclusions and Recommendations

Introduction

The dispersal of technological innovation throughout the publicly available communications infrastructure is changing the way individuals interact.

As communications tools move onto the internet, they are becoming social, meaning they are interactive. Participants do not simply receive information, but dynamically volunteer information themselves. These tools are networked, dynamic and evolutionary. Social interactions on them may be publicly available or protected from public view in some way, and may involve a single voice in the dark or a virtual mob. Social networks such as Facebook and Twitter are obvious examples of social communications media, but even older information communications formats, such as newspapers, as they move onto the internet offer new means of interacting with readers. These range from permitting readers to post comments to news stories to promoting the live interaction of "readers" with online journalists or interview subjects.

Communications tools are becoming increasingly mobile, as well. Divisions between communications categories are crumbling: telephony and broadcast no longer make good definitions for categories of communications; internet and proprietary networks are overlapping. All of the tools available over the internet are being made available over networks that have historically borne much greater control than the internet. The regulability of these private networks has implications for security policy.

Communications media are also fractured today like never before. Consider telephony: in the past, a single network ensured regulability from a public safety perspective. The introduction of mobile networks complicated that picture, but the inherent regulability of these networks was not compromised. Today, the internet has introduced new tools and formats for voice communications, and the potential for participants to use encryption further complicates the regulability of communications. Expand the range of communications to include text exchanges and one gets a sense of the challenge facing public safety officials.

Finally, these innovations in communications technologies has permitted a greater range of instant, real-time communications. Text now enjoys the same immediacy as voice communications. However, many of these technologies also introduce persistence to what may be considered a real-time exchange. Text messages, for example, may replace a vocal conversation but stay on the network for later review.

These disruptive innovations pose challenges to the abilities of those charged with ensuring public safety to do their jobs. The potential responses to these challenges raise, in turn, challenges to both ethical and legal rules governing the conduct of public safety officers. This report explores key ethical and legal trends over the next decade and considers the implications of these trends for cyber security policy.

This Report considers both ethical and legal trends in relation to cyber security policy. This mandate merits some discussion. First, the context limits the Report's exploration of trends. Although one might fully expect the adoption of alternative energy sources to be a dominant ethical and legal trend over the next decade, it is one which is unlikely to have implications for cyber security policy and so receives no consideration in this Report. The Report examines

cyber security, and so focuses on ethical and legal trends in *cyber* space - communications media and tools.

Second, "ethical trends" refer to the evolution of those norms governing the conduct of those charged with ensuring the safety of the Canadian public. "Norms" in this sense embraces the collective understanding of acceptable behaviour that act to both guide and restrain behaviour. Laws may reflect norms; theft, for example, is a violation of both the *Criminal Code* and our common understanding of acceptable behaviour. But not all norms find an equivalent in our laws. Plagiarism, for example, violates many rules of social interaction but finds no equivalent in the laws of Canada.

Third, "legal trends" refer to the evolution of the rule of law and its enforcement. The "rule of law" refers to the principle that governance occurs through adherence to known principles. Law enforcement agents act pursuant to lawful authority: what they enforce are laws, not policies or arbitrary decisions. Their exercise of authority is also derived from law: their powers of action are again derived from law, and not arbitrary. Institutions of democratic governance provide authority for both the law enforced and the powers of action permitting its enforcement.

Cyber security policy is ordinarily conceived of as the realm of public officers, but in practice the execution of those policies requires significant co-operation amongst public and private entities. For this reason, this Report's examination of ethical and legal developments will consider developments for both public and private actors. What happens in the marketplace may have a significant impact on individual action. In this sense, private actors - businesses - may act as a regulator of individual behaviour. This may accordingly have implications for cyber security policy.

Any exercise in prognostication is necessarily an exercise in guesswork. However, that guesswork can be guided by making reasoned assumptions.

First, this Report proceeds on the assumption that developments in technology and the safeguarding of the public over the next decade will have their roots in present developments. This Introductory section began with a discussion of the recent evolution of communications technologies, and offered the thesis that modern communications media and tools are becoming increasingly social, mobile, fractured and instant. The Report assumes this trend will continue.

Second, this Report assumes that the public response to the the tragedy of 9/11 will be generational, and not simply political. In other words, the Report proceeds with the view that the response of governance institutions to 9/11 has fundamentally changed the way those institutions approach security and the trade-offs involved. This approach has profound implications for privacy and other civil liberties, and potentially challenges principles that lie at the root of democratic states.

Finally, the Report assumes that no catastrophic, unforeseeable event disrupts global society over the next decade. A report drafted in the year 2000 prognosticating on the future of security

policy in the first decade of the twenty-first century would have been reduced by 9/11 a year later to the status of a historical curiosity. Similarly, scandal, gross abuse of power, or public outrage over a glaring usurpation of democratic institutions could result in the scaling back of powers enjoyed by law enforcement agents. These sorts of events are always possible, but by nature not amenable to prediction.

In Part I, the Report describes the methodology employed in its development. In Part II, the Report turns to considering likely key ethical and legal trends over the next decade and their implications for cyber security policy. The Report focuses on the following four key trends:

(1) **The Decline of Privacy** - The next decade will see a steady erosion in both the degree of privacy enjoyed by individuals in the marketplace and the willingness of regulators to take firm action to limit the ability of market participants to intrude on the privacy of individuals.
(2) **Hacktivism** - Individuals are willing to act collectively to use use online communications tools and privacy enhancing technologies to engage in "extra-legal" activism - policy-directed action that may violate the law. Hailed as online civil disobedience or damned as terrorism, the phenomena will continue.
(3) **The Surveilled State** - Law enforcement agents will enjoy unprecedented powers to surveill ordinary citizens and subjects both within and without their borders.
(4) **The Hacktivist State** - Mirroring Hactivism, state agents will enjoy aggressive new powers to investigate and disrupt threats to cyber security.

For each of these key trends, the Report offers a description of the trend, identifies the drivers behind the trend, and considers its Implications for cyber security policy. Part III concludes this Report with recommendations for government action in light of these trends.

Part I - Methodology

Crafting this paper involved undertaking significant research. Our research will embraced three streams:

- Academic Literature Survey: We conducted a traditional survey of academic periodicals and other secondary literature, making use of both legal and social science databases and search tools.
- Public Source Survey: In the area of computer and online security, much of the most innovative writing and thinking occurs in non-traditional venues, such as blogs; websites of civil society organizations; publications of security researchers, research firms and consulting firms; online publications not otherwise indexed by academic periodical indexes; and, of course, government publications. We conducted a thorough online search of these sources.
- Primary Source Research – Interviews: We interviewed a half dozen or so individuals known to us to be involved in thinking about technological security, threat detection and harm prevention, including:
    - David McMahon, Bell Canada, National Security and Complex Programs;

- Bill St. Arnaud – former Chief Research Officer for CANARIE Inc., Canada's Advanced Internet Development Organization;
- Professor Ron Diebert, Director of the Citizen Lab, Monk School of Busness, University of Toronto;
- members of the Software Security Research Group, a collaborative project between SITE (the School of Information Technology and Engineering) at the University of Ottawa and IBM;
- Google Engineering – individuals at Google provided their time and thoughts on some of the
- Security firm contacts – We will reach out to contacts at businesses involved in selling security solutions to consider their perspectives. Targeted firms include Sophos (Vancouver) Blue Coat (Ottawa) and Symantec (Cupertino).

Our initial research centred around technological phenomena reshaping the ways we communicate today. These include:

- "Cloud Computing";
- The mobile network;
- "Social Media" and security;
- the industrialization of malware production (the economic basis for online
- crime); and
- "Hacktivism".

Finally, we posed questions to individuals at Public Safety to gain an understanding of their perspectives, and their expectations with respect to this Report.

Part II - Analysis

The second decade of the twenty-first century has seen the emergence of a number of online phenomena, and the continuation of many phenomena originating in the previous decade. These are, to a significant extent, driven by the disruptive technological innovations canvassed in the Introduction of this Report: social media, fractured communications streams, mobile networks, and real-time exchanges. They are also global phenomena: the innovative use of communications technologies that facilitated the Arab spring has also helped differentiate the Occupy movement from previous protest movements in North America.

This Report has focused on the following four key emerging or continuing ethical and legal trends:

(1) **The Decline of Privacy** - The next decade will see a continuing diminishment of the privacy enjoyed by individuals.
(2) **Hacktivism** - Online activism will continue to explore the grey areas at the borders of lawful activity, and the forbidden areas beyond the law.
(3) **The Surveilled State** - States will move closer to the model of citizen oversight exercised by China than that espoused in the past by Western states.
(4) **The Hacktivist State** - States will begin enacting laws legitimizing the State's authorization of the kinds of tactics employed by Hacktivists against them.

The first two of these trends focus largely on developments in the private sphere, rather than the public sphere, but which have obvious implications for cyber security. The final two trends more directly involve the exercise of public power but, interestingly, potentially implicate private actors acting as state agents. An overarching theme, common to all of these trends, is the increasing interdependence of public and private agents in securing public safety online.

Some might characterize this list as overly pessimistic, and taking a dim view of civil liberties' prospects in the coming decade. Certainly, that is one facet of these trends. However, with accountability, realistic safeguards against abuse, enshrined instiutional balances, and when derived from lawful authority, expanded state powers may be consistent with liberty and democratic values. Moreover, expanded state powers can do a world of good when directed against real threats to liberty, democracy, and economic values.

Issue #1: The Decline of Privacy

(a) Description

The first decade of the twenty-first decade has seen the sphere of privacy enjoyed by individuals shrink. This has predominantly occurred online through the development of an infrastructure of commercial surveillance. Social networking services such as Facebook have developed sophisticated infrastructures to mine the personal data of site users. Regulators have blessed these activities provided the service is transparent about its practices. The transparency requirement is met so long as the service discloses its practices, even ex post, somewhere on its service. In this way, "transparency" is replacing consent as the mechanism for evading liability for invasion of privacy, and contractual standards of exchange are replacing knowledge as the standard for consent. The end result is that individuals currently enjoy a sphere of personal privacy greatly diminished from that enjoyed a decade ago.

The next decade will see continued erosion of both the sphere of privacy enjoyed by individuals in the marketplace and a willingness of regulators to limit the ability of commercial actors to intrude on the privacy of individuals. The legal model describe above for obtaining the right to collect, use and exchange the personal information of individuals is expanding out from social networks to mobile networks and even use of internet-based devices such as the iPad. The coming decade will see continued expansion of the reach of the information network into an ever-expanding range of devices: from smart-phones and smart-metres today to smart energy devices tomorrow to even networked automobiles tomorrow. Each of these devices will collect, use and exchange the personal information of users and individuals interacting with those users. The proprietors of those devices will similarly employ contracts and notices to evade restrictions on the manner in which it may deal with that personal information.

(b) Drivers

The decline of privacy may be laid at the feet of three predominant drivers: technology, the marketplace, and the regulatory regime overlying privacy laws.

From a technological perspective, the emergence of tools and services that permit effective surveillance of users has permitted this system to evolve. However, these tools have been around for some time. What is different today is the emergence of a marketplace willing to use these tools. Finally, the development of a legal framework amenable to this market structure has enabled the phenomenon. This legal framework has its origins in two camps: one American, the other Canadian. First the absence in the United States of dedicated privacy protection laws means that privacy interests may be dealt with in that jurisdiction on a liability rules basis: under the US framework, fraud, misrepresentation, and unfair trade practices trigger liability, not an absence of consent. Second, Canada's comprehensive private sector personal information protection legislation, PIPEDA, has been interpreted to adhere effectively to the American standard of privacy protection. Globally, other privacy regulators have not departed markedly from the lead set by Canadian privacy regulators.

(c) Implications

Privacy is not dead, contrary to some assertions. It is, however, a greatly reduced impediment to the collection, use and disclosure of personal information by private actors. This replacement of consent with transparency as the tool for evading liability for dealing with personal information has significant benefits for public agents such as law enforcement and public security agencies.

First, individual privacy rights may pose a potential barrier to private actors in securing the viability of their own infrastructure. For example, objectives of public safety include securing critical infrastructure such as communications facilities and public internet infrastructure. Most agreements among service providers and their customers will include sweeping consents to ensuring infrastructure integrity and responding to security threats.

Second, law enforcement and security agencies routinely engage in public-private partnerships in furtherance of general public safety. Simply, public agencies lack the expertise oversee the operation of private networks and services. Similarly, private actors lack the expertise (and lawful mandate) to address security concerns arising from use of their services and facilities. Co-operation between public and private actors has grown common. While it is possible for laws to address the liability concerns of both participants to these partnerships, it can be simpler to deal with individual privacy claims contractually. Consent can address a number of risks law enforcement may encounter in collecting and using evidence in court: why bother with a warrant when the user has already clicked "OK" to disclosures to law enforcement requests?

Issue #2: Hacktivism

(a) Description

Individuals are willing to act collectively to use use online communications tools and privacy enhancing technologies to engage in "extra-legal" activism - policy-directed action that may violate the law. Hailed as online civil disobedience or damned as terrorism, the phenomena will continue over the coming year.

Hacktivism was not born with the Wikileaks-cablegate controversy of 2010, nor did it first achieve political signficance with the Arab Spring of 2011. However, Hacktivism did occupy the global spotlight with the consecutive development of these events. Today, we may describe "Hacktivism" as politically motivated digital disruption of specific targets. While some Hacktivist

groups operate under a brand (such as "Anonymous" and "LulzSec"), in practice Hacktivism is a leaderless, geographically dispersed and socio-economically diverse phenomenon.

We must distinguish politically motivated attacks from hackers and "script kiddies" motivated by entertainment or the "challenge" of overcoming the defenses of a formidable online presence. Hacktivism, in contrast, is motivated by political objectives and generally involves a collective of like-minded participants. This implies no formal organization but simply an agreement to work on a common objective.

We should also recognize that Hacktivism does not exclusively employ illegal tactics such as breaching security and engaging in denial of service attacks. Hacktivism also employs legal tools of protest. Civil protest is inevitably moving online.

(b) Drivers

The emergence of Hacktivism has been driven by technology and, this Report argues, by a normative response to public-private security and law enforcement partnerships.

From a technological perspective, the primary tools of Hacktivism remain data breach and denial of service attacks. These have proven effective tools: once selected, a target is inevitably compromised. Organizational tools involve commonplace online communications vehicles such as image boards, Internet Relay Chat and private servers. Hacktivists also make ample use of privacy-enhancing technologies, using encryption and onion routing to cover traces of their activities. These are not new techologies. Indeed, hacking collectives are not themselves new phenomena. What is new is the politically motivated co-ordintated deployment of these web service disruption tools against select targets.

The cause of this is arguably normative: commercial actors have been perceived to be in alliance with law enforcement and in so doing have arguably broken a norm of neutrality: commercial actors do not co-operate with law enforcement against the interests of customers who are not alleged to have broken any laws. The cardinal example of this remains the reaction of Anonymous to the cessation of payments by financial intermediaries to Wikileaks in response to the publication by Wikileaks of American diplomatic cables in 2010. In disrupting the websites of these intermediaries, Anonymous sent a message that these actors were violating norms of acceptable behaviour.

(c) Implications

The continuing exploits of Hacktivist groups will have significant ongoing implications for cyber security policy.

First, Hacktivism opposes the private half of public-private partnerships directed towards politically ambigous or controversial investigations or operations. Private actors acting as state agents invite attack. This may in turn compromise law enforcement or public safety strategies.

Second, public institutions may find themselves targets of Hacktivist attacks. While this it is common for government agencies to find theselves targets of security breach attempts, Hacktivist attacks are different in kind. They do not seek to remain quiet or undiscovered; quite

the reverse, Hacktivism seeks publicity. The point is not to go undetected, but to make news. To the extent that such attacks target public infrastructure, they raise additional public safety concerns.

Finally, individuals are now vulnerable to politically-motivated attacks. Such attacks need not violate any laws: scraping publicly available data off websites such as Facebook may violate no laws but still achieve the objectives of the Hactivist: to influence the future action of the target, and to influence public opinion on the target.

Issue #3: The Surveilled State

(a) Description

The coming decade will see Canadian law enforcement agents obtain unprecedented powers to surveill ordinary citizens and subjects both within and without their borders. This has been a devlopment long in coming: ever since Canada signed the Cybercrime Convenion, Canadian law enforcement agencies have sought expanded powers to investigate, gather evidence, and intercept digital communications. A number of previous attempts to modify Canadian laws governing law enforcement access to private information have failed to pass into law, due both to the controversial nature of those laws and the vagaries of Canadian electoral politics. With the current majority government's commitment to a "law and order" ideology, those barriers appear certain to be overcome in the near future.

Nor will that expanded surveillance agenda be satisfied with the passage of the current lawful access proposals. A second wave of expanded law enforcement powers will come with the obligations attached to further international instruments, most notably those implicated in current discussions involving the Perimeter Agreement with the United States. Finally, as discussed in the previous section, informal public-private partnerships are serving to greatly expand the state's reach into the personal information of Canadians in a manner completely outside the scope of legislation governing public surveillance powers.

Canada one decade from now will be a comprehensively serveilled state. Privacy will arise as a by-product of staying offline - increasingly difficult to do in a world in which even common household items are online - or by taking extra-ordinary steps to utilize privacy enhancing technologies to maintain privacy.

(b) Drivers

The drivers behind the emergence of the surveillance state are largely technological and normative, and enabled by the emergence of a marketplace able to navigate away from liability for privacy invasion.

From a technological perspective, the tools of widespread public surveillance are only recently evolved. It has simply been a question of storage, processing power, and network architecture. From a normative perspective, the tragedy of 9/11 has provided security agencies with motivation to push an unprecedented security agenda. It is clear, as American Secretary of State Hilary Clinton asserts, that security trumps the economy in a hierarchy of public policy

priorities; however, it is even clearer that security trumps privacy in any contest between the two. This agenda has been abetted by marketplace developments placing private actors - such as online service providers and network access merchants - as custodians of access to personal information of their customers. Those developments have placed these private actors in the perfect position to act as agents of the state in surveillance operations.

(c) Implications

The emergence of the surveillance state will have profound effects on civil liberties, dramatically weakening the rights individual citizens enjoy. This will potentially provide a series of crises.

First, expanded state powers of investigation will foreseably raise the potential for abuse of those powers. Civil libertarian challenges to the expansion of law enforcement powers call for checks, balances, and oversight in the use of these powers. The challenge for proponents of expanded state powers is to see the imposition of these checks and balances as necessary safeguards rather than meddlesome irritants to the use of those powers. This sets aside, of course, fundamental questions about the need for expanded state powers to begin with, or the question of whether these powers should aim for the outer limits of constitutional authority or more conservatively for standards already settled by law as well within constitutional limits.

Second, and more fundamentally, ubiquitous state surveillance may amount to a rechacterization of what it means to live in a liberal democracy. Traditionally, we have defined the difference between authoritarian states and Canada as comprising both liberty and democracy. We have long regarded privacy as inherent to liberty. Ubiquitous state surveillance challenges that regard. Is liberty no more than the freedom to shop under the watchful eye of the state? If so, is the only real difference between authoritarian regimes and Canada that Canadians elect their government? And if so, ubiquitous state surveillance promises a crisis of democracy itself.

Or is this concern simply alarmist? After all, Canadians only enjoy constitutional protection against unreasonable search and seizure by the Canadian government. We enjoy much more limited protections against the surveillance activities of foreign governments, including the United States. Online communications take no heed of borders. Indeed, emails from one part of Canada to another are liable, even likely, to be routed through borders to the United States and beyond.

Issue #4: The Hacktivist State

(a) Description

Mirroring Hactivism, state agents will enjoy aggressive new powers to investigate and disrupt threats to cyber security. States will begin enacting laws legitimizing the State's authorization of the kinds of tactics employed by Hacktivists against them, and going beyond, to disrupt the manner in which the internet itself facilitates communications with target sites. In its simplest form this may include state authorization of security firms to destroy botnets distributed on the personal computers of individuals. More complex remedies interfere with the functioning of the internet itself.

The internet has long been regarded by civil libertarians as inviolate: disrupt the bedstone principles upon which the internet was built and you will threaten the media's potential as a generator of innovation and economic growth. The next decade will see the creation of new law enforcement powers that challenge this assumption. States will start to enact laws that violate principles that the internet was built upon, such as the end-to-end principle, and disrupting the rules that govern internet addressing: why build a case against a target when the root can be re-written to elimate the target from the net entirely?

We can already see the earliest forms of these powers in, of all things, the advocacy of the American government in the service of the entertainment industry. First, the U.S. Immigration and Customs Enforcement agency ("ICE"), an agency of the United States Department of Homeland Security, has taken exceptional steps to address allegations of copyright infringement. On the basis of unproven allegations of infringement supported by untested evidence, ICE has seized domain names registered to third parties, replacing the internet sites with a notice of seizure.

This remedy is being touted as the centrepiece of legislation currently before Congress, the House bill, *Stop Online Piracy Act*, H.R. 3261, and its Senate counterpart, the *PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property) of 2011*, U.S. Senate Bill S.968. The remarkable nature of these remedies should be clear: they propose treatment of speech akin to that afforded in Canada to unambigous cases of online child pornography imagery. Globally, it is a remedy akin to the kind of consorship practiced in authoritarian regimes. If accepted in the context of intellectual property rights enforcement, we can expect the remedy to spread both to other areas of private rights - defamation, trade-mark infringement, etc. - and to areas of public concern, including security and law enforcement.

(b) Drivers

The phenomena of aggressive remedial action to security threats - and, apparently, to the merely commercial interests of intellectual property owners in the United States - is not based on the recent emergence of technology. The ability to seize domain names has long existed by not used. Rather, these seem based on market interests and the normative position of regulators supporting those commercial interests.

(c) Implications

The emergence of robust remedies for addressing security concerns - of both the informational integrity and economic variety - are significant.

First, state-sponsored Hacktivism runs the risk of provoking indeterminate liability. State actors - whether law enforcement or private actors acting as state agents - must be secure in the knowledge that their intervention is based on accurate information, targeted solely at bad actors, and will not harm innocent parties. Failure of any of these conditions may result in liability. Accordingly, there will be pressure brought for legislative "cover" for these kinds of activities. Advocates will demand that such laws ought to provide authorization of the remedy (extending

to any private parties acting as state agents), and that the laws provide immunity from prosecution or lawsuits within "safe harbours" of activity (a "responsible intervention" defense).

Second, more aggressive remedies involving domain name seizures will provoke a stronger reaction amongst civil libertarians and, potentially, others. At its root, domain seizures challenge the globe's trust and confidence in the United States as custodian of the internet. American authorities control "the root" - the domain name system that underlies all communications over the internet. Locally, national domains are potentially subject to the same sorts of remedies: the Canadian government could conceivably pass laws compelling CIRA, the Canadian Internet Registry Authority, to pull the plug on targeted domain names. To address these fears, states may take measures to protect national firms against the threat of irresponsible domain stewardship. This raises the spectre of a balkanized internet.

From an economic perspective, suspicion of governmental power over the internet may undermine trust and confidence in the internet as a vehicle of communications and commerce. This is turn may undermine innovation on the 'net. To the extent that cyber security policy promotes the economic potential of the internet for securing Canada's well-being, these dramatic new remedies pose as many potential problems as solutions.

Part III - Conclusions and Recommendations

Bibliography

Cameron, Bud

From: Cameron, Bud
Sent: January-05-12 10:00 AM
To: Hatfield, Adam
Subject: Stratfor Hack

The Anonymous collective hacked into a private intelligence company, Strategic Forecasting Inc. They have begun releasing private info of their clients' accounts with address, credit card, account passwords. The first batch released had [redacted] Being processed for notifications [redacted]
This batch is only about 5 percent of the total; another batch expected today.
Ccirc preparing a note to Robert for SA. [redacted]
Bud

Klassen, Nathan

From: Williston, Sandra
Sent: January-05-12 9:42 AM
To: Klassen, Nathan
Subject: RE: Briefing note for RD -- can you prepare a routing slip and file number

Hackers attack US security think tank Stratfor, promise more targets for Christmas
Associated Press (APR)
Cassandra Vinograd
Dec 25 08:04

LONDON _ Hackers on Sunday claimed to have stolen 200 GB of emails and credit card data from United States security think-tank Stratfor, promising a weeklong Christmas-inspired assault on a long list of targets.
Members of the loose hacking movement known as ``Anonymous'' posted a link on Twitter to what it said was Stratfor's secret client list _ including the U.S. Army, the U.S. Air Force, Goldman Sachs and MF Global.
``Not so private and secret anymore?,'' the group taunted in a message on the microblogging site.
Anonymous said it was able to get credit details, in part, because Stratfor didn't bother encrypting them _ an easy-to-avoid blunder which _ if true _ would be a major embarrassment for any security company.
Stratfor said in an email to members that it had suspended its servers and email after learning that its website had been hacked.
``We have reason to believe that the names of our corporate subscribers have been posted on other websites,'' said the email, passed on to The Associated Press. ``We are diligently investigating the extent to which subscriber information may have been obtained.''
The email, signed by Stratfor Chief Executive George Friedman, said the company is ``working closely with law enforcement to identify who is behind the breach.''
``Stratfor's relationship with its members and, in particular, the confidentiality of their subscriber information, are very important to Stratfor and me,'' Friedman wrote.
Stratfor's website was down midday Sunday, with a banner saying ``site is currently undergoing maintenance.''
Wishing everyone a ``Merry LulzXMas'' _ a reference to spinoff and fellow troublemakers Lulz Security _ Anonymous also posted a link on Twitter to a site containing the email, phone number and credit number of a U.S. Homeland Security employee.
The employee, Cody Sultenfuss, said he had no warning before his details were posted.
``They took money I did not have,'' he told The Associated Press in an email. ``I think why me? I am not rich.''
Anonymous warned it has ``enough targets lined up to extend the fun fun fun of LulzXmas through the entire next week.''
The group has previously claimed responsibility for attacks on companies such as Visa, MasterCard and PayPal, as well as others in the music industry and the Church of Scientology.

On December 25, 2011, the Anonymous group hacked into a private intelligence agency, Strategic Forecasting Inc. or STRATFOR, based in Austin, Texas.

The attack began with the release of STRATFOR's client list announced at https://twitter.com/#!/AnonymousIRC/status/150679351589998593 followed by release of accounts in batches believed to belong to STRATFOR's customers.

The release announced in another Twitter post at https://twitter.com/#!/AnonymousIRC/status/150985258999885824 includes emails, passwords (hashed with MD5), home/office addresses and credit card information (full 16-digit number, expiry date and CVV number).

STRATFOR has brought down their site following the attack but kept their members posted on the status of the attack via their Facebook page.

UPDATE (December 30, 2011): The Anonymous group has just released the remaining accounts making the total of leaked STRATFOR's accounts with credit card information to a total of approx. 75,000.

Additionally, login information for approx. 860,000 STRATFOR's registered users have been leaked as well but they don't include credit card information.

CCIRC is working with LE to identify Federal Government users who registered with the site. To date, 34 gc.ca users were identified and notified through CTEC (Federal Government CERT). Further analysis is being performed to identify and notify any Provincial, Municipal and Critical Infrastructure users who have been affected.

CCIRC's recommendation users should be advised to change the password of all other accounts, (business or personal on the Internet), that use elements from the compromised password.

Also, to contact their bank regarding the possible breach of their credit card and to monitor for any unusual transactions on the card.

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: Klassen, Nathan
Sent: January-05-12 9:32 AM
To: St-Louis, Danielle
Cc: Williston, Sandra
Subject: Briefing note for RD -- can you prepare a routing slip and file number

Hi Danielle,

Can you prepare a routing slip and file number WRT a brief Sandra and I are preparing for RD? Please ensure AH also gets a copy.

Title = **CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY**

RDIMS =541243

Cheers,

Nate

P.S. Since Bud is no longer here the routing slip will probably go from us to Windy.

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-05-12 8:44 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 5, 2012/ le 5 janvier 2012

Print Media

Government set to 'freeze' spammers
The federal government is preparing to launch a spam reporting centre (SRC) that will crack down on the illegal and annoying calls, texts and email messages that flood Canadians' cellphones, inboxes and social network accounts such as Facebook and Twitter. Private-sector bids closed this week on helping the government establish and operate a facility that observers say is desperately needed to meet international standards and eliminate Canada's reputation as a spammer haven. Industry Canada is developing a division that will be responsible for identifying and analysing trends in spam and related threats to electronic commerce. The government, which has allocated $700,000 annually to operate the facility, believes spam is an increasing threat to the Canadian economy because it can undermine consumer confidence in the online marketplace and erode productivity. Dubbed "The Freezer," the new centre will accept unsolicited electronic messages forwarded by individuals, businesses and organizations in Canada, including spam, malware (malicious software), spyware, short message services (SMS), and false and misleading representations involving the use of any means of telecommunications, says Industry Canada. Ottawa Citizen, A3 (Montreal Gazette, Windsor Star, Calgary Herald, Edmonton Journal, Vancouver Sun, National Post)

Better Business Bureau warns of top 10 scams
Even the Better Business Bureau isn't immune to its top 10 scams of 2011. The group, dedicated to keeping businesses honest, is itself the victim of "brand spoofing," on the Internet also known as "phishing," said president Lynda Pasacreta. Internet fraudsters send BBB clients emails mimicking its logo and directing them to click on a hyperlink to review a customer complaint. That allows the fraudsters access to the companies' confidential online data using spyware, she said. A similar brand-spoof scam masquerading as a Canada Revenue Agency notice of a refund landed in Dianne May-lor's email box Wednesday. It offered her an extra $410 from her revised 2011 tax return, as long as she clicked on a link. The Province, A4

Resolve to keep your computer virus-free
An opinion piece states, "Resolve to stay free of viruses and spyware - Every day, frustrated computer users call about slow systems that are bogged down with pop-up ads, re-directing them on the Internet, generating error messages or preventing booting up. The most common culprits are viruses and spyware or malware. Let me repeat my mantra: Install a free anti-virus and anti-spyware program such as Microsoft Security Essentials, and set it to automatically download and install updates. If you haven't done this yet, make a post-holiday gift of antivirus to your computer. While you're at it, resolve not to open email attachments from unknown senders - even if it most recently came from your sister. Don't click on pop-up ads (especially those professing that your computer is infected) or download programs or files from questionable sources. Trust me: The torrent site from which you're considering a download hasn't vetted the content to confirm that you'd really get a desired video or music file, free of viruses or spyware." Red Deer Advocate, B2

Online Media

Top 10 scams of 2012
The Better Business Bureau has released its list of the top 10 scams of 2012, warning scammers are capitalizing by using false pretences to con consumers. The list is developed jointly by the BBB, Consumer Protection B.C., and the B.C. Crime Prevention Association. CBC News

Cyber attack strands ETrade customers
AUSTRALIA'S second-biggest online broking business, ANZ Bank's ETrade, was forced to shut down over the Christmas-New Year period by a "malicious" cyber attack offshore. The shutdown was prompted by thousands of emails bombarding the broking site, in a denial-of-service attack. It is understood that, as risk assessments were performed on individual countries, access was restored. Access was unavailable from some countries for nearly two weeks. One frustrated customer emailed BusinessDay on December 31, saying that he was trying to prepare a tax return while in the US and Canada and still couldn't access his account. Sydney Morning Herald

Anonymous threatens Sony, spares customers
The loosely organized hacker group known as Anonymous has Sony in its sights once again. After releasing a video a few days ago wherein they threaten to destroy Sony's network, the group, which has been organizing in the IRC channel #OpSony, has clarified the meaning of their declaration. Unlike the infamous PlayStation Network hack of 2011, the target of this attack is not Sony's customers or even the Playstation Network itself, but Sony's executives. As a direct response to Sony's alignment with recent SOPA legislation, Anonymous intends to "dox" (find and expose personal information) about the company's executives. The group has already begun to publicize some private information (including credit card numbers) and plans to continue releasing more and more information in as public a way as possible in the near future. IT World Canada

Japan Fights Virus With Virus
The Japanese government is developing a computer virus to track down the source of a cyber-attack and neutralize it, underscoring the seriousness of the threat. According to a report from The Times of India, software company Fujitsu is reportedly developing the "electronic weapon," a process that has taken three years and $2.3 million, to combat Internet-based threats. The virus works by monitoring for attacks, identifying the source, and closing it down to prevent further programs. Forbes; Branchez-Vous; ZDNet; Huffington Post

Banking Trojans Cover Their Tracks
Virtually all modern viruses, Trojans, and other malware threats exist to make money for their creators. Botnet herders rent out their private armies of infected computers to spew spam. Android Trojans secretly send texts to premium numbers. Possibly the most lucrative, though, are banking Trojans. A banking Trojan like Zeus or SpyEye insinuates itself into the victim's browser and takes control of the online banking experience using what's called a "man in the browser" attack. Security giant Trusteer reports that in 2011 several banking Trojans developed a new type of attack specifically designed to postpone discovery as long as possible. After the actual theft, the Trojan manipulates the victim's view of online transactions, hiding the fraudulent activity. Those who haven't gone paperless will eventually receive evidence in the form of a mailed statement, but by hiding online evidence the criminals have bought extra time in which to complete transactions or siphon off additional funds. PC Magazine; InfoWorld

Sites knocked offline by OpenDNS freeze on Google
Innocent websites were blocked and labelled phishers on Wednesday following an apparent conflict between OpenDNS and Google's Content Delivery Network (CDN). OpenDNS - a popular domain name lookup service* - sparked the outage by blocking access to googleapis.com, Google's treasure trove of useful scripts and apps for web developers. According to reports, a flood of errors hit pages that used Google-hosted jQuery and hundreds of thousands of sites fell over. Visitors to websites were confronted with a message saying: "Phishing site blocked. Phishing is a fraudulent attempt to get you to provide personal information under false pretenses." Other visitors were greeted with a 404 error, aka the dreaded 'file not found' message. The Register

Spam Attacks on Twitter Massive during November 2011: Kaspersky
According to its most recent November 2011 monthly report, Kaspersky Labs states that spammers massively attacked Twitter.com the micro-blogging social networking site during November 2011. Thus, members of Twitter appeared to have hugely spammed invitations asking people to enroll themselves within the social network. Furthermore, Twitter.com was as well used for registering false notifications during November 2011 although in smaller amounts compared to 2010 summer that had an explosion of the said kind of notifications across the Net. Nevertheless, spammers find them popular even now: whenever the web-link is clicked, users get diverted onto a site serving one Viagra ad as well as malware. SPAM Fighter

APWG Reports Data Theft Program Propagation Surge of January-June 2011
The Anti-Phishing Working Group (APWG) recently issued its Phishing Activity Trends Report for H1-2011 i.e. first ½-year of 2011 according to which, certain crimeware's propagation rose during January-June 2011, with malicious programs, designed to steal data climbing to a new infection level as well as remaining stable thereof, so published Marketwatch.com in news on December 25, 2011. Specifically, during H1-2011, there was an over 45% rise in data-stealing programs as well as general PC Trojans from total malware spotted between January 2011 and April 2011. Thereafter, the increase leveled at much more than 40% during H2-2011 i.e. July-December 2011. Previously, the maximum increase in these malware programs was 44% during just one month i.e. August 2010. SPAM Fighter

Smart Grid Security Inadequate, Threats Abound
Near chaos. That's the current state of security for smart grids, according to Pike Research. A recent report by the research firm finds that a lack of security standards, a hodgepodge of products and increasingly aggressive malicious hackers will make 2012 a challenging year for securing smart grids. CIO

Government engineers actively plan for cyberwar
A decade ago, most viruses and worms were unleashed by curious students, pranksters and punks wanting to see what kind of damage they could inflict. That quickly evolved into criminals and thieves writing most of the malware once they realized money could be made. Now, governments have arrived for the party. State-sponsored cyberwar is an increasing concern as more and more nations arm themselves with cyber-weapons. CSO Online

Pentagon Solutions: NDU iCollege team talks Stuxnet, cyber threats
A team from the National Defense University's iCollege, which was recently honored by the the Defense Department's chief information officer for a special cybersecurity workshop, joined Pentagon Solutions. The event hosted more than 200 people from the Pentagon, international defense organizations, industry and academia. The workshop focused on identifying cyber threats, such as the Stuxnet worm, and responding to them. It also highlighted risks to the power grid and other critical infrastructure. Federal News Radio

Will We See More Relatives of Stuxnet in the Near Future?
When the Duqu Trojan made its appearance, many people in the security industry believed it was related to the Stuxnet Trojan. Now, after confirmation from Kaspersky Lab that the same team did, indeed, create both pieces of malware, the question is this: Will we see more Stuxnet relatives in the coming months? The answer is most likely yes. IT Business Edge

Smartphone hacking will rise in 2012, experts warn
Security experts predict 2012 will be a breakthrough year for cyber-attacks on smartphones. There are now enough of these mobile computers in use to make them an inviting target. "Shopping and mobile banking are things that are going to leave a trail and contain lots of goodies that criminals can go after," says Rachel Ratcliff Womack with the digital security firm Stroz Friedberg. MSNBC

Overlapping criminal and state threats pose growing cyber security threat to global Internet commerce, says Open Group speaker
This special BriefingsDirect thought leadership interview comes in conjunction with The Open Group Conference this January in San Francisco. The conference will focus on how IT and enterprise architecture support enterprise transformation. Speakers in conference events will also explore the latest in service oriented architecture (SOA), cloud computing, and security. We're here now with one of the main speakers, Joseph Menn, Cyber Security Correspondent for the Financial Times and author of Fatal System Error: The Hunt for the New Crime Lords Who are Bringing Down the Internet. ZDNet

A look ahead at healthcare law, privacy and security
Industry experts representing healthcare law, privacy, security, regulatory and data breach were asked to forecast healthcare data trends for 2012. The overall forecast? Protecting patients' protected health information (PHI) should be viewed as a patient safety issue. If the right actions are not taken, experts predict healthcare data breach will reach epidemic proportions this year. Help Net Security

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-03-12 8:27 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Allison, Catherine; Baker, William V.; 'Black, Dave'; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; 'Clarfield-Henry, Alexis'; Crépeault, David; 'CSIS Media Monitoring'; De Curtis, Laura; 'Dunn, John'; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; 'Gilbert, Monica'; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; Panthaky, Jasmine; 'Patry, Line'; Patton, Michael; 'RCMP Emerging Trends'; Roberts, Shane; Robinson, N.; 'Salas, Anik'; 'Slade, Nancy'; Spendlove, Jim; Stanfield, Charles; 'Stewart, Christena'; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; 'Wadasinghe, Cheryl'; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
January 3, 2012/ le 3 janvier 2012

Print Media

Software scam hits Windsor area - Police get hundreds of complaints
Canada's No. 1 fraud is a computer scam that has gone viral throughout Windsor-Essex. Windsor police Staff Sgt. Gerry Corriveau, with the financial crime unit, said he received hundreds of calls in 2011 from consumers who describe someone calling them claiming they are able to help protect their personal computers from viruses. One scenario involves a caller claiming they are from Microsoft or another reputable software company. Consumers say the scammers strongly suggest purchasing an antivirus repair service by credit card over the telephone. Windsor Star

Online Media

Amazon Shipment Spam Campaign Delivers Malware - If the recipient clicks on a link in the message, they're taken to a Web site serving Windows malware
A new spam campaign claiming to come from Amazon.com states that a smartphone is being shipped to the recipient, in an attempt to spread malware. "Users who may be tempted to click on the links contained in the message are taken to a website that serves a piece of malware which relies on unpatched Windows vulnerabilities to drop its payload," writes Softpedia's Eduard Kovacs. "The malware in question is a variant of Cridex, especially designed to steal personal and financial information from the computer it lands on, reports Hoax Slayer," Kovacs writes. eSecurity Planet

Hackers hitting NGOs with backdoor attacks
Hackers may be targeting non-government organizations with a series of backdoor attacks, a computer security firm warned this week. Trend Micro said it has found evidence that Amnesty International (AI), whose UK website was attacked recently, is "not the only intended target for the attack. Based on our investigation, it seems that the initially reported affected organization is just one of the targets in this attack and that the attack itself is fashioned specifically for the targets," it said in a blog post. It cited earlier reports the attack on AI's website involved an iframe that redirected users to another compromised site in Brazil. GMA News

Indian cyberspace hit by Kim Jong-Il malware mails: IT sleuths
Indian computer security analysts have detected and alerted internet users against "malicious spam mails" in the name of the dead North Korean leader Kim Jong-Il leading to hacking and crashing of vulnerable e-mails. The Indian Computer Emergency Response Team (CERT-In), country's national agency to respond to computer security incidents, has found the malware virus streaming into the Indian cyberspace. IBN Live

Saudi hackers publish Israeli credit card numbers on the Internet

Israelis won't be in a hurry to cyber shop this week, as thousands woke up horrified Tuesday to find their credit card numbers along with their personal details published online. Overnight, Saudi hackers named Group-XP claimed they broke into a leading Israeli sports site, redirecting surfers to a page where they could download a file containing the sensitive information. The hackers claimed they published valid and current personal and credit card information belonging to nearly half a million Israelis. Credit companies pored over the lists throughout the night and cite a much lower number. According to the Bank of Israel, the number of compromised cards is approximately 15,000. Los Angeles Times

Stuxnet possède au moins quatre frères et sœurs
Stuxnet n'est pas seul. Le virus qui a détérioré des installations nucléaires en Iran, appartient en effet à une famille comptant au moins cinq cyber-armes nuisibles sorties de la même plate-forme de développement. Voilà ce qu'affirme le spécialiste russe de la sécurité Kaspersky Lab. Les experts en cyber-sécurité affirment depuis assez longtemps déjà que les Etats-Unis et Israël sont à l'origine de Stuxnet, mais ces deux pays ne veulent donner aucun commentaire en la matière. Plus tôt cette semaine, le Pentagon (le siège du ministère américain de la défense) a refusé aussi de réagir à l'enquête menée par Kasperksy. Le Vif

Operation AntiSec publishes full client list obtained in Stratfor hack
A hacker operation founded to expose and punish governmental corruption and slimy big business tactics lived up to its word last week, releasing what it claims is a full list of clients who have patronized cyber security advisement firm Stratfor. AntiSec, a global collaboration between Anonymous and upstart hacker group LulzSec, previously released a sliver of data one day after Christmas: 30,000 pieces of personal information for Stratfor customers, including credit card information. Days later, the hacktivists released the whole enchilada. MYCE.com

Japan developing ethical virus in war against cyber crime
Fujitsu is developing a 'seek and destroy' virus for the Japanese government, one that it hopes will identify and combat cyber attacks. This brings new meaning to the phrase – the best defence is a good offence. According to a report by Yomiuri Shimbun, countries such as the U.S. and China have already put similar countermeasures in place. Japan has faced a tough time in online security in the recent past, with numerous cyber attacks in 2011 that crippled everything from local government portals, to the parliament, and Japanese embassies and consulates across the world. The three-year $2.3 million project is still ongoing, and for now, the virus is still in closed environment testing stages. Relevantly, the country would have to make amendments to its laws to allow for the manufacture of the ethical virus, with all virus development still an illegal activity. Think Digit

TDS Enables Koobface Botnet to Earn Bigger Profit
The Koobface botnet, popularly known for using pay-per install and pay-per click mechanisms yearning huge amount for its masterminds has recently been upgraded with a classy traffic direction system (TDS). The TDS controls all the traffic that are related to affiliated websites, reports security researchers at security firm, Trend Micro. The TDS feature forwards the traffic into various other locations and proves to be helpful in gaining hefty amount for the crooks through access into specific sites. With Google going stricter with their creation of botnets that combats creation of fake e-mail accounts by spammers, cyber criminals are taking privilege of Yahoo mail for the accomplishment of their task. SPAMFighter News

Dvorkin, Corey

From: Dvorkin, Corey
Sent: January-03-12 8:25 AM
To: Anderson, Ian; Grigsby, Alexandre; Bradley, Kees; Mohammed, Melanie
Cc: Bonvie, Jeff
Subject: Predictions!

On Dec. 27th, 2011, Rachel King wrote for ZDNet on cybersecurity company McAfee's cyber predictions for 2012. Here are a few of McAfee's predictions:

- There will be an increase in targeted cyberattacks as opposed to general spam e-mails. In this sense, cybercriminals will migrate from broad attempts at ensnaring computer users to targeted "phising" e-mails.

- Hackers will increasingly target mobile devices.

- Cyber-criminals will increasingly target utility systems and use that information to blackmail operators.

- We'll see a proliferation in fake security certificates.

- New hacktivist groups will be created. Interestingly, McAfee feels that the hacker group Anonymous will either disband or reorganize in 2012.

There are many more predictions, and more in-depth analysis. The McAfee predicition report can be found here.

Corey Michael Dvorkin
Acting Director / Directeur par intérim
Cyber Policy / Politiques cyber
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 OP8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: January-02-12 8:49 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
January 2, 2012 / le 2 janvier 2012

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

Un cas humain de H5N1 recensé en Chine

Un possible cas humain de grippe aviaire H5N1 a été recensé à Shenzhen dans le sud de la Chine, ont annoncé les autorités sanitaires locales. La ville borde Hong Kong où la présence du virus a été confirmée chez deux oiseaux la semaine dernière. Un chauffeur de bus de 39 ans, hospitalisé le 21 décembre avec de la fièvre, a été testé positif vendredi au virus H5N1, selon un communiqué diffusé sur les sites Internet des autorités sanitaires de la ville de Shenzhen et la province du Guangdong. Les experts de la province pensent qu'il a bien été contaminé par le virus de la grippe aviaire et ont signalé le cas au ministère chinois de la Santé pour qu'il confirme le diagnostic. L'Organisation mondiale de la santé a été prévenue par le ministère, selon le communiqué. Le Quotidien, 54

Avalanche victim identified

RCMP have identified the 45-year-old man who died in an avalanche while on a heli-skiing tour near Revelstoke, in southeast B.C. Police say the victim is Ronald Gregory Sheardown, a former Canadian from Stouffville, Ont., who had been living in Dubai. Sheardown was among a group of 11 people and a guide with Canadian Mountain Holidays when the snowslide came crashing down on some of them Friday afternoon. Three people managed to dig themselves out, but Sheardown was pulled out unresponsive after being located via the signal from his personal avalanche transceiver. Red Deer Advocate, A6; Toronto Star; Vancouver Province; Globe and Mail

CYBER SECURITY / CYBERSÉCURITÉ

Academics hack web activists

If the word "hacker" brings to mind a social outcast eating junk food in his mom's basement, you are probably underestimating the power of "hacktivism," or online activism. Academics have been studying for years the very non-academic undertakings of hacktivists - especially the group Anonymous. These include the repeated hacking of the Church of Scientology's Web site, the infamous online message board 4Chan and the philosophy of "doing it for the lulz." Their findings, while not your average classroom fare, are helping to paint a picture of a leaderless, geographically and socioeconomically diverse and powerfully disruptive group. New Brunswick Telegraph-Journal, B3

LAW ENFORCEMENT AND POLICING BRANCH / SECTEUR DE LA POLICE ET DE L'APPLICATION DE LA LOI

Murders at 25-year low - After 4 years of declines, city records 45 homicides, lowest number since 1986

Toronto has closed the book on 2011 with the lowest homicide total in a quarter century. The city recorded 45 homicides, the lowest number since 1986, when there were 37 murders. In 2010, there were 61 homicides. This is also the fourth straight year of declines since 2007, when the city recorded its deadliest year (matched in 1991) with 86 homicides. The plunge in Toronto's homicide numbers no doubt bolsters Chief Bill Blair's image. Blair's image took a hit in 2010 following the mass arrests during the meeting of G20 leaders and the controversy that followed. Regarding the homicide rate, Blair says there's still more work to do. "I think we can make this city safer," the chief told the Star. The chief attributed some of the decline in 2011 to the disruption of gang activity following sweeping raids carried out across the city and region. Toronto Star, GT1

RCMP officer sues over exploding doll - Twisted prank hurt hands, he claims

A Mountie has filed suit against two fellow officers in the bomb-squad unit, the RCMP and the province of B.C. after a mechanical doll he kept at his desk was rigged to explode, disfiguring him to the point of requiring hand surgery and hearing aids in both ears. Cpl. Tyrone Hempston suffered "severe injuries" after returning from Christmas holidays to his desk at the Explosive Disposal Unit in Delta on Jan. 4, 2010, where he noticed some-one had tampered with his Dirty Bertie mechanical doll. "He sat down and picked up the doll, held it in both hands close to his lap, then switched it on and it exploded in his hands," according to the writ filed in Vancouver Supreme Court of B.C. Vancouver Province, A4

Latest Hobbema homicide sparks call for new programs
Hobbema cops urge better anti-domestic violence programs after a slaying on the troubled reserve Saturday. "We want to get a handle on domestic violence," said RCMP Const. Perry Cardinal. "We want to bring in different programming -- like something that can (align) our domestic violence unit, the women's shelter and the victim services centre to clean all of this up." Mounties were called to a Samson Cree Nation home some time around 7:40 p.m. on New Year's Eve where they found a 34-year-old man with multiple stab wounds. Calgary Sun, 7 (Edmonton Sun); Edmonton Journal (Windsor Star); Red Deer Advocate

Cops to probe man's death
The Vancouver Police Department Major Crime Homicide Squad will investigate the death Friday of a man in custody of the Surrey RCMP. A 58-year-old male arrested Dec. 23 for breaching a court order was found lying on his cell floor Dec. 26. He was taken to hospital and died Friday. Vancouver Province, A4

Accident sends officers, driver to hospital
A pair of RCMP constables are feeling lucky to see the new year arrive after an allegedly speeding driver crashed his van into the officers' parked cruiser near Terrace, B.C., sending all three to a nearby hospital. David Schiffer, a 35-year-old Czech national working in Terrace, was driving on Highway 16 near Ferry Island late Friday night when Constable Philip Crack and Auxiliary Constable Shelley Ullery clocked his white van travelling more than 120 kilometres an hour in a 50 km/h zone. The officers say he hit the brakes but lost control, and seconds later the van careened sideways into the back of the police car they were sitting in. Both constables and Mr. Schiffer were taken by ambulance to Mills Memorial Hospital and later released, and though the extent of their wounds has not been divulged, the RCMP considers them fortunate. Globe and Mail, S1

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

How they screen the screeners - Airport guards who flunk tests for finding bombs through X-rays face suspension of screening credentials, not loss of employment
The continuing threat of aviation terrorism means guards are gauged on their ability to pick out improvised explosive devices (or IEDs) from carry-on luggage. Records show they are also tested on their ability to spot hidden guns, knives, grenades in carry-on bags - and even martial-arts weapons, such as the deadly metal throwing stars associated with Japanese ninjas. Dending a guard home for good is no easy thing in Canada. Despite failed tests, a guard could be back at work within a few weeks. His poor tests resulted in the suspension of his screening credentials, not in his being fired. Globe and Mail, A5

Border staff, police clash - No-arms rule spat rekindled
A dirty-bomb alert involving armed Montreal customs agents has re-ignited a bitter dispute over whether Canada's border services personnel should be allowed to take part in joint operations with other law enforcement agencies. Almost a year after the Canada Border Services Agency's Ottawa hierarchy halted joint operations with police forces across the country, the Ottawa Citizen has learned that Montreal agency managers twice refused to join a multi-force anti-terrorism search earlier last month after intelligence reports indicated cyanide and other dirty-bomb materials were stashed in a trailer at a Montreal storage yard. Local CBSA managers declined the request from leaders of the joint armed forces, RCMP and Quebec provincial and Montreal city police emergency force for fear of contravening their bosses' "no co-operation" edict laid down last December. Windsor Star, B1 (Ottawa Citizen, Vancouver Sun)

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Bill C-10 will target gangs not teens, minister says - Federal crime bill
Canadian jail cells are not going to be filled with teenagers and college students who share marijuana with friends, according to Justice Minister Rob Nicholson, who says his crime bill has been grossly misrepresented. In a year-end interview with Postmedia News, he said mandatory minimum sentences for marijuana production are designed to target

organized crime, gangs and grow-ops. They don't apply to youths -- and even new provisions that aim to penalize adults who are trafficking drugs around schools mean perpetrators would have to be caught with an "eight-pound joint" to be saddled with a mandatory minimum under the safe streets and communities act, he argued. The omnibus crime bill, which bundled nine different bills into one, Bill C-10, is poised to pass in early 2012. National Post, A5

Hijabs don't hinder prison guards
An editorial states "Last week, Quebec moved to allow Muslim women prison guards to wear hijabs on the job, but it only did so as part of a settlement of a human rights complaint filed four years ago. However, the decision will hopefully pave the way for other Muslim women interested in correctional careers, in Quebec and in the rest of Canada. Accommodating the hijab as part of a guard's uniform is no different than allowing Sikh RCMP officers to wear their turbans instead of the regulation hats. Turbans have never interfered with the ability of a Mountie to do his job, and it will be the same for the hijab, as long as women guards wear head scarves with Velcro fastenings that allow for quick removal in an emergency. Unlike burkas and niqabs, the hijab does not obscure the face. The line in the sand should be drawn at hijabs - they are as far as government should go in permitting religious or cultural head coverings among female guards." Calgary Herald, A8

PUBLIC SERVICE / FONCTION PUBLIQUE

PS job fears grow as cuts draw closer - 'Everything points to bleak times'
An axe hangs over federal government departments and public servants and where it falls finally should be known within weeks. The government is finalizing decisions on a sweeping operating spending review to chop billions of dollars annually from the federal budget. It has unions fearing that potentially, tens of thousands of federal employees could receive pink slips. Treasury Board President Tony Clement is leading the strategic review that is searching for $1 billion in cuts in the upcoming 2012-13 spring budget, $2 billion for 2013-14, and $4 billion annually by 2014-15 and beyond. Nearly 70 government departments and agencies have submitted scenarios for a five- and 10-per-cent cut to their budgets as part of an examination of about $80 billion in direct program spending. More than 600 proposals are being considered. The government needs the savings to help eliminate a $31-billion deficit by 2015-16, at the earliest. Ottawa Citizen, A3 (Vancouver Province, Fredericton Daily Gleaner)

INTERNATIONAL / INTERNATIONAL

Canadian role in peace relations questioned - Efforts fail to end Afghan-Pakistani border bickering
Canada's contribution to Afghan-Pakistan peace is being questioned after a recent investigation found distrust and long-standing disputes were at the root of a cross-border air-strike that killed 24 Pakistani soldiers in November. The joint U.S.-NATO study recommends several actions to prevent another such incident -- actions Canada has been trying to undertake for four years, with mixed results. The investigators made seven recommendations. Since November 2007, Canada has taken the lead in facilitating dialogue and understanding between officials on either side of the heavily travelled but unsecure border. Initially labelled the Dubai Process, the effort has since been renamed the Afghanistan Pakistan Co-operation Process. The government has boasted some successes over the years, but there have also been indications the Canadian efforts have not addressed many of the underlying issues. Numerous U.S. diplomatic cables released through WikiLeaks showed Afghan and Pakistani officials bickering as often as not. National Post, A16

Olympic health workers get shot against bio-terrorism
Five hundred health workers have been vaccinated against smallpox to deal with any biological terror attack at this year's Olympics. The move highlights the level of concern over the prospect of extremists turning to germ warfare. Britain has also stockpiled sufficient smallpox vaccines to "mount a UK-wide vaccination program" in the event of a deliberate release of the disease, which was declared eradicated in 1980. A report last year warned Games venues or public transport would make an "appealing target" for terrorists to launch biological attacks. The deadly disease could be spread by aerosols and is highly contagious. Vancouver Sun, B4 (Ottawa Citizen)

California cracks down on global slave labour - Law forces firms to check supply chains
A new California law will force retailers and manufacturers to disclose how they guard against slavery and human trafficking throughout their supply chains, ratcheting up scrutiny of some of the largest U.S. corporations. Beginning today, about 3,200 major companies doing business or based in California, a list that includes Apple and Gap Inc., will be required to disclose steps they take, if any, to ensure their suppliers and partners do not use forced labour. Companies risk getting sued by the state attorney general if they flout that law. But experts say the real pressure will come from the court of public opinion: consumers who care about ethical working conditions and take an interest in how their favourite brands get made. Calgary Herald, B4

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-31-11 11:17 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
December 31, 2011 / le 31 octobre 2011

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

B.C. gov't confirms it will strike working group on Japanese tsunami debris
The B.C. government says it will begin working with national and municipal officials this January to prepare for the massive wave of debris heading to Pacific Northwest shores because of the March 11 earthquake and tsunami in Japan. Meanwhile, residents in the B.C. coastal community of Tofino are bracing themselves for the sad arrival of detritus from the devastating disaster, even while they debate amongst themselves whether the ruins have already started reaching the shore. Julianne McCaffrey, a spokeswoman for the Emergency Management B.C., part of the Ministry of Public Safety and Solicitor General, has confirmed the government is creating a Provincial Tsunami Debris Working Group. She said the arrival of the debris, which some experts have argued covers an area the size of California, has raised some "complex jurisdictional issues," which the working group will clarify, so officials hope to identify key members by Jan. 6. Whitehorse Daily Star, 27

Bird-flu research spurs fears of bioterrorism
The World Health Organization issued a stern warning Friday to scientists who have engineered a highly pathogenic form of the deadly H5N1 bird-flu virus, saying their work carries significant risks and must be tightly controlled. The United Nations health body said it was "deeply concerned about the potential negative consequences" of work by two leading fluresearch teams who this month said they had found ways to make H5N1 into an easily transmissible form capable of causing lethal human pandemics. The work by the teams, one in The Netherlands and one in the United States, has already prompted an unprecedented censorship call from U.S. security advisers who fear that publishing details of the research could give potential attackers the know-how to make a bioterrorism weapon. The U.S. National Science Advisory Board for Biosecurity has asked two journals that want to publish the work to make only redacted versions of the studies available, a request to which the journal editors and many scientists object. Calgary Herald, A12

Bus driver ill with bird flu virus
A 39-year-old bus driver is in critical condition after testing positive for the deadly H5N1 bird flu virus in Shenzhen, southern China, state media reported Saturday. National Post, A13

Vandals compound Slave Lake wildfire damage
Vandals are wrecking new homes under construction in Slave Lake. Sometime overnight on Dec. 29, two homes built to replace those lost in the May 15 wildfires were broken into, with damage to windows, doors and drywall. More than 400 homes were lost in the wildfire now blamed on arson. Some 80 homes have been restarted, McKale said. Edmonton Sun, 7

Avalanche claims veteran backcountry ski patroller
Duncan MacKenzie, an avid outdoorsman and long-time ski patroller, set off into British Columbia's backcountry with three other skiers for a pristine day on the slopes. By the day's end, he was sitting on a mountain with critical injuries suffered as he was carried nearly two kilometres down the slope in an avalanche, which struck late Thursday afternoon in a remote area near Pemberton. The Canadian Avalanche Centre has been warning that mild temperatures have created heightened risks throughout British Columbia. The centre's latest bulletin for the area put the risk at considerable at lower elevations and high in alpine areas. Vancouver Sun, A5; National Post; Calgary Sun; Chronicle-Herald; Le Quotidien

Good and bad among 2011's top public policy stories
It has been a year full of politics - maybe fuller than many Canadians would have preferred. But what were the public policy highlights of 2011? There were in fact numerous important decisions or initiatives that constitute potential "game changers" for our country. Here, in descending order, is the Public Policy Forum's Top 10 List of Canadian policy stories

of the year... The 'tough on crime' bill. In September, the Conservative government introduced a sweeping new law advancing several criminal justice initiatives such as new mandatory minimum sentences. With heated criticism from legal and corrections communities that the measures are unwarranted given falling crime rates, the federal government also faced opposition from some provinces expected to share the costs of prison expansion. 3. Provincial governments respond to natural disasters. Disastrous floods in Manitoba and Quebec and wildfires in Alberta and Ontario were managed during the summer months by provincial public services, sometimes aided by the Canadian military. The responses were prompt and in most cases very effective, vividly demonstrating the changing nature of public service delivery: dealing with the real needs of citizens on the ground and in the community. Vancouver Sun, C4

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Twitter and the #Taliban
An editorial states, "Moves by the U.S. Congress to censor Twitter and other social media used by the Taliban are understandable. The dissemination of the poisonous message espoused by the group is unwelcome, and, indeed, Taliban propaganda can harm efforts to stabilize Afghanistan. Even so, social media has proven time and again to be a friend of democracy movements. Unless matters of national security are being disclosed, the U.S. should resist the temptation to censor the Twitterverse... Senator Joe Lieberman, chair of the U.S. Senate's Homeland Security Committee, has turned to Twitter in hopes of removing terrorist organizations from it. Taliban tweeters have already amassed more than 10,000 followers on the microblogging network. Although these users have a twisted message, one that is at odds with U.S. and allied policy, Western governments should be very cautious about censoring 140-character updates on Twitter, for the simple reason that their example may be used by repressive regimes (in fact, like the Taliban, if they are ever returned to power) to themselves quash dissent." Globe and Mail, F8

CYBER SECURITY / CYBERSÉCURITÉ

Hackers post spy firms' email addresses
Hackers affiliated with the group Anonymous published hundreds of thousands of email addresses they claimed belong to subscribers of private intelligence analysis firm Strategic Forecasting Inc. The list, published late on Thursday, includes email addresses appearing to belong to people working for large corporations, the U.S. military and major defence contractors - information that hackers could potentially use to target them with virus-tainted emails in an approach known as "spear phishing." The Antisec faction of Anonymous last weekend disclosed that it had hacked into the firm, which is widely known as Stratfor and is also dubbed a "shadow CIA" because it gathers open-source intelligence on international crises. The Pentagon said it saw no threat so far. Windsor Star, A13

LAW ENFORCEMENT AND POLICING BRANCH / SECTEUR DE LA POLICE ET DE L'APPLICATION DE LA LOI

Mountie sues officers over exploding mechanical doll
An RCMP officer has filed a lawsuit against two fellow officers in the bomb-squad unit, the RCMP and the province of B.C. after a mechanical doll he kept at his desk was rigged to explode, which disfigured him to the point of requiring hand surgery and hearing aids in both ears. Cpl. Tyrone Hempston suffered "severe injuries" after returning from Christmas holidays to his desk at the Explosive Disposal Unit in Delta on Jan. 4, 2010, where he noticed someone had tampered with his "Dirty Bertie" mechanical doll. Hempston's lawsuit alleges Cpl. Nigel Blake and Const. Martin Simpson "conspired to shock" him by placing a "high explosive" SD-100 detonator that had been confiscated from a U.S. film company trying to bring them into Canada and turned over to the EDU for disposal. Both the defendants Blake and Simpson knew or ought to have known - an SD-100 - (is) a dangerous explosive that should not be used for recreation and that their actions were in violation of the unit's zero horseplay policy," the writ stated. The lawsuit includes the federal attorney general, who is responsible for the RCMP, and the provincial solicitor general under whom the RCMP is contracted to the province. Edmonton Journal, A14

RCMP to question Vancouver mayor
RCMP plan to speak with Vancouver Mayor Gregor Robertson after his 21-year-old former foster son was charged with drug trafficking and weapons offences. Mounties held a news conference Friday to formally announce charges against Jinagh Navas-Rivas and four other men. Police allege the group was running a "dial-a-dope" cocaine business. Mr. Robertson is on vacation in Hawaii but RCMP spokesman Sergeant Peter Thiessen said police will speak with him soon. Mr. Navas-Rivas is not in custody and hasn't been seen since the charges were laid. Globe and Mail, A5; Vancouver Sun; The Guardian

Fake 911 call ties up N.B. RCMP for six hours
Mounties in New Brunswick say they spent six hours Thursday searching for a teen they believed was injured in the woods, only to find he was fine and dandy. London Free Press, B3

Nine charged in trafficking case
An undercover police investigation into cocaine trafficking in Red Deer has resulted in charges against nine people. Red Deer RCMP say a weeklong investigation targeted street-level drug traffickers in the central Alberta city's downtown, from Nov. 28 to Dec. 4. Warrants have been issued for four people. Calgary Herald, B2

Codiac RCMP target drunk drivers
There will be taxis and special late-night Codiac Transpo buses out on the roads of Metro Moncton this New Year's Eve. You should use them. There will also be plenty of Codiac Regional RCMP police cars cruising around the streets of Moncton, Dieppe and Riverview this weekend. If you're out and about, no question about it, you will see them around. Drunk-driving deaths are actually down in New Brunswick this year, thankfully, but the RCMP wants to be sure the year ends that way. Despite that happy statistic, another figure suggests the message on drinking and driving is still not getting out to some, even as laws and court rulings have gotten more strict. Times & Transcript, A11

Woman who struck, killed Quebec cop dies in crash
A woman who was killed in a car crash Tuesday southeast of Montreal is the same woman who struck and killed a former St. Albert Mountie with her car a few weeks earlier. Nancy Pichette was being investigated by police for the death of Vincent Roy, the police officer killed Dec. 1 in Bromont, Que., about 85 km southeast of Montreal. Roy, 37, was walking on the shoulder of a road towards a car he had stopped for a moving violation when Pichette hit him with her car. Roy, who had been working as a police officer in Quebec for four months before he was killed, had previously been a Canadian Forces reservist, an agent for the Canada Border Services Agency and an investigator for the RCMP in St. Albert. Edmonton Sun, 24

Scrap the registry, then its records
An editorial states, "In a recent letter to the editor of the Edmonton Journal - a fellow Postmedia paper - Claude Roberto, the secretary general of the Bureau of Canadian Archivists, objected to plans by the Tory government to destroy the information collected on individual gun owners by the federal longgun registry when the registry is closed next year. Mr. Roberto quoted from the Library and Archives of Canada Act and cited the United Nations' Declaration on Archives to justify his contention that the records belong to "society" and not to the government, so it is not up to the government to decide whether they should be destroyed quickly. We disagree. The inviolability of government records cannot trump the rights of individual, law-abiding citizens to protect their privacy from unwarranted government scrutiny." National Post, A14

The customer is always right
An editorial states, "To the surprise of many justice watchers, Mountie management in Alberta got a pass from the inquiry that examined the Mayerthorpe tragedy where four junior RCMP officers were slaughtered by the local lunatic. Amid allegations from within the ranks that RCMP brass had given James Roszko free rein in the small community (because it was easier than putting up with his constant complaints), the inquiry was satisfied with the forces performance -- boosting skeptical thought that inquiries are much more about showcasing a particular political position and much less about inquiring. The RCMP -- this time in B.C. -- was under fire (again) from the B.C. Civil Liberties Association when it was learned investigators were embarking on a so-called DNA sweep in an attempt to identify the killer of four Prince George women. While the BCCLA prattled on about the sky falling, investigators, who had been examining the files for months, continued their work that culminated in the arrest of a man who now faces charges in the four cases. The BCCLA had no comment. The role, if any, played by DNA is not yet clear." Winnipeg Free Press, I6

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Oppal's inquiry faces major hurdles and tight deadline
Missing Women Commissioner Wally Oppal faces a serious hurdle this new year: His inquiry is taking too long and the legal manoeuvring is threatening its credibility. When the former attorney general was appointed in September 2010 to determine what went wrong with the investigation and initial prosecution of serial killer Robert Pickton, the provincial government wanted a report by the end of 2011. That was overly ambitious. Oppal was granted a six month extension by Victoria but after roughly two months of public hearings even he is exasperated. During the holiday break, one would hope, Oppal's staff was searching for a much-needed solution to this unseemly stasis. Oppal must wrest control of the proceedings back from the lawyers with their oath-driven, court-nurtured bad habits. Vancouver Sun, A8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Man linked to genocide faces deportation
Almost eight years after the Supreme Court of Canada unanimously ruled that he is inadmissible to stay in Canada because he helped incite the Rwandan genocide, Léon Mugesera could finally face deportation to his homeland on Jan. 12. But the Quebec City resident, who has been fighting expulsion from Canada since 1995 and has been in legal limbo since the 2005 Supreme Court decision, is circulating an email to drum up support from friends - and he has hired a lawyer to launch more legal action. He hired lawyer Johanne Doyon to attempt to quash the latest decision, but in the meantime was told by the Canada Border Services Agency, which carries out expulsions, that his deportation is imminent. The Canada Border Services Agency would not comment specifically on Mugesera's case, but said the government is committed to ensuring those involved in crimes against humanity are not given safe haven in Canada. Montreal Gazette, A4; Montreal Gazette

Deported teen still lives in fear
This week, the Star is catching up with some of the fascinating people we've covered. Today: Daniel Garcia, a student deported to Mexico. From the start, Daniel Garcia's story was all about "where" - where he could stay, where he felt at home, where he would be safe. Last December, the Toronto high school student made headlines when he was unexpectedly arrested and sent to a Canada Border Services Agency detention centre. His application for refugee status had been denied, and Garcia, then 18, was to be deported to his native Mexico on New Year's Day. The fear for Garcia and his network of friends and advocates was that the homophobic thugs who shot and killed his lesbian sister's partner were waiting to kill him, too. One year since their controversial deportations, both Garcia and his sister are safe, says Sayed Hussan, a friend of Garcia and member of No One Is Illegal. Brenda has gone into hiding, and Daniel has been constantly on the move. Hussan doesn't know where either sibling currently lives in Mexico. Toronto Star, GT10

American fugitive apprehended in Winnipeg
An American fugitive who may have tried to fake his own death after pleading guilty to defrauding an insurance company of $7 million was nabbed with the help of a sharp-eyed employee at a pharmacy here. Police allege Travis Magdalena Scott had been on the run for months and was trying to start a new life in Canada, Winnipeg police said Friday. In May, Scott pleaded guilty in U.S. federal court to one count of wire fraud and one count of money laundering after defrauding an insurance company of at least $7 million by submitting false claims, the FBI says in a news release on its website. Winnipeg Sun, 6; Winnipeg Free Press

Gang admits 'smuggling'
Alleged Chinese smuggling kingpin Lai Changxing, who Canada deported after a 12-year legal battle, has "confessed" and is being handed over to prosecutors, state-run media said Friday. Lai, who was extradited in July after China promised he would not be executed, was handed over for prosecution in the southeastern city of Xiamen after investigation of his case closed, the Xinhua news agency said. Lai is accused of running a Fujian smuggling ring that moved contraband estimated to be worth up to $10 billion, in what state media has said could prove the largest economic crime since 1949. StarPhoenix, C9; Vancouver Sun; Ottawa Citizen

COMMUNITY SAFETY AND PARTNERSHIPS / SECURITE DE LA POPULATION ET PARTENARIATS

Nicholson braces for wrath over controversial crime bill
Canadian jail cells are not going to be brimming with teenagers and college kids who share pot with their pals, according to Justice Minister Rob Nicholson, who maintains one of the most contentious facets of his omnibus crime bill has been grossly misrepresented. Mandatory minimum sentences for marijuana production are designed to target organized crime, gangs and grow-ops, he said in a yearend interview with Postmedia News. They don't apply to young offenders and even new provisions that aim to penalize adults who are trafficking drugs around schools mean perpetrators would have to be caught with an "eight-pound joint" to be saddled with a mandatory minimum under the Safe Streets and Communities Act, he argued. In January, Nicholson will meet with his provincial counterparts in what will undoubtedly be a difficult session. Ottawa Citizen, A3 (Montreal Gazette, Telegraph-Journal, Daily Gleaner, Times & Transcript, Winnipeg Free Press, Edmonton Journal)

'Afghanistan' of the North
While the world was distracted by Attawapiskat, another desperate cry for help was getting little notice in remote northern Ontario, where addiction to the prescription drug OxyContin is devastating reserves. Although the federal government is well aware of the spiralling drug crisis in the North - it provides health care on reserves - First Nations officials from

northwestern Ontario say they can't understand why, at a time when the government is being accused of ignoring the plight of people on reserves like Attawapiskat, it is not only providing inadequate resources to cope with the drug problem, but is throwing roadblocks in the way of treatment that could be a low-cost, effective solution. In places like Eabametoong First Nation, sometimes known as Fort Hope, 350 kilometres north of Thunder Bay, as many as 75 per cent of adults in the community of 1,200 are addicted to the prescription painkillers, including pregnant women and, more worrisome, their newborn babies. It is a similar story at many of the small reserve communities throughout northern Ontario. Ottawa Citizen, A1

Certain beats severe justice
An opinion piece states, "The Harper government is committed to spending billions of dollars on prisons in order to crack down on crime. Those who oppose this approach are called soft on crime and accused of not standing up for victims, and the ensuing debate typically falls along party lines. Partisan politics aside, however, evidence shows a prison-focused approach will do little to either reduce the number of victims or to help them deal with the consequences of their victimization. But there are measures that are effective -- and positive examples we can follow. Many criminologists would agree the Conservatives have some things right. First, Canada does have too much crime. Far too many Canadians are victimized and the Department of Justice has recently estimated that the annual cost of crime is $100 billion. Second, victims are not well-treated in Canada. Little is spent on victims and there have only been marginal improvements in this over the last several years, no matter the party in power. Despite their rhetoric, the Conservatives are investing only token amounts in actually improving services for victims. Cracking down on crime through increasing penalties and implementing mandatory minimum sentences does little or nothing to reduce crime or make Canada safer." Winnipeg Free Press, I1

INTERNATIONAL / INTERNATIONAL

U.S. hopes Taliban talks can resume in spring
The Obama administration hopes to restore momentum in the spring to U.S. talks with the Taliban insurgency that had reached a critical point before falling apart this month because of objections from Afghan President Hamid Karzai, U.S. and Afghan officials said. One goal of renewed talks with the insurgents would be to identify cease-fire zones that could be used as a steppingstone toward a full peace agreement that stops most fighting, a senior administration official told The Associated Press. It is a goal that so far has remained far out of reach. Chronicle-Herald, B2

Britain's growing trouble with terror alerts
Britain has announced in advance it will raise its terrorism threat level during the London Olympics next summer, but that could be the last time the five-point scale is used. The reason? There is mounting evidence such systems are often misunderstood and do little to generate crucial tips about terror plots. Data obtained by The Associated Press under a Freedom of Information request show terror tips from the public have consistently fallen when alerts are raised and risen when the scale is lowered, confounding expectations that boosting threat levels promotes greater vigilance. Toronto Star, WD2

Bomb kills 8
A bomber remotely detonated an explosive-laden car outside the home of a Pakistani former minister, killing at least eight people and wounding 30, police officials in the city of Quetta, the provincial capital of Baluchistan, said on Friday. The car was parked outside the house of Naseer Mengal, a former minister of petroleum and natural resources, police officials said. Several militants exchanged fire with private security guards after the blast. Windsor Star, A13

Blast kills five at Nigerian mosque
At least five people were killed in a bomb explosion at a mosque in the northern Nigerian city of Maiduguri after Friday prayers, police sources said. Several more worshippers were wounded and the blast took place as people were leaving the mosque, police said. Maiduguri is the base of Boko Haram, the Islamist group that claimed responsibility for the Christmas Day attacks on churches in which 27 people died. Hamilton Spectator, A12

OTHER / AUTRE

Report on Pakistan attack highlights lack of trust
Canada's contribution to Afghan-Pakistan peace is being questioned after a recent investigation found distrust and long-standing disputes were at the root of a cross-border airstrike that killed 24 Pakistani soldiers in November. The joint U.S.-NATO study recommends a number of actions to be taken to prevent another such incident - actions Canada has been trying to undertake for four years, with mixed results. On the night of Nov. 25, 100 Afghan and 14 American soldiers were patrolling near the border when they came under fire. It was only after they had called in several airstrikes that they

realized the shooting was from Pakistani troops, 24 of whom had been killed. The U.S. military and NATO each launched investigations, the latter led by Canadian Brig.-Gen. Mike Jorgensen. Their joint findings, released on Dec. 22, blamed the U.S. military officials for failing to notify Pakistan of the operation beforehand, and criticized Pakistani officials for refusing to provide locations of border posts and checkpoints. Ottawa Citizen, A6

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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 2:32 PM
To: Bendelier, Kenneth
Subject: Critical: AntiSec: Anonymous Hackers Threaten 'Unholy Havok' with New Year's 'Project Mayhem'

Importance: High

Generated by your Alert Subscription on Folder:
- Anonymous
Source: ibtimes
Complete item: http://uk.ibtimes.com/articles/274510/20111230/antisec-anonymous-hackers-threaten-unholy-havok-new.htm

Description:
Following up its "LulzXmas" attack on security firm Stratfor, Anonymous has revealed its New Year's resolution promising a new "Project Mayhem" hacking rampage.

Reportedly set to begin on 31 December, Anonymous announced the new "Fight Club" themed project on Friday, via a statement on Pastebin. In its statement the collective promised to mount a series of cyber attacks on multiple law enforcement agencies.

"We call upon all allied battleships, all armies from darkness, to use and abuse these password lists and credit card information to wreak unholy havok upon the systems and personal email accounts of these rich and powerful oppressors. Kill, kitties, kill and burn them down... peacefully. XD XD" read Anonymous' statement.

Continuing: "On New Years Eve, there will be 'noise demonstrations' in front of jails and prisons all over the world to show solidarity with those incarcerated. On this date, we will be launching our contributions to project mayhem by attacking multiple law enforcement targets from coast to coast. That's right: once again we bout to ride on the po po. Problem, officer? umad?"

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 1:17 PM
To: Bendelier, Kenneth
Subject: Information: Report details extent of Anonymous hack on Stratfor

Generated by your Alert Subscription on Folder:
- Anonymous
Source: CNet
Complete item: http://news.cnet.com/8301-1009_3-57348995-83/report-details-extent-of-anonymous-hack-on-stratfor/

Description:
Now that the Yuletide fog has cleared, details are emerging about the extent of an Anonymous hack on security think tank Strategic Forecasting that was first reported Christmas Day and appears to have affected some 50,000 individuals.

Austin, Texas-based Strategic Forecasting, or Stratfor, disclosed over the weekend that its Web site, which remains down, was hacked and information about its corporate subscribers--who include the likes of the U.S. Army, U.S. Air Force, and Miami Police Department--was disclosed. AntiSec, an Anonymous-affiliated hacktivist group, quickly claimed responsibility and promised "mayhem" with plans to release even more documents.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 1:38 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous targets military-gear site in latest holiday hack

Generated by your Alert Subscription on Folder:
- Anonymous
Source: CNet
Complete item: http://news.cnet.com/8301-1009_3-57349976-83/anonymous-targets-military-gear-site-in-latest-holiday-hack/?part=rss&subj=news&tag=2547-1_3-0-20&tag=nl.e703

Description:
In what its calling another round of "LulzXmas festivities," an Anonymous-affiliated hacktivst group today is claiming yet another breach and posting of customer information.

On Christmas Day the target was security think tank Strategic Forecasting, or Stratfor. This time it was SpecialForces.com, a Web site that sells military gear.

"Continuing the week long celebration of wreaking utter havoc on global financial systems, militaries, and governments, we are announcing our next target: the online piggie supply store SpecialForces.com," the group wrote in a Pastebin posting today.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 12:14 PM
To: Bendelier, Kenneth
Subject: Important: Stratfor Delayed The Launch Of An Anonymous-Hacked Web Site

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://www.asnowtech.com/stratfor-delayed-the-launch-of-an-anonymous-hacked-web-site-2175696.html

Description:
Strategic Forecasting, the security think tank that took down its Web site after it was hacked by Anonymous over the Christmas weekend, will not relaunch the site for at least a week, as the firm recovers from the theft of thousands of credit card numbers and other personal information belonging to clients.

George Friedman, chief executive and founder of the Austin, Texas-based firm, said Wednesday on the for the security breach. To say we wish this hadnt happened is a massive understatement.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 12:07 PM
To: Bendelier, Kenneth
Subject: Important: In a controversial move, Anonymous hacks Stratfor for LulzXmas PUBLISHED

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://www.dailydot.com/news/anonymous-antisec-stratfor-hack/

Description:
As part of LulzXmas, a week-long AntiSec operation, Anonymous attacked the security think tank Stratfor on Christmas Eve. The hack included the release of a private client list and reportedly 2.7 million emails, as well as bank and credit card information of Stratfors employees and subscribers (approximately 4,000).

The attack, however, has prompted members of the hacktivist collective to speak out against the cyber-assault.

Weeks ago, Anonymous uploaded a vague video onto YouTube promising virtual mayhem dubbed LulzXmas, an operation which promised to end the year with various web security breaches. As reported by the Daily Dot, another collective in the organization then promised to give Santa a break this year by pledging to siphon $1 million from bank accounts held by the wealthy.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 9:43 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous: Message to SONY on SOPA

Generated by your Alert Subscription on Folder:
- Anonymous
Source: YouTube
Complete item: http://www.youtube.com/watch?v=WjOPXpd9PSU

Description:
Hello, SONY.
We are Anonymous.

It has come to the attention of the Anonymous activist community that you have chosen to stand by the Stop Online Piracy Act. This act will halt online businesses and restrict access to many sites for many users. Supporting SOPA is like trying to throw an entire company from off a bridge. Your support to the act is a signed death warrant to SONY Company and Associates. Therefore, yet again, we have decided to destroy your network. We will dismantle your phantom from the internet. Prepare to be extinguished. Justice will be swift, and it will be for the people, whether some like it or not. Sony, you have been warned.

To those doubting our powers. We've infiltrated the servers of Bank of America, The United States Department of Defense, The United Nations, and Lockheed Martin. In one day.

For their approval to SOPA, we have also declared that our fury be brought upon the following persons. Justin Bieber. Lady Gaga. Kim Kardashian. and Taylor Swift.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 9:32 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hacks Online Military Gear Store

Generated by your Alert Subscription on Folder:
- Anonymous
Source: CRN
Complete item: http://www.crn.com/news/security/232301113/anonymous-hacks-online-military-gear-store.htm;jsessionid=w05-m28wsJj3TjMectdgxw**.ecappj03

Description:
Hacker collective Anonymous, which claims to be on a weeklong holiday hacking spree, says it has stolen more than 20,000 credit cards and passwords from the Web site of Special Forces Gear, an online store for military gear. The group posted a statement on the online message board Pastebin Tuesday claiming it stole 14,000 passwords and 8,000 credit card numbers from the site a few months ago. Anonymous claims to have posted the data on the Web.

On Wednesday, Gardena, Calif.-based Special Forces Gear confirmed the hack, which occurred in August. Founder Dave Thomas, a retired lieutenant colonel who served in the Army Special Forces, said the passwords taken were more than a year old, and most of the credit card numbers were expired. "We don't have evidence of any credit card misuse at this time," Thomas said in an e-mail.

E-Secure-IT
https://www.e-secure-it.com

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-30-11 8:11 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
December 30, 2011 / le 30 décembre 2011

Online media

Now that's a bit rich: Chinese government protects ITS citizens against hackers - after series of high-profile Chinese attacks on West
The Chinese government is stepping up internet security for its own citizens this week after a series of leaks of personal data from social networking sites and 'phishing' attacks on bank accounts. The government announced it would work with 10 Chinese search engines - which already censor the internet under Chinese law - to ensure 'fake' banks appear lower in search rankings. Daily Mail UK

China to curb online phishing
China's ten major search engines have agreed to put banks' official homepages at the top of search results in a bid to curb cyber scams, authorities said. The move was jointly pushed by Ministry of Public Security, banking industry organizations and several commercial banks in response to growing public concerns over the safety of online accounts and transactions since 2010, a statement said. Economic Times

Hackers set to dump intel-analysis firm's emails
Security analysts are bracing for the release of millions of emails that computer hackers stole from a U.S. intelligence-analysis firm whose clients include federal agencies, large corporations and foreign countries. The emails could reveal sensitive material to foreign spy agencies and corporate rivals about Stratfor's clients, which include employees of the Pentagon, Bank of America and the Austrian armed forces, among others. Washington Times

A Tough Cyber Year
Its been an eventful 12 months in cyberspace, with some international headline grabbing events including the Stuxnet worm and hacking by the group Anonymous. In a number of cases, events have upended the conventional wisdom on cyberspace and have set in motion responses that will have a long term impact on cyberspace. The Diplomat

Small business defense against cybercrime
Small businesses can innocently expose themselves to cybercrime when an employee opens an email that appears to be from the CEO, not updating the anti-virus program or having a laptop lost or stolen. Eduard Goodman, Chief Privacy Officer for Identity Theft 911 has seen an increase in small businesses being targeted for cybercrime within the last five to seven years. Reuters

Confidence in cloud, cybersecurity key to growth
Cloud computing and cybersecurity are both hot, fast-growing markets. But faith in the cloud took a knock with outages at Amazon and elsewhere in 2011. And the hacking of targets from Sony to Hollywood star Scarlett Johansson, whose email was broken into, underlines the need for better security. Reuters

Six security forecasts for 2012
My crystal ball tells me that 2012 is a relatively predictable one. That's largely because we've experienced significant changes in the political, business and security landscapes, ones that are sufficient to inspire some form of predictable short term action. Amongst other things it means some interesting action items will percolate up the management agenda. Computer Weekly

Stuxnet, Duqu Date Back To 2007, Researcher Says
The origins of the dangerous Stuxnet computer virus that targeted Iran's nuclear power program last year could date back as far as 2007, according to new research. Stuxnet and the related Duqu virus discovered earlier this year share a similar architecture and may have been developed by the same team of developers--along with other pieces of malware--several years ago, according to a security researcher at Kapersky Lab. Information Week

Let's Terminate Malware in 2012
Antivirus research is a cat and mouse problem. Each time the virus writers develop a new technique to spread malware or steal private data, antivirus experts rush to build countermeasures. To actually defeat the malware coders, we need to get out of strictly reactive mode. That requires looking at the motivations that drive malware creators, not just at their actions. PC Magazine

Finding the Cleanup Crew After a Messy Hack Attack
In the film "Pulp Fiction," Harvey Keitel plays the Wolf, a fast-talking and meticulous man who is called in to deal with the aftermath of an accidental shooting. In the messy world of computer security breaches, Kevin Mandia is something like the Wolf. Mr. Mandia has spent his entire career cleaning up problems much like the recent breach at Stratfor, the security group based in Austin, Tex., that was hacked over the Christmas weekend. New York Times

The world wide web of deception
IT engineer Wang Youhua has become "extremely busy" these days, ever since reports of the hacking of some well-known websites surfaced in mid-December. Some of the registered members of these portals had their private information leaked. China Daily

Railways warned of hacker risk
Computers that control train networks have been exposed as being at risk of hacker attacks, according to a German security expert. Speaking at a security conference in Berlin, the expert said hackers could shut down railway switching systems by overloading them with traffic. Aljazeera

Anonymous Hacks SpecialForces.com, Posts Passwords and Credit Card Data
Members of the hacker collective Anonymous claim they have stolen about 14,000 user passwords and 8,000 credit card numbers from SpecialForces.com, a military and law enforcement equipment retailer. The data breach occurred several months ago, according to Anonymous, but the group only now decided to post the data online. The purloined password list had reportedly been posted online several weeks ago as well. PC World

IT Security Predictions for 2012
As Dilbert author Scott Adams once said, the great thing about predicting the future is that if you're right you can point back to your initial prediction and proclaim your genius, if you're wrong, most people wouldn't remember your predictions in the first place. So with that caveat in mind, here are some of the things I expect to see in the IT security news in the coming 12 months. Windows IT Pro

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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 5:35 AM
To: Bendelier, Kenneth
Subject: Critical: Heads-Up - Anonymous Operation Backdoor

Importance: High

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: YouTube
Complete item: http://www.youtube.com/watch?v=eCuvlVHt93E&feature=share

Description:
Greetings World,we are Anonymous.In the very near future "Anonymous" members will use their extensive hacking and social Engineering skills to enter the main system of a world wide Banking Organisation and attempt to "Walk Away" with a target of 50,000,000 corrupt US Dollars, or the equivalent in the chosen currrency,The funds will then be general population, in what will be the largest charitable cyber theft in history.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 3:05 AM
To: Bendelier, Kenneth
Subject: Critical: UPDATE - Second batch Stratfor Leaked Account details released by Anonymous

Importance: High

Generated by your Alert Subscription on Folder:
- Anonymous
Source: dazzlepod
Complete item: http://www.dazzlepod.com/stratfor/

Description:
UPDATE (December 30, 2011): The Anonymous group has just released the remaining accounts, i.e. first name starting from N to Z, making the total of leaked accounts with credit card information to a total of 73,162. The table below has been updated to include these accounts. Additionally, login information for 860,000 STRATFOR's registered users have been leaked as well but they don't include credit card information; we may update the table below to include all the 860,000 accounts later.

General background:

On December 25, 2011, the Anonymous group hacked into a private intelligence agency, Strategic Forecasting Inc. or STRATFOR, based in Austin, Texas. The attack began with the release of STRATFOR's client list announced at https://twitter.com/#!/AnonymousIRC/status/150679351589998593 followed by release of accounts in batches believed to belong to STRATFOR's customers.

The release announced in another Twitter post at https://twitter.com/#!/AnonymousIRC/status/150985258999885824 includes emails, passwords (hashed with MD5), home/office addresses and credit card information (full 16-digit number, expiry date and CVV number). The table below is the list of the leaked accounts with the passwords removed.

STRATFOR has brought down their site following the attack but kept their members posted on the status of the attack via their Facebook page.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-30-11 2:46 AM
To: Bendelier, Kenneth
Subject: Important: Hacking Group 'Anonymous' Takes First Step in 'Master Plan,' Vows to Strike Again

Generated by your Alert Subscription on Folder:
- Anonymous
Source: ABC News
Complete item: http://abcnews.go.com/US/hacking-group-anonymous-vows-hit/story?id=15234349#.TvkShVYlpI5

Description:
The global activist hacking group Anonymous claims to have obtained thousands of credit card numbers and personal information from the high-profile clients of a leading analytical intelligence company, all in the name of charity.

Up to $1 million was reportedly stolen from Stratfor, in Austin, Texas, a leading provider of military, economic and political analysis for clients that include Apple and the U.S. Air Force.

AntiSec plundered 200gb of their mails and more booty, read a tweet by @AnonymousIRC on Saturday.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 11:28 PM
To: Bendelier, Kenneth
Subject: Important: 13,000 More cc Details From STRATFOR Leaked By Anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
Source: cyberwar news
Complete item: http://www.cyberwarnews.info/2011/12/26/13000-more-cc-details-from-stratfor-leaked-by-anonymous/

Description:
Well i am sure you have heard it already, STRATFOR got hacked, shamed and now all its data is being slowly leaked online, if slowing what u call pretty much all within one day so far.

The latest dump has over 13,000 further credit card details from what STRATFOR says is its client subscription list for various services its provides.

Dump announced by YourAnonNews

Once again the leak has been dumped on wikisend and is in the format of a tar,gz with a text file that is 4+mb and contains all the account details.

The pastebin statement for LulzXmas part 2

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 10:53 PM
To: Bendelier, Kenneth
Subject: Important: Update: Anonymous Hacks SpecialForces.com, Posts Passwords and Credit Card Data

Generated by your Alert Subscription on Folder:
- Anonymous
Source: PC World
Complete item:
http://www.pcworld.com/article/247072/update_anonymous_hacks_specialforcescom_posts_passwords_and_credit_card_data.html

Description:
Members of the hacker collective Anonymous claim they have stolen about 14,000 user passwords and 8,000 credit card numbers from SpecialForces.com, a military and law enforcement equipment retailer. The data breach occurred several months ago, according to Anonymous, but the group only now decided to post the data online. The purloined password list had reportedly been posted online several weeks ago as well.

A Twitter account associated with Anonymous has posted a screenshot of an e-mail from SpecialForces.com dated Dec. 15 admitting to the data breach. The purported SpecialForces.com e-mail confirms that Anonymous obtained customer usernames, passwords, and possibly encrypted credit card information.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 1:58 PM
To: Bendelier, Kenneth
Subject: Important: Stratfor hacked by Anonymous Hackers for #AntiSec

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Hacker News
Complete item: http://thehackernews.com/2011/12/stratfor-hacked-by-anonymous-hackers.html

Description:
Stratfor who provides strategic intelligence on global business, economic, security and geopolitical affairs just now has been defaced by Anonymous Group of Hackers. Mirror of Hack is available here.

Private Clients List of Stratfor is also leaked on a Pastebin note. For all this clients have been exposed sensible information including credit cards (which supposedly have been used to make $1 million in donations), as well as over 200 GB of email correspondence. As a result of this incident the operation of Stratfors servers and email have been suspended.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 12:18 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous Operations re-ignite war on Sony for Sopa support

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Daily Attack
Complete item: http://thedailyattack.com/2011/12/29/anonymous-operations-re-ignite-war-on-sony-for-sopa-support/

Description:
Anonymous Operations re-ignite war on Sony for Sopa support

http://thedailyattack.com/2011/12/29/anonymous-operations-re-ignite-war-on-sony-for-sopa-support/

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 11:56 AM
To: Bendelier, Kenneth
Subject: Important: Occupy Wall Street plus Anonymous may equal city computer outages

Generated by your Alert Subscription on Folder:
- Government US
- Cyberwar / Cyber conflict / Cyber war
- Anonymous
Source: nextgov
Complete item: http://www.nextgov.com/nextgov/ng_20111228_8727.php?oref=topnews

Description:
Note to the Homeland Security Department: expect hackers to join forces with offline activists in 2012 for strikes on transportation computer systems and other critical networks. According to annual predictions released by security firm McAfee, anti-Wall Street demonstrators occupying parks in cities across the country and digital vigilantes associated with hacktivist group Anonymous may soon operate as "cyberoccupiers."

"Think about the effectiveness if you actually shut down transportation in the place that you're sitting in at," said Dave Marcus, security research director for McAfee Labs. "You actually take the step of taking their power offline."

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 11:28 AM
To: Bendelier, Kenneth
Subject: Information: Kuwait Government will suspend Twitter accounts of Anonymous Users

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Hacker News
Complete item: http://thehackernews.com/2011/12/kuwait-government-will-suspend-twitter.html

Description:
In Kuwait, the Ministry of Interior is in the process of enforcing a rule of their own on Twitter which prevents Kuwaiti users from using anonymous accounts. The ministry said in a press statement that such measure comes in order to preserve the rights of citizens and residents of people who were used to slander them and their families under fake names, saying that such is a crime punishable by law.

The statement went on to say that the move was meant to protect the rights of citizens and residents who have found themselves the subject of slander through statements made by these anonymous accounts, a crime punishable by law in the country, as it is in the UAE.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 8:15 AM
To: Bendelier, Kenneth
Subject: Important: Occupy Wall Street plus Anonymous may equal city computer outages

Generated by your Alert Subscription on Folder:
- Government US
- Cyberwar / Cyber conflict / Cyber war
- Anonymous
Source: nextgov
Complete item: http://www.nextgov.com/nextgov/ng_20111228_8727.php?oref=topnews

Description:
Note to the Homeland Security Department: expect hackers to join forces with offline activists in 2012 for strikes on transportation computer systems and other critical networks. According to annual predictions released by security firm McAfee, anti-Wall Street demonstrators occupying parks in cities across the country and digital vigilantes associated with hacktivist group Anonymous may soon operate as "cyberoccupiers."

"Think about the effectiveness if you actually shut down transportation in the place that you're sitting in at," said Dave Marcus, security research director for McAfee Labs. "You actually take the step of taking their power offline." For example, Anonymous this summer wanted to get back at the Bay Area Rapid Transit District for jamming passengers' cellphones amid demonstrations against BART police violence. The instigators could have made a bigger statement by crippling the railway's control system instead of doing what they did -- leaking the e-mail addresses of its riders and posting nude photos of its spokesman.

E-Secure-IT
https://www.e-secure-it.com

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-29-11 8:15 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
December 29, 2011 / le 29 décembre 2011

Online media

Occupy Wall Street Plus Anonymous May Equal City Computer Outages
Note to the Homeland Security Department: expect hackers to join forces with offline activists in 2012 for strikes on transportation computer systems and other critical networks. According to annual predictions released by security firm McAfee, anti-Wall Street demonstrators occupying parks in cities across the country and digital vigilantes associated with hacktivist group Anonymous may soon operate as "cyberoccupiers." National Journal

Lethal Stuxnet cyber weapon is 'just one of five' engineered in same lab - and three have not been released yet
Online security experts Kaspersky Labs say that three hi-tech cyber weapons of the sort that damaged Iran's Bushehr nuclear plant may have been crafted in the same laboratory - and not yet released. The viruses have never been seen 'in the wild' - and it's unclear whether they, like Stuxnet, would be built to cause failures at nuclear plants, or engineered for another purpose. Daily Mail UK

Stuxnet had five cousins
Russian computer security outfit Kaspersky Lab said that the Stuxnet virus that damaged Iran's nuclear programme was likely to be one of at least five cyber weapons developed on a single platform. The security boffins have tracked the development of the virus back to 2007. TechEye

Viewpoint: We must resist over-hyping security threats
2011 has been the year of cybersecurity awareness, with the headlines frequently featuring reports of serious cyber-attacks and references to "cyber-warfare". As a result, "cybersecurity" has gained much needed attention, allowing us to address some very real issues. BBC News

The year in security: Hacktivists, botnets and smartphones
Cyber criminals don't work to annual deadlines, but December nevertheless offers us a chance to look back at the past 12 months and identify the year's major themes and trends. As with most areas of tech, the things we're talking about this year in information security may seem familiar, but they are no less relevant. V3.co.uk

Cybersecurity insurance: What small businesses need to know
Sure, you can install anti-virus programs. You can even go a step further and encrypt your data and heavily protect your passwords. In fact, these are but a few of many steps business owners can take to prevent cybersecurity breaches and subsequent data theft. Washington Post

Cyber war, car malware among top tech threats: report

A security research firm predicted on Wednesday that cyber attacks involving governments, organizations and even cars will become major threats in 2012. The McAfee Lab's 2012 Threat Predictions report finds that attacks on virtual currency, mobile hacking and legal spam will make headlines next year. CTV News

Carmakers, U.S. worry about hacking of cars
Imagine this nightmarish possibility: al-Qaida terrorists remotely disabling the brakes on thousands of cars racing down a Bay Area freeway during the morning commute, leading to massive chaos, death and destruction. Implausible? Maybe not, some experts warn. San Jose Mercury News

Hacktivism, Targeted Attacks Dominate 2011 Security Trends
Targeted attacks, hacktivist campaigns and the rise of mobile malware were just a handful of security news that dominated 2011's headlines. The past year was a momentous one in many aspects for the security industry, with high profile cyber-attacks and data breaches, but also a year in which many of the incidents evoked a sense of d j vu amongst industry observers. CIO Insight

New Wave of Hacker Attacks Coming
All my buddy Mario wanted was a can of beans to have for lunch one day last month. What he got, though, was a big pain in the bank account, when it turned out that his ATM card may have been one of the thousands of credit and debit cards potentially comprised by a devilishly clever band of hackers in Northern California. CIO

Aggressive Phishing Attack Targets Military Personnel
The U.S. military received an unwanted present this Christmas holiday season in the form of an "aggressive" phishing attack that's been making the rounds of .mil email accounts, according to the Army. There are several attacks making the rounds, the most notable coming in the form of an email with the subject line "Deposit Posted" that appears to be from USAA, a financial services company that services members of the military as well as their families and veterans, according to an article on the U.S. Army's website. Information Week

The war on terabytes
THE financial industry has done such a good job of bringing itself to its knees over the past four years that it is easy to overlook the threats it faces from outside. High among them is electronic attack. In 2010 Symantec, a cybersecurity firm, estimated that three-quarters of all “phishing” attacks, in which people are deceived into surrendering private details such as account numbers, are aimed at the finance sector. Bob Greifeld, the boss of NASDAQ, has described his bourse as being under “literally constant attack”. The Economist

The next target for hackers: your car
Banking on smartphones and web-connected cars will provide fertile hunting ground for hackers in 2012, as cyber criminals follow consumers into an increasingly mobile world, a report by McAfee Inc. said Wednesday. Montreal Gazette

Major cyber security events of 2011
If 2010 was the Year of Vulnerability to cyber crime, then 2011 was the year hackers took advantage of that vulnerability. Below, we take a look back over the past 12 months at some of the defining moments in hacker history. Financial Post

Hackers to exploit new avenues of attack in 2012
Banking on smartphones and web-connected cars will provide fertile hunting ground for hackers in 2012, as cyber criminals follow consumers into an increasingly mobile world, a report by McAfee Inc. said Wednesday. Attacks against popular smartphone and tablet operating systems such as Google Inc.’s Android software have been rapidly accelerating in recent months. Financial Post

Homeland Security uncovered Anonymous attack on Public Advocate’s office
Homeland Security officials were among the first to discover that the Public Advocate's Office website was hacked over Christmas weekend. The federal Multi-State Information Sharing and Analysis Center notified the city's tech department about the cyberattack in which data about thousands of users was stolen. New York Daily News

Feature: Social networking security
Like its close relative BYO IT, social media was once seen as a consumerisation fad that IT departments could afford to ignore. But if 2011 has shown us anything, it is that Twitter, Facebook and LinkedIn are now viewed as essential business tools and not the productivity-sapping employee distractions they once were. Computerworld

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 7:54 AM
To: Bendelier, Kenneth
Subject: Information: Is Anonymous Friend or Foe?

Generated by your Alert Subscription on Folder: - Anonymous
Source: Various Sources
Complete item: http://theminaretonline.com/2011/11/30/article20480

Description:
When hearing of an organization that took down 40 child porn websites, was able to get sufficient information to take down the second most powerful drug cartel in Mexico and regularly works to reveal governmental and corporate corruption, it may be easy to assume that it is essentially good. This organization, referred to as Anonymous, does play the hero in certain cases, but they usually do so through illegal means. Unfortunately, there have been dozens of other operations carried out by Anonymous that were just as illegal, but far less righteous. It is difficult to know whether or not to be in favor of these vigilantes, as not all of their crimes are for the common good. I am generally in favor of Anonymous and their intentions, but many others are not.

Its a bit difficult to explain what Anonymous actually is. Anonymous is an international hacking group that originated in 2003 on the Internet, specifically the imageboard 4chan, as recognized by Luke Allnutt in his article on the Tangled Web. Its not exactly an official group because there arent set members, nor a leader. Their name was inspired by the Anonymous username that is shown when website visitors comment or post without specifying the originator of the content. As the anonymous posters became more numerous, the idea of Anonymous was formed for any and all anonymous Internet users as an unnamed collective. Any member of Anonymous must never reveal their identity. To become a member, it is as simple as concealing oneself whilst performing online activities.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 5:53 AM
To: Bendelier, Kenneth
Subject: Important: Swiss data hacked in 'Anonymous' attack

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Local
Complete item: http://www.thelocal.ch/national/20111228_2141.html

Description:
The department of Foreign Affairs, the Swiss army, private bank Julius Br and Nestl are among the victims of a hacking attack targeting US security firm Stratfor on Christmas Eve. Swiss German-language public radio DRS revealed on Tuesday that it had received access to a vast file containing the credit card details, phone numbers, passwords and private addresses of Swiss citizens working for companies which use Stratfors services.

The file, thousands of pages long, was one of the documents stolen by Anonymous, a hacking syndicate. In an online message posted on Sunday, Anonymous derided Stratfor for exposing their clients to the risk of theft by neglecting to encrypt identity data.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 5:44 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Affiliates Are Unhappy About the 'Robin Hood' Hack

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Atlantic Wire
Complete item: http://www.theatlanticwire.com/technology/2011/12/anonymous-affiliates-are-unhappy-about-robin-hood-hack/46718/

Description:
Now that the afterglow of the latest AntiSec assault on the global intelligence firm Stratfor is dulling a bit, some members affiliates of Anonymous are protesting the hacking of a regular old, hard-working American company. This week, the details of AntiSec hacktivists' latest project, loosely dubbed Anonymous' LulzXmas, is stealing headlines in classic LulzSec fashion. The hack reportedly resulted in over 200 gigabytes of Stratfor's data, including everything from log-ins to credit card numbers, and received coverage in all the big outlets from Fox News to The New York Times (and The Atlantic Wire, too). It was reported that AntiSec stole a bunch of money from the rich Stratfor customers and gave it to charities like The Red Cross. But now, doubts are beginning to surface about whether AntiSec's Robin Hood move might backfire.

After all, what happens when the charities are inevitably forced to give that money back to the Startfor customers who unknowingly donated? Further, as details emerge of a two-month-old hack on a small business -- albeit one that potentially supplies pepper-spray to the pepper-spray-loving cops who then spray it all over Occupy protesters -- some wonder whether AntiSec is actually fighting the good fight. Based on rumors that the hackers are preparing to launch a full-on assault against the "some of the most powerful men in the world," however, we're pretty sure Anonymous is not defending the One Percent.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 5:38 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous 'Robin Hood' hacking attack hits major firms

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Telegraph
Complete item: http://www.telegraph.co.uk/technology/news/8980453/Anonymous-Robin-Hood-hacking-attack-hits-major-firms.html

Description:
Thousands of private and government organisations are examining their accounts after hacktivists linked to the Anonymous collective stole credit card information from an American security firm on Christmas Eve and used it to make donations to charities.The attack targeted Stratfor, a Texas-based company which produces analysis on international security issues for international clients including banks, oil companies and police agencies.

As well as claiming to have donated $500,000 to charities online using the stolen data, the hackers posted parts of their haul online. The files included more than 50,000 credit card numbers of which 10,000 were not expired, 87,000 email addresses and 44,000 encrypted passwords, of which around half could be easily cracked.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 5:32 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hackers Still Active, Closing 2011 with a Bang

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: NewsFactor
Complete item: http://www.newsfactor.com/news/Anonymous-Closing-2011-with-a-Bang/story.xhtml?story_id=12300BB06CW9

Description:
Anonymous keeps doing this because it works, and that's part of the problem," said Zeus Kerravala, principal analyst at ZK Research. "PayPal has been the No. 1 target." Anonymous gained fame last year when it issued a hit list of Web sites hostile to WikiLeaks, including PayPal, Visa and MasterCard.

Anonymous struck again on Monday morning -- and the backlash by the infamous hacking group may not be over yet. Anonymous, which took down Strategic Forecasting's Web site over the weekend, has vowed to strike again. This time, the targets are Stratfor members who are speaking out to support the firm. As a result of the hack, Stratfor said it has reason to believe the names of its private corporate subscribers have been posted on other Web sites. Its Web site remained down Tuesday afternoon. The last update from Stratfor was Sunday night.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 5:09 AM
To: Bendelier, Kenneth
Subject: Information: IT Security & Network Security News & Reviews: Anonymous, RSA Lead the Top IT Security News of 2011

Generated by your Alert Subscription on Folder:
- Anonymous
Source: EWeek
Complete item: http://www.eweek.com/c/a/Security/Anonymous-RSA-Lead-the-Top-IT-Security-News-of-2011-601850/

Description:
A series of data breaches, cyber-attacks and privacy missteps by major organizations dominated the news when it came to security in 2011. These incidents also revealed how vulnerable personal information was in this modern, interconnected society. Security was no longer something that tech-savvy professionals and hobbyists thought about, as breach notifications piled up in the Average Joe's mailbox.Some experts called 2011 the Year of the Hack, as hackers targeted everyone. It seemed like no industry was spared, as defense contractors reported intrusion attempts, gaming and entertainment companies were breached, and small and midsize financial institutions reported criminals targeting online banking to fraudulently transfer money overseas.

The past 12 months could also be dubbed the "Year of the Data Breach," as criminals, hacktivists and cyber-spies all went after critical databases, stealing and leaking tons of sensitive information. To be fair, some of the biggest stories of 2011 weren't by malicious criminals as some clueless insiders played a part, too. Here, eWEEK looks at, in no particular order, 11 of the biggest security stories that kept us on the edge of our seats in 2011.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 3:27 AM
To: Bendelier, Kenneth
Subject: Important: 10 things you need to know about Anonymous Stratfor hack

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: venturebeat
Complete item: http://venturebeat.com/2011/12/28/anonymous-stratfor-hack-10-things-to-know/#.TvutXSFGGTo.twitter

Description:
On Dec. 24th, hacker collective Anonymous stole credit card info and other sensitive data from U.S. security firm Stratfor, but keeping track of who and what are affected by the scandal can be difficult.

Weve put together a 10-point FAQ for better understanding the major hacking incident, which blew up in the news cycle on Christmas and continues to worry people as more details are released.

1. What is Stratfor?
2. What is Anonymous?
3. What got hacked?
4. What information has Anonymous published?

5. If Im a Stratfor customer, am I at risk? What should I do?
6. How does the U.S. government use Stratfor?
7. Does this put government data or military operations at risk?
8. What will happen to the charities that Anonymous donated money to using fraudulent credit card numbers?
9. Where can I follow up-to-the-minute updates about the Stratfor hack?
10. What can we expect to come next?

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 3:07 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous - Christmas Message Stratfor security breached

Generated by your Alert Subscription on Folder:
- Anonymous
Source: You Tube
Complete item: http://www.youtube.com/watch?v=1vX_QpGpKE4

Description:
Geploaad door StrikerPrototype op 28 dec 2011 AntiSec plundered 200gb of their mails and more booty

We Donated The Money to American Red Cross and Save the Children

1 Million Dollar's Were Stolen

Stratfor Did NOT encrypt the Client Information , lol wut ?

Expect Us

More Information :-
http://www.youtube.com/watch?v=1vX_QpGpKE4

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 2:34 AM
To: *Bendelier, Kenneth*
Subject: Important: 'Anonymous' stages Christmas hack on military merchant

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Rawstory
Complete item: http://www.rawstory.com/rs/2011/12/28/anonymous-stages-christmas-hack-on-military-merchant/?utm_source=twitterfeed&utm_medium=twitter

Description:
In a recent post to text-sharing website pastebin, a hacker or hackers with the cyber activist group Anonymous claimed responsibility for stealing confidential data from the website of a military gear merchant whose customers are thought to be mostly former soldiers and members of law enforcement.

The website SpecialForces.com retails tactical and survival gear, weapons, uniforms and other merchandise geared toward members of the military. The hackers post claimed that they had accessed the retailers secure servers and scooped up all of their customers data, including passwords and credit card information. The information was published online in a torrent file.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 1:31 AM
To: Bendelier, Kenneth
Subject: Information: McAfee says Anonymous will reorganize or disband in 2012

Generated by your Alert Subscription on Folder:
- Anonymous
Source: venturebeat
Complete item: http://venturebeat.com/2011/12/28/mcafee-2012-security-predictions/

Description:
McAfee released its online security threat predictions for 2012 today, predicting that much of the hacking drama that started in 2011 will only grow in the new year.

When technology evolves, so do cyber criminals tactics for compromising new software, hardware, online accounts and more. Whole conferences, such as the Black Hat and Defcon conferences in Las Vegas, focus on how people are able to gain access to our machines without permission. But 2011 was filled with the beginnings of a new breed of vigilante hacker, as well as the new world of mobile devices to breach.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 1:27 AM
To: Bendelier, Kenneth
Subject: Important: Homeland Security uncovered Anonymous attack on Public Advocate's office

Generated by your Alert Subscription on Folder:
- Anonymous
Source: NYDailyNews
Complete item: http://www.nydailynews.com/new-york/homeland-security-uncovered-anonymous-attack-public-advocate-office-article-1.998171

Description:
Homeland Security officials were among the first to discover that the Public Advocate's Office website was hacked over Christmas weekend.

The federal Multi-State Information Sharing and Analysis Center notified the city's tech department about the cyberattack in which data about thousands of users was stolen.

"They contacted us to confirm the breach," said Public Advocate spokesman Wiley Norvell. "We picked up on suspicious activities earlier in the weekend."

Members of the hacking collective Anonymous took credit for the attack. They posted the stolen information on the data- sharing site filebeam.com, Norvell said.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 1:22 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Stratfor Hack: Charities Hope To Return Fraudulent Funds From $1 Million Scandal

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Huffington Post
Complete item: http://www.huffingtonpost.com/2011/12/28/anonymous-stratfor-hack-c_n_1172926.html

Description:
Some of the charities that benefitted from a recent $1 million hacking scam are working to return the misappropriated funds, Philanthropy.com reports.

The hacking movement, "Anonymous, announced on Twitter Sunday that it had stolen thousands of credit card numbers from clients of the Texas-based private-intelligence company Stratfor, in order to make Christmas donations, according to the Associated Press. Two major charities, the American Red Cross and Care, said they're trying to determine how many fraudulent gifts they received so they can return them.

"We're happy to work with anyone to make sure they're refunded," Melanie Pipkin, a spokeswoman for the Red Cross, told Philanthropy.com.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-29-11 1:17 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hacking Attack Titled 'Robin Hood' Hits The Major Firms

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://www.techgadgetsweb.com/6586/anonymous-hacking-attack-titled-robin-hood-hits-major-firms

Description:
The cyber attack targeted Stratfor which is a company from Texus carrying out analysis on the international security issues especially for banks, police agencies, and oil companies.

Besides, claiming to own a donating as much as $500,000 to online based charities by stealing data, hackers posted some specific parts of their online haul. The stolen files included above 50,000 numbers of credit cards of which approximately 10,000 were within the date of expiration, total of 87,000 email addresses & 44,000 encrypted passwords including almost half that could b cracked quite easily.

Major British firms including BP, HSBC & Tesco were enlisted in those files.

On the Boxing Day, hackers claimed to have a sample of stolen emails of the servers of Stratfor.

This is just a preview of the upcoming mayhem, stated in message from the hackers.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-28-11 2:23 PM
To: Bendelier, Kenneth
Subject: Important: SpecialForces.com hacked: Anonymous strikes again - LulzXmas continues

Generated by your Alert Subscription on Folder:
- Anonymous
Source: EXAMINER
Complete item: http://www.examiner.com/anonymous-in-national/specialforces-com-hacked-anonymous-strikes-again-lulzxmas-continues

Description:
Tango down: a website belonging to Special Forces Gear, a company that sells military and law enforcement equipment, has been hacked by the international Internet hacktivist collective known as Anonymous.

On Tuesday, Annonymous enthusiasts announced via a Pastebin release that SpecialForces.com had been hacked. The attack comes as part LulzXmas, an Anonymous operation being run by #AntiSec, a loose but prolific collection of cells within the Anonymous collective.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-28-11 2:11 PM
To: Bendelier, Kenneth
Subject: Important: Hacking Group Anonymous Takes First Step in Master Plan, Vows to Strike Again

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://geinvestigations.com/blog/tag/working-with-the-hacking-group-lulzsec-on-a-series-of-hacking-attacks-it-called-operation-anti-security/

Description:
The global activist hacking group Anonymous claims to have obtained thousands of credit card numbers and personal information from the high-profile clients of a leading analytical intelligence company, all in the name of charity.

Up to $1 million was reportedly stolen from Stratfor, in Austin, Texas, a leading provider of military, economic and political analysis for clients that include Apple and the U.S. Air Force.

#AntiSec plundered 200gb of their mails and more booty, read a tweet by @AnonymousIRC on Saturday.

Anonymous, an online community with no hierarchical organization, had been working with the hacking group Lulzsec on a series of hacking attacks it called Operation Anti-Security, or Operation AntiSec.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-28-11 12:54 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hackers Plunder Top US Security Think Tank

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Security News Daily
Complete item: http://www.securitynewsdaily.com/anonymous-hackers-stratfor-1447/

Description:
The "Anonymous" hacking group gave U.S. global intelligence firm Stratfor a big batch of Christmas coal by infiltrating the company's network and stealing thousands of emails and credit card details from its high-profile clients, with the goal of raiding the stolen accounts and donating $1 million to charity.

The hackers claimed they stole 200 gigabytes of private emails, as well as the credit card details of more than 90,000 clients of Strategic Forecasting, Inc., (Stratfor) an Austin, Texas-based research firm that advises top companies and government agencies on security, economic, business and political affairs.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-28-11 12:31 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hacks SpecialForces.com

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Security News Daily
Complete item: http://www.securitynewsdaily.com/anonymous-specialforces-hack-1451/

Description:
The prolific hacking group Anonymous has launched the second wave of its holiday campaign of break-ins, entering SpecialForces.com and leaking thousands of confidential user details, including credit card numbers.

"Continuing the weeklong celebration of wreaking utter havoc on global financial systems, militaries, and government, we are announcing our next target: the online piggy supply store SpecialForces.com," Anonymous wrote in a Dec. 27 Pastebin post.

SpecialForces.com, based in Gardena, Calif., sells such equipment as handcuffs, nightsticks, tasers, knives, clothing and tactical gear to law enforcement agencies and the military.

E-Secure-IT
https://www.e-secure-it.com

St-Louis, Danielle

From: St-Louis, Danielle
Sent: December-28-11 9:21 AM
To: [redacted] Champoux, Martin; Coady, Therese; Danaitis, Algis; Dick, Robert; Dole, Natalie; Dvorkin, Corey; Hatfield, Adam; Labelle, Sébastien; Panchyson, Dorian; Selman, Semira
Subject: CCIRC WEEKLY SUMMARY FOR WEEK OF DEC 12
Attachments: PS-SP-#527919-v1-FEEDBACK_FORM_FOR_WEEKLY_SUMMARY_FOR_EXECS.DOC; PS-SP-#536525-v5-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_DEC_12_2011.DOC

Good morning,

please find attached the CCIRC Weekly Summary of significant cyber events and incidents reported to and observed by CCIRC, with analysis where required. Please note this product is *not* intended for wide circulation since it is still in the pilot phase. Here are the highlights:

HIGHLIGHTS:

CCIRC Products: Two technical advisories were posted on Public Safety Canada's website.
- AV11-049: Microsoft Security Bulletin Summary for December 2011
- AV11-050: Security Update for Critical Vulnerabilities in Adobe Reader and Adobe

Notable Incidents:
- Malicious e-mails from threat actors impersonating prominent Canadian financial institutions, a telecommunications company and Canada Revenue Agency
- User account information for Canadian and US corporate, government, law enforcement as well as a Canadian university's users posted on the internet by hackers
- A telecommunications service provider experienced cyber-attack; over 200,000 affected in a Canadian province

International: Personal information for two US police departments' officers posted online

Vulnerability Warnings: Specific vulnerabilities of websites in the federal, provincial, food and education sectors were posted on the internet.

Noteworthy Open Source Reports:
- Hacker group posts online user account information for law enforcement, federal, military, loss prevention professionals and employees of certain large corporations
- DHS releases strategy to respond to cyber threats titled "Blueprint for a Secure Cyber Future: The Cyber security Strategy for the Homeland Security Enterprise"
- Report titled "Managing Automation Systems: Critical Infrastructure Operators' Challenges & Opportunities" released by Industrial Defender, a US company

This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca <mailto:bud.cameron@ps-sp.gc.ca> .

Danielle St-Louis
Administrative Assistant | Adjointe administrative Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: 613-991-7738
Fax | Téléc.: 613-996-0995
E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-28-11 8:15 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
December 28, 2011 / le 28 décembre 2011

Print media

GSM phones vulnerable to hijack scams, researcher says
Vulnerability in a widely used wireless technology could allow hackers to gain remote control of phones and instruct them to send text messages or make calls, according to an expert on mobile phone security. They could use the vulnerability in the GSM network technology, which is used by billions of people, to make calls or send texts to expensive, premium phone and messaging services in scams, said Karsten Nohl, head of Germany's Security Research Labs. Vancouver Sun, C3

2011-12-27

New jobs for a new age
Cyber warfare will likely increase in the coming years, and therefore the need for tech-savvy soldiers will also rise. Chronicle-Herald, C1

2011-12-26

Hackers attack security think-tank
The loose-knit hacking movement Anonymous claimed Sunday to have stolen thousands of credit card numbers and other personal information belonging to clients of U.S.-based security think-tank Stratfor. Chronicle-Herald, B1

Android phones targeted for 2012 cybercrime
Cybercrimes are becoming more mobile. As more smartphones and tablets are being used, cyber thieves aren't just targeting personal computers to steal information for financial gain, say antivirus security experts. Hamilton Spectator, A12

Hewlett-Packard fixes LaserJet printer security flaw
Hewlett-Packard has released a firmware update it says will fix a susceptibility in some of the company's popular LaserJet printers that could allow hackers to take control of the devices remotely. Calgary Herald, B8

Online media

Hackers could shut down train lines – expert
Hackers who have shut down websites by overwhelming them with web traffic could use the same approach to shut down the computers that control train switching systems, a security expert said at a hacking conference in Berlin. Reuters

Will 2012 be the year we all get hacked?
Through our governments, our tablets or our cars, cyber criminals in 2012 will be exploiting new avenues of attack. The emergence of new hacker strategies to target physical infrastructure, major financial institutions and mobile devices made 2011 a transformative year for digital security, says the 2012 Threat Predictions report released by McAfee Inc. on Wednesday. In 2012, the company expects those risks will mature, making everyone from state actors to individual smartphone users a likely target. Financial Post; ZDNet

S. Korea's military lowers cyber alert level to normal
South Korea's military has lowered its cyber alert level to normal, about a week after it was raised in the wake of the death of Kim Jong Il, the late leader of the Democratic People's Republic of Korea (DPRK), local media reported on Wednesday. Xinhua

2011-12-27

Cyber Threat to Power Grid Puts Utility Investors at Risk
The electric-utility industry's concerns about cyber security has escalated sufficiently for several investor-owned utilities to include cyber-attacks as a material risk factor in recent filings with the U.S. Securities and Exchange Commission. Forbes

2011-12-26

2012 will see a rise in cyber-espionage attacks and sophisticated malware, experts say
The security industry expects the number of cyber-espionage attacks to increase in 2012 and the malware used for this purpose to become increasingly sophisticated. ITworld

Iran develops new cyber defense model
Head of Iran's Passive Defense Organization says Iran has developed a new defense model that is different from passive defense and specific to the country's defensive requirements in countering any potential cyber attacks. PressTV

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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-28-11 7:49 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Survival Guide for Citizens in a Revolution

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: Various Sources
Complete item: http://www.multiupload.com/1GA9HET58U

Description:
http://www.multiupload.com/1GA9HET58U

http://www.multiupload.com/RS_1GA9HET58U

http://www.multiupload.com/MU_1GA9HET58U

http://www.multiupload.com/UK_1GA9HET58U

http://www.multiupload.com/UH_1GA9HET58U

http://www.multiupload.com/DF_1GA9HET58U

http://www.multiupload.com/HF_1GA9HET58U

http://www.multiupload.com/ZS_1GA9HET58U

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-28-11 6:19 AM
To: Bendelier, Kenneth
Subject: Important: Stratfor Denies Anonymous Compromised Client List

Generated by your Alert Subscription on Folder:
- Anonymous
Source: EWeek
Complete item: http://www.eweek.com/c/a/Security/Stratfor-Denies-Anonymous-Compromised-Client-List-496506/

Description:
Stratfor has asserted that hackers from the Anonymous collective did not steal its confidential client list, but rather a list of people who had purchased its publications.Strategic Forecasting, an organization that focuses on intenerational security issues, is downplaying the severity of the cyber-attack it suffered over the weekend, claiming its client list had not been stolen.

A group of hackers claiming to be part of the hacktivist collective Anonymous attacked the global intelligence think tank on Dec. 24 and stole approximately 200GB of information, such as credit card numbers and other personal information, from Stratfor's servers, according to various posts on Twitter.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-28-11 3:47 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous stole over 9K active credit card numbers in Stratfor hack

Generated by your Alert Subscription on Folder:
- Anonymous
Source: pastebin
Complete item: http://pastebin.com/scbC0A0i

Description:
A clearer picture of the damage from the Stratfor hacking incident from Christmas Eve is coming into focus, with an independent analysis confirming more than 9,000 active credit card numbers were stolen from the security think tank.

In a high-profile incident that blew up the news on Christmas, the notorious hacker group Anonymous claimed to have stolen credit card data and other client details from Austin-based security think tank Stratfor, with the intent of donating $1 million in stolen cash to charity. When the story broke, it was still unclear what exactly had been stolen, but now an independent analysis has broken down the numbers.

New York-based data loss and identity theft prevention service Identity Finder issued a report today that stacks up how much data was stolen from the A through M names from Stratfors customer list. Anonymous is expected to release data from the N through Z names in the coming days.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-27-11 2:26 PM
To: Bendelier, Kenneth
Subject: Important: 'Anonymous' hackers hit US security firm Stratfor

Generated by your Alert Subscription on Folder:
- Anonymous
Source: BBC
Complete item: http://www.bbc.co.uk/news/world-us-canada-16330396

Description:
The activist hacker group Anonymous says it has stolen thousands of emails, passwords and credit card details from a US-based security think-tank.

The hackers claim they were able to obtain the information because the company, Stratfor, did not encrypt it.

They say Stratfor's clients include the US defence department, law enforcement agencies and media organisations.

The Austin-based company says it has now suspended the operation on its servers and email.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-27-11 10:26 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Operation Falcon, Anti Police Brutality Program 2012

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: YouTube
Complete item: http://www.youtube.com/watch?v=EcN80M6IvKU

Description:
Anonymous Global Anti Police Brutality Program 2012.
https://www.facebook.com/pages/Fawkes-Security/268120943244762
https://www.facebook.com/groups/160102654090712
https://twitter.com/#!/FawkesSecurity

greetings citizens, we are anonymous. during a time of recession, revolution and government down fall, we, the people of the world rely on the stable order of law enforcement with a fair justice system, in more recent times this is simply not the case. more people through out the world are increasingly becoming the subject of police brutality and puppets of a corrupt criminal justice system. minoritys of law enforcement all over the world are abusing their powers to the extent of causing serious harm or death to innocent people. in no way should a police officer who represents safety of the community and lifes be above the law. a large number of these cases are never investigated, even after official complaints.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-27-11 10:03 AM
To: Bendelier, Kenneth
Subject: Information: Press Release: Stratfor hack NOT Anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
Source: pastebin
Complete item: http://pastebin.com/8yrwyNkt

Description:
Emergency Christmas Anonymous Press Release

12/25/2011

THE STRATFOR HACK IS NOT THE WORK OF ANONYMOUS

Stratfor is an open source intelligence agency, publishing daily reports on data collected from the open internet. Hackers claiming to be Anonymous have distorted this truth in order to further their hidden agenda, and some Anons have taken the bait.

The leaked client list represents subscribers to a daily publication which is the primary service of Stratfor. Stratfor analysts are widely considered to be extremely unbiased. Anonymous does not attack media sources. In this excerpt from Time, there is a brief description of how Stratfor analysts uncovered a possible US backed coup in Iraq preceding the US invasion.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-27-11 9:18 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Mused - The recent attack on Stratfor brings to light some questions

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Cryptome.org
Complete item: http://cryptome.org/0006/anonymous-mused.htm

Description:
The recent attack on Stratfor [1][2][3] brings to light some questions that can not be ignored. As we all well know, Anonymous has taken credit [4] for this attack. With events such as this it is very possible that there are goings-on behind the scenes that need to be taken into account.

Lets start with Anonymous' [5], and it's sub-organization #antisec [6], as a whole. Anonymous fancies itself as some sort of hacktivist organization fighting for the greater good of all mankind. In reality it is nothing more than a name that different groups can hide behind in order to leak/drop information and attach itself to the Anonymous "brand" or rather, it's PR infrastructure. For example, there are various Twitter accounts [7][8] and IRC servers .

[9] that serve as the main conduit for news and information related to recent Anonymous activity. Not only is Anonymous very good at PR, they piggy-back off of preexisting movements in order to gain attention and new members. For example, the "antisec" or "pr0j3kt m4yh3m" movement was not started by Anonymous, rather multiple groups started some years ago created this movement [10][11]. Anonymous has adopted it as their own after the movement slowed down due to various reasons (group members growing older and getting a job, getting arrested [12], drug overdoses, etc).

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-27-11 8:40 AM
To: Bendelier, Kenneth
Subject: Important: 'Anonymous' plans for 'violent revolution' - Hacking group that helped protests warns of 'bloody mess'

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: Wnd
Complete item: http://www.wnd.com/?pageId=381477

Description:
The hackers known as "Anonymous," who helped organize and support the Occupy movement's protests, have released an online survivor guide for citizens "in case of a violent revolution in your country." The guide warns protests can be a "bloody mess." It trains rioters on how to avoid tear gas, rubber bullets and live ammunition.

The 15-page PDF document claims police will not help protesters and may actually be enemies of the revolution while warning that protest groups may be infiltrated by "fake civilians." The Anonymous survival guide was published just before the hacker group claimed Sunday to have stolen thousands of credit card numbers and other personal information belonging to clients of U.S.-based security think tank Stratfor.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-27-11 2:31 AM
To: Bendelier, Kenneth
Subject: Important: Message from AnonSanta

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: pastebin
Complete item: http://pastebin.com/q5kXd7Fd

Description:
Greetings Global Pirates,

We truly hope that youve been enjoying the Lulzxmas festivities so far. The gifts that AnonSanta left under the LulzXmas tree are just the beginning. As we speak, his little helpers at the North Pole are readying his battle sleigh of lulz with more goodies to bring you LulzXmas joy all week long. Joy in the form of over $500,000 being expropriated from the bigshot clients of Stratfor. You didnt think wed let 2011 end without a BANG, did you?

However, if you are one of the hundreds of thousands of customers of STRATFOR Global [Un]Intelligence, you probably woke up Christmas morning to find heaps of burning coal in your stocking. But dont fret. Take comfort in the fact that at least youre not George Friedman or any of the STRATFOR IT guys right now.

We create chaos. We create mayhem. We curb stomp companies that play fast and loose with their customers private and sensitive information. We bring pain to greedy whitehats willing to flip for a dime on government payrolls. And dont worrytheres plenty more havoc in store for the rest of the week. So throw a log on the fire, grab some hot chocolate and settle in for a long week of lulz.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-27-11 12:16 AM
To: Bendelier, Kenneth
Subject: Important: Confidential Client List Safe From Anonymous, Says Hacker Target

Generated by your Alert Subscription on Folder:
- Anonymous
Source: CSOonline
Complete item: http://www.csoonline.com/article/697083/confidential-client-list-safe-from-anonymous-says-hacker-target

Description:
The damage from a weekend data breach at a think tank on international security issues appears to have been inflated by the assault's perpetrators, the hacker collective known as Anonymous.

After Anonymous ransacked think tank Stratfor's computers and stole away thousands of credit card numbers and other personal information, it claimed to have also clipped the company's confidential client list. That list contains sensitive information about Stratfor's high profile clients, such as Apple, the U.S. Air Force, and the Miami Police Department.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 11:37 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous: Operation Robin Hood

Generated by your Alert Subscription on Folder:
- Anonymous
Source: You Tube
Complete item: http://www.youtube.com/watch?v=R76QLTiiAaU

Description:
we are p0isAnon. Anonymous and TeaMp0isoN have joined forces to fight censorship in the name of OpCensorThis. There is a new operation that has been taking place over the actions of Banks in response to the Occupy Movement. We have watched our brothers and sisters being refused their hard earned money by the banks on top of being beaten and brutalized by officers during peaceful demonstrations. Congratulations banks, you have gotten our attention.

You ignore your customers and use authorities to censor their voices. Operation Censor This will not stand for such acts and is spawning another operation under Operation Cash Back which already removed well over 500,000 accounts from banks and put them into credit unions. This is the next step. Banks have stolen millions from its customers as well as lacked the security to protect them. We give you Operation Robin Hood.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 11:21 PM
To: Bendelier, Kenneth
Subject: Important: Financial fraud against Anonymous Analytics

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://www.secnews.gr/archives/35224

Description:
A new group chaktiviston, member of the famous group Anonymous called Anonymous Analytics has published a report which accused the Chinese company Chaoda Modern Agriculture for " 11 years of fraud and financial crime . " The company is one of the largest suppliers of China's vegetables.

This new "portion" of Anonymous has now progressed to a new place, trying to uncover the fraud are companies

through which earn much profit.

The group Anonymous Analytics claims that the administration of Chaoda has transferred more than 400 million dollars from the company through false accounting and payments to fictitious companies . Recently announced an inquiry to the company, shortly before the release of the report, driving its shares drop to 26% before the suspension of trading.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 11:06 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous attacks security firm Stratfor, $1M stolen/donated

Generated by your Alert Subscription on Folder:
- Anonymous
Source: geektech
Complete item: http://geektech.in/archives/6917

Description:
Whitehat security firm Stratfor underwent a massive hack by Anonymous hackers on eve of Christmas or should we tell LulzXmas as the Anonymous would call it. STRATFOR provides intelligence to a range of commercial and government customers, and has been beefing up its coverage of cyber, and specifically of Anonymous. Official website of Stratfor stratfor.com went offline after the attack but those interested can view a mirror of the deface.

More Information :-
http://geektech.in/archives/6917

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 10:37 PM
To: Bendelier, Kenneth
Subject: Important: Started - OpRobinHood by Anonymous on Christmas Day

Generated by your Alert Subscription on Folder:
- Anonymous
Source: digital life
Complete item: http://www.digitallife.gr/xekinhse-to-oprobinhood-apo-tous-anonymous-anhmera-xristougennwn-14657/

Description:
We have an update on Operation Robin Hood from the online activist group, Anonymous . The purpose of this operation is to steal part of the wealth held by some (1%) and to redistribute the remaining 99% , according to the time announcement. How do we manage it? By hacking into websites of companies using this 1% for various services, thereby taking, credit card details and personal information to proceed with withdrawals from their bank accounts and the amounts to be deposited in a non-profit organizations .

That was the security company Stratfor specializes in risk management and "sells online petitions risk. From dawn Sunday's page is "down", while Anonymous announced they have at their disposal thousands of numbers, credit cards, emails, addresses, the database company.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 10:31 PM
To: Bendelier, Kenneth
Subject: Important: Digitallife.gr: Started in OpRobinHood by Anonymous on Christmas Day

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://www.techfeeds.gr/internet/digitallifegr-ksekinise-to-oprobinhood-apo-tous-anonymous-animera-christougennon.html

Description:
We have an update on Operation Robin Hood from the online activist group, Anonymous. The purpose of this operation is to steal part of the wealth held by some (1%) and to redistribute the remaining 99%, according to then report them. How do we manage it? By hacking into websites of companies.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 1:04 PM
To: Bendelier, Kenneth
Subject: Important: Malicious Hackers Play Robin Hood, Anonymous Disavows Action

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: Read Write Web
Complete item:
http://www.readwriteweb.com/archives/malicious_hackers_play_robin_hood_anonymous_disavo.php?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+readwriteweb+%28ReadWriteWeb%29

Description:
A rogue group of malicious hackers penetrated the database of U.S. think tank Stratfor over the Christmas holiday weekend and stole thousands of credit card files. Those credit cards were then subsequently used to make online payments to a variety of charitable organizations. Modern day digital Robin Hood? Think again.

The hack was perpetrated by a groups of malicious hackers loosely affiliated with anti-security group Anonymous. It is hard to tell what hackers are actually part of Anonymous these days as with each successive scheme, one group will claim it is working under the Anonymous banner while another will disavow the action. At this point, Stratfor does not really care what the hackers call themselves.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 12:57 PM
To: Bendelier, Kenneth
Subject: Important: Stratfor Targeted by Hacking Group Anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
Source: EWeek
Complete item: http://www.eweek.com/c/a/Security/Stratfor-Targeted-by-Hacking-Group-Anonymous-652070/?kc=rss

Description:
Hackers posted what they claimed to be personal details of the company's clients on the information-sharing site Pastebin.

The loosely-associated band of hackers known as Anonymous claims to have targeted the global intelligence think tank Strategic Forecasting, known as Stratfor, boasting on the microblogging site Twitter that personal information, including credit card numbers, belonging to Stratfor clients had been stolen. As of Monday morning, Stratfors Website was down, with a placeholder page saying the site was undergoing maintenance and asking visitors to check back soon.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 12:46 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous claims to hack US security firm Stratfor

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Channel News Asia
Complete item: http://www.channelnewsasia.com/stories/technologynews/view/1173403/1/.html?

Description:
Online "hacktivist" group Anonymous claimed Sunday it had stolen a trove of emails and credit card information from US-based security firm Stratfor's clients, and vowed additional attacks.

Hackers provided a link on Twitter to what they said was Stratfor's private client list, which included the US Defence Department, Army, Air Force, law enforcement agencies, top security contractors and technology firms like Apple and Microsoft.

They also posted images online claiming to show receipts from donations made by the hackers on behalf of some of Stratfor's clients by using their credit card data.

E-Secure-IT
https://www.e-secure-it.com

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-26-11 8:59 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
December 26, 2011 / le 26 décembre 2011

MINISTER / MINISTRE

Former KGB translator spends third Christmas in Vancouver sanctuary
Pastor Richard Hergesheimer said many of his flock were moved by the present moment in the tortuous life of the performer, Mikhail Lennikov. Since June 2, 2009, the former Japanese translator for the KGB has taken sanctuary inside the walls of the church in southeast Vancouver. Federal Court judge ordered Lennikov deported in June 1999 under a law that dictates any former member of a spy agency that spies on democratic governments is inadmissible. If the **Public Safety Minister, currently Vic Toews**, finds Lennikov is not "detrimental to the national interest," as the law reads, Toews has the power to stay the deportation order. Times-Colonist, A8

Failure to appeal is appalling
A letter to the editor states, "The following is a copy of a letter to Robert B. Trevors, Minister Responsible for Public Safety. I am writing to express my complete disgust with the Blais decision not to appeal the verdict in the recent Losier/police language case in Fredericton. How can you as Minister responsible for public safety let this abomination of a decision so critical to public safety stand and not say a word?... I have written the Premier and I will write the **Federal Minister of Public Safety**..." Telegraph-Journal, A4

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

La Colombie-Britannique se prépare au nettoyage
Le gouvernement de la Colombie-Britannique compte travailler avec les autorités fédérales et municipales afin de nettoyer les débris transportés par le tsunami de mars 2011 au Japon et qui vont envahir les rives de la région de Vancouver. Le Soleil, 13 (Hamilton Spectator); Times-Colonist (Edmonton Journal, Windsor Star, Leader-Post, Ottawa Citizen, Calgary Herald)

Area flood damage exceeds $25 million
This year's heavy rainfall caused millions in property damage and has put pressure on area municipalities to address flooding issues. At least $25 million in property damage was caused from flooding of almost 1,000 homes during six storms that were categorized as one in 100-year events. Windsor Star, A5

CYBER SECURITY / CYBERSÉCURITÉ

Hackers attack security think-tank
The loose-knit hacking movement Anonymous claimed Sunday to have stolen thousands of credit card numbers and other personal information belonging to clients of U.S.-based security think-tank Stratfor. Chronicle-Herald, B1

Android phones targeted for 2012 cybercrime
Cybercrimes are becoming more mobile. As more smartphones and tablets are being used, cyber thieves aren't just targeting personal computers to steal information for financial gain, say antivirus security experts. Hamilton Spectator, A12

Hewlett-Packard fixes LaserJet printer security flaw

Hewlett-Packard has released a firmware update it says will fix a susceptibility in some of the company's popular LaserJet printers that could allow hackers to take control of the devices remotely. Calgary Herald, B8

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

RCMP Waterloo?
An editorial states, "It's said that the first step in recovery is admitting you have a problem. Bob Paulson, the RCMP's new commissioner, has taken that step, but recovery is still far from certain. That's because, as Mr. Paulson has stated, the force is so dysfunctional and the problems so large that only radical surgery will set it right again..." Winnipeg Free Press, A12

GROWING PAINS
Three of my travelling companions are members of the International Policing Operations Branch of the RCMP, which is responsible for coordinating a program that sees Canadian police officers assigned to international locations to assist the development of the local police. I am struck by the level of security. Again I was reminded of our briefing in Ottawa, where we were informed of the challenges involved in the recruitment and training of candidates for both the Afghanistan National Army (ANA) and the Afghanistan National Police (ANP). Two of us get into an armoured vehicle with RCMP Chief Supt. Ev Summerfield, who is in charge of all Canadian police officers in the country. Calgary Sun, 4

Police probe two weekend shootings in Surrey
Police are dealing with the second shooting in as many days in Surrey. In the early hours of Christmas Day, a 54-year-old woman was shot in an apartment in the 13300-block of King George Boulevard in Whalley. When police arrived they found a woman suffering from non-life-threatening injuries. Early reports from officers suggested the woman was shot in the chest, said Staff Sgt. Heather Stark of the Surrey RCMP. Vancouver Sun, A8; The Province

Plan may backfire on well-meaning
Quebec police offer this warning to would-be cyber-sheriffs who try to catch suspected online predators: Watch out. Vigilantes have no legal protection and could be charged. London Free Press, C2

Senior members in the dark?
A letter to the editor states, "The newly appointed commissioner of the RCMP, Bob Paulson, is a senior member of this organization. And it's only now that this disgraceful, far-reaching harassment has come to his attention?" Toronto Star, A18

Stripping away our human rights
A letter to the editor states, "...Last week a Conservative MP said he wants Parliament to extend human rights to the unborn. Never mind that many of us feel that our human rights have been stripped away. Native Canadians have no rights; the UN has confirmed that and the Conservatives slam the UN. Women in the RCMP have no rights and are ignored by Ottawa..." Toronto Star, A18

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

The secrets of secret compartments
Just metres from the Canadian border, Paul Vogt pops the top on a secret compartment in the ceiling of a commercial truck's cab. "There were 50 kilos of cocaine in this," says Vogt, the Canada Border Services Agency's local expert on clandestine compartments. Vancouver Sun, A6

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Two cons found dead in cells
The Christmas Eve deaths of a convicted murderer and a convicted drug trafficker have triggered an investigation at Drumheller Correctional Facility. Autopsies on both are set for early next week. Meanwhile, RCMP continues to investigate. Calgary Sun, 11 (Edmonton Sun); Chronicle-Herald; Calgary Herald (Edmonton Journal, Times-Colonist)

Family outraged by light sentence for attack

For beating a nonnative builder to within an inch of his life during the fiery native occupation in Caledonia, Ont., a young aboriginal man was sentenced to less than two years in jail, plus time served - a punishment that leaves the victim's family demanding an inquiry into how the courts treat First Nations offenders. Ontario Superior Court Judge Alan Whitten on Friday cited the sad legacy of residential schools and the disproportionately large population of incarcerated aboriginal offenders as reasons he did not give Richard Smoke a harsher sentence for an attack he described as "senseless and vicious" and "just a notch below culpable homicide." Windsor Star, A10

INTERNATIONAL / INTERNATIONAL

Terrorist attacks across Nigeria kill 39
Terror attacks across Nigeria by a radical Muslim sect killed at least 39 people Sunday. A massive explosion killed the majority on the steps of a Catholic church after celebrating Christmas mass. Chronicle-Herald, A1; Leader-Post; Hamilton Spectator

Canada calls for 'justice'
Foreign Affairs Minister John Baird on Sunday condemned the series of deadly attacks against Christians celebrating Christmas in Nigeria that killed at least 27 people. Ottawa Sun, 11

North Korea and H5N1
An opinion piece states, "Western intelligence agencies have been warning for years about the terrible consequences that would ensue if Iran were to get nuclear weapons. Better bomb the place before they do. But North Korea already has nuclear weapons, and now they are falling into the hands of a young man whose main qualification for office is that he is less weird than his half-brother, who was caught trying to sneak into Japan on a false passport to visit Disneyland Tokyo..." Daily Gleaner, C9

OTHER / AUTRE

Make sure passport in 'perfect' shape going to Mexico, WestJet warns
WestJet is warning Canadians travelling to Mexico they should make sure their passports are in "perfect condition" before visiting the popular winter destination. Passport Canada's website says people with damaged passports may face delays at checkpoints or be prohibited from boarding. Vancouver Sun, A11; Edmonton Sun

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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 6:54 AM
To: Bendelier, Kenneth
Subject: Important: 'Anonymous' Claims Hack of Credit Data From Security Group .

Generated by your Alert Subscription on Folder:
- Anonymous
Source: WSJ
Complete item: http://online.wsj.com/article/SB10001424052970203479104577120530217909036.html

Description:
Members of the loose-knit movement "Anonymous" claimed on Sunday to have stolen a raft of emails and credit-card data from U.S.-based security think tank Stratfor, promising it was just the start of a weeklong, Christmas-inspired assault on a long list of targets. One alleged Anonymous affiliate said the goal was to use the credit data to take a million dollarsincluding, apparently, from individuals' accountsand give the money away as Christmas donations. Images posted online claimed to show the receipts.

A Twitter account tied to Anonymous posted a link to what they said was Stratfor's tightly guarded, confidential client list. Among those on the list: The U.S. Army, the U.S. Air Force and the Miami Police Department.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 6:28 AM
To: Bendelier, Kenneth
Subject: Important: Alleged Stratfor hack could be biggest in history of Anonymous / LulzSec

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Wordpress
Complete item: http://100gf.wordpress.com/2011/12/25/alleged-stratfor-hack-could-be-biggest-in-history-of-anonymous-lulzsec/

Description:
Members of Anonymous and LulzSec are claiming to have carried out possibly the biggest and most significant hacking attack in their short history. They claim to have allegedly hacked Stratfor, one of the worlds leading global intelligence companies.

The claims, which have not been verified by Stratfor at the time of writing, include allegations that email correspondence, client lists and payment information have been acquired by the hackers. There are unconfirmed claims that charitable donations have been made using some of this payment information.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 6:25 AM
To: Bendelier, Kenneth
Subject: Important: Alleged Stratfor hack could be biggest in history of Anonymous / LulzSec

Generated by your Alert Subscription on Folder:
- Anonymous
Source: ibnlive
Complete item: http://ibnlive.in.com/news/anonymous-hackers-target-us-security-think-tank/215134-11.html

Description:
The loose-knit hacking movement "Anonymous" claimed Sunday to have stolen thousands of credit card numbers and other personal information belonging to clients of US-based security think tank Stratfor. One hacker said the goal was to pilfer funds from individuals' accounts to give away as Christmas donations, and some victims confirmed unauthorised transactions linked to their credit cards.

Anonymous boasted of stealing Stratfor's confidential client list, which includes entities ranging from Apple Inc. to the US Air Force to the Miami Police Department, and mining it for more than 4,000 credit card numbers, passwords and home addresses.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 4:48 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous claims hack on security think tank

Generated by your Alert Subscription on Folder:
- Anonymous
Source: CNet
Complete item: http://news.cnet.com/8301-1009_3-57348300-83/anonymous-claims-hack-on-security-think-tank/

Description:
Anonymous is claiming to have stolen 200GB worth of data, including e-mails and clients' credit card information, from a U.S.-based security think tank, the Associated Press reported today.

The hacking group also used Twitter to post a link to a list of clients apparently belonging to think tank Stratfor Global Intelligence.

"Not so private and secret anymore?" read one of numerous tweets from AnonymousIRC, a Twitter account linked to Anonymous.

This morning Stratfor's site was down. A notice reads: "Site is currently undergoing maintenance."

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-26-11 4:40 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Stratfor hack publishes personal emails George Friedman - founder of Stratfor

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: pastebin
Complete item: http://pastebin.com/HmDs0EM4

Description:
Anonymous Stratfor hack publishes personal emails George Friedman - founder of Stratfor.

Comments in pastebin item:
- just a small preview of the mayhem to come.
1 out of 2.7 million

Info on Friedman - George Friedman is an American political scientist and author. He is the founder, chief intelligence officer, financial overseer, and CEO of the private intelligence corporation Stratfor. He has authored several books, including The Next 100 Years, The Next Decade, America's Secret War, The Intelligence Edge, The Coming War With Japan and The Future of War.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-25-11 10:52 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hacked Copseek.com and leakded the information

Generated by your Alert Subscription on Folder:
- Anonymous
Source: pastebin
Complete item: http://pastebin.com/6Z13RNn5

Description:
NjTexanGrl@aol.com:3b8c69a77da5261aaf4a399a35d16b51
cop_teach@hotmail.com:e106e0e434cc70b70cf076b828128c60
ugojwt2@aol.com:2522c8a5837a7c180888dfc71ef7bdb2
kwmumworm@yahoo.com:e75cb6863fa93d697be65451f9b103f0
damsilberman@yahoo.com:29ae93f4f9aa1ca9f31604e0d27f4a9e
jj_wiss@yahoo.com:6890fb49a2971e24c738f4ac56b6a4a2
stargazer276@aol.com:782cc6a94b62f0e1045e0b69f3838816
IMWRTH1@AOL.COM:d0dab92d332617496ad4611ed17bfa54
missy_14_28@yahoo.com:e979b459f2ee4511d1ca8fa6f96e785a
Instructorstu@aol.com:e0cde46a9fe425aef07f80cae2ffa114
brooks_christopher@yahoo.com:cc989606b586f33918fe0552dec367c8

E-Secure-IT
https://www.e-secure-it.com

Williston, Sandra

From: [redacted]
Sent: December-25-11 9:22 PM
To: [redacted]
Cc:
Subject: Media Item: Hackers attack US security think tank Stratfor, promise more targets for Christmas

Hackers attack US security think tank Stratfor, promise more targets for Christmas

Associated Press (APR)
Cassandra Vinograd
Dec 25 08:04

LONDON _ Hackers on Sunday claimed to have stolen 200 GB of emails and credit card data from United States security think-tank Stratfor, promising a weeklong Christmas-inspired assault on a long list of targets.

Members of the loose hacking movement known as ``Anonymous'' posted a link on Twitter to what it said was Stratfor's secret client list _ including the U.S. Army, the U.S. Air Force, Goldman Sachs and MF Global.

``Not so private and secret anymore?,'' the group taunted in a message on the microblogging site.

Anonymous said it was able to get credit details, in part, because Stratfor didn't bother encrypting them _ an easy-to-avoid blunder which _ if true _ would be a major embarrassment for any security company.

Stratfor said in an email to members that it had suspended its servers and email after learning that its website had been hacked.

``We have reason to believe that the names of our corporate subscribers have been posted on other websites,'' said the email, passed on to The Associated Press. ``We are diligently investigating the extent to which subscriber information may have been obtained.''

The email, signed by Stratfor Chief Executive George Friedman, said the company is ``working closely with law enforcement to identify who is behind the breach.''

``Stratfor's relationship with its members and, in particular, the confidentiality of their subscriber information, are very important to Stratfor and me,'' Friedman wrote.

Stratfor's website was down midday Sunday, with a banner saying ``site is currently undergoing maintenance.''

Wishing everyone a ``Merry LulzXMas'' _ a reference to spinoff and fellow troublemakers Lulz Security _ Anonymous also posted a link on Twitter to a site containing the email, phone number and credit number of a U.S. Homeland Security employee.

The employee, Cody Sultenfuss, said he had no warning before his details were posted.

``They took money I did not have,'' he told The Associated Press in an email. ``I think why me? I am not rich.''

Anonymous warned it has ``enough targets lined up to extend the fun fun fun of LulzXmas through the entire next week."

The group has previously claimed responsibility for attacks on companies such as Visa, MasterCard and PayPal, as well as others in the music industry and the Church of Scientology.

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

s.16(2)(c)

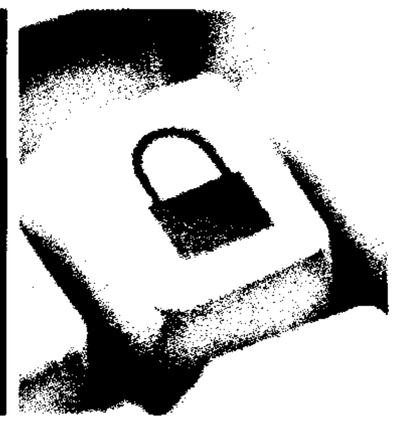
Public Safety Canada | Sécurité publique Canada

Canada

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-009



For the Week of 10 Dec – 16 Dec 2011

Issued: 22 Dec 2011

HIGHLIGHTS:

CCIRC Products: Two technical advisories were posted on Public Safety Canada's website.

- AV11-049: Microsoft Security Bulletin Summary for December 2011
- AV11-050: Security Update for Critical Vulnerabilities in Adobe Reader and Adobe

Notable Incidents:

- Malicious e-mails from threat actors impersonating prominent Canadian financial institutions, a telecommunications company and Canada Revenue Agency
- User account information for Canadian and US corporate, government, law enforcement as well as a Canadian university's users posted on the internet by hackers
- A telecommunications service provider experienced cyber-attack; over 200,000 affected in a Canadian province

International: Personal information for two US police departments' officers posted online

Vulnerability Warnings: Specific vulnerabilities of websites in the federal, provincial, food and education sectors were posted on the internet.

Noteworthy Open Source Reports:

- Hacker group posts online user account information for law enforcement, federal, military, loss prevention professionals and employees of certain large corporations
- DHS releases strategy to respond to cyber threats titled "Blueprint for a Secure Cyber Future: The Cyber security Strategy for the Homeland Security Enterprise"
- Report titled "Managing Automation Systems: Critical Infrastructure Operators' Challenges & Opportunities" released by Industrial Defender, a US company

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

CCIRC PRODUCTS: The following advisories were posted on Public Safety Canada's website:

- **AV11-049: Microsoft Security Bulletin Summary for December 2011.** This is a monthly summary of updates and information available to improve the security of certain Microsoft products. CCIRC reviews this information issued weekly by Microsoft, and summarizes the most critical ones for its stakeholder community.

- **AV11-050: Security Update for Critical Vulnerabilities in Adobe Reader and Adobe.** The purpose of this advisory is to bring attention to recently released security updates for Adobe Reader and Adobe Acrobat. Adobe software is extremely popular for publishing and reading documents in pdf format. This popularity makes it an attractive target for those who would wish to use these vulnerabilities to compromise users' computer systems. Organizations that use Adobe can improve their computer networks' security if they follow the recommended mitigation advice in accordance with this Advisory.

NOTABLE INCIDENTS– 10 DECEMBER THROUGH 16 DECEMBER 2011:

Canadian Critical Infrastructure:

Government and Safety. User account information for a law enforcement equipment website, including passwords, was posted on the internet. Users of these compromised accounts included employees of a Canadian federal department, certain Canadian, US and Australian law enforcement agencies, emergency services and a private security company. The impact is unknown.

Comment: CCIRC has seen law enforcement websites and computer systems become targets of hackers a number of times in 2011, with successful compromises in some cases. Some hackers post the information they've obtained on certain well-known websites for "bragging rights".

It's unlikely that this particular incident would have resulted in a compromise of the website users' computer systems. However, any number of threat actors could use the compromised account information to launch other malicious attacks on these users. These secondary attacks could indeed result in compromising these users' computer systems.

Financial Sector. Malicious e-mails from threat actors impersonating prominent financial institutions, including Canada Revenue Agency, were sent to computer users. CCIRC notified these institutions, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be identified as such, warning future unsuspecting users. The malicious sites are

hosted in United States, Russia and Canada. The site hosted in Canada is registered to an individual in China.

Telecommunications Sector. Malicious e-mails from threat actors impersonating a prominent telecommunications service provider were sent to computer users. CCIRC notified the provider, as well as Microsoft Smartfilter, Google and the Anti-Phishing Working Group, so the malicious sites can be marked as such and warn future unsuspecting users. The malicious site is in Brazil.

CCIRC also received a report that a telecommunications service provider experienced a distributed denial of service attack on a server which disabled web browsing for over 200,000 customers in a Canadian province. Over half of the users had their services restored in five hours, and the rest thereafter. The incident is being investigated by the company. No other company in that sector reported being affected by a similar attack, or seeing traffic related to that attack. Industry Canada, as the co-chair of the Canadian Telecommunications Cyber Protection (CTCP) group, is the federal government point of liaison on this matter.

Other Sectors:

CCIRC discovered that an online business directory website was defaced. CCIRC sent a notification and mitigation advice to the website owner's technical contact and to the internet service provider hosting the website.

A University's user was among the group whose user account was compromised in the incident described in the Government & Safety section earlier.

International: CCIRC that discovered hackers posted personal information belonging to officers of two US police departments, on the internet. This is in addition to the compromise of the law enforcement equipment website described in the Government & Safety section, which resulted in user account information being posted online for U.S. law enforcement agencies, as well as the Canadian and Australian ones.

VULNERABILITY WARNINGS: CCIRC discovered certain websites in the federal, provincial, food and education sectors were posted on a hacker website that specializes in advertising websites that are vulnerable to cross-site scripting (XSS) attacks. CCIRC notified the affected organizations and offered mitigation advice. The impact is unknown.

Comment: This type of vulnerability can be used to compromise a legitimate website, turning it into a malicious site. This then allows a threat actor to monitor a website visitor's computer activity, or even copy or delete files on the visitor's computer.

NOTEWORTHY OPEN SOURCE REPORTS:

- **Hacker posts online user account information for law enforcement, federal, military, loss prevention professionals and employees of some big corporations.** A hacker who claims to be part of Anonymous and Lulzsec, the famous hacking groups, compromised the website of the Coalition of Law Enforcement and Retail (CLEAR). This resulted in user account and personal information of website members being posted on the internet. Website members included over 2,400 U.S. law enforcement, federal, military, loss prevention professionals as well as employees of large corporations like Microsoft. The stated motive was revenge for police treatment of "Occupy Wall Street" protesters.

  Comment: The incident in this report is in addition to the compromises described earlier in this report but have a similar impact on website visitors. This was an SQL injection attack, which is common and effective because its prevention can be prohibitively resource intensive. CCIRC has issued a number of products over the years, which describe SQL injection attacks and offer mitigation advice.

- **20 Cybersecurity Objectives for DHS:** The US Department of Homeland Security released a strategy to respond to cyber threats, titled "Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise". This strategy for multiple stakeholders outlines 20 specific objectives for DHS under two major categories: protecting critical information infrastructure and the strengthening of the cyber ecosystem.

  Comment: This strategy has a similar approach to Canada's Cyber Security Strategy but goes one step further in defining more detailed objectives, and describing in more detail the role the federal government will play in strengthening cyber security in the U.S.

- **Managing Automation Systems: Critical Infrastructure Operators' Challenges & Opportunities.** Industrial Defender, a U.S. company that specializes in security & compliance for automation systems, published its recent survey of critical infrastructure professionals worldwide. Over 71% of respondents expect increased connectivity between corporate IT networks and the formerly isolated control environments. Managing the overlapping requirements of operations, security and compliance is proving particularly challenging in multi-vendor environments with assets from a mix of industrial automation suppliers.

  Comment: Critical Infrastructure stakeholders in Canada also have an increasing awareness of the importance of cyber security and form part of CCIRC's client base. They are also engaged by the federal government through public-private sector forums that have been set up as part of the Critical Infrastructure Action Plan in general, and by Public Safety Canada National Cyber Security Directorate, which includes CCIRC, specifically on cyber security.

UNCLASSIFIED
DRAFT

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-25-11 2:47 PM
To: Bendelier, Kenneth
Subject: Critical: Stratfort hacked by Antisec - here some specific comments from Anonymous

Importance: High

Generated by your Alert Subscription on Folder:
- Major Site Security Breaches - Hack / DDos Attacks
- Anonymous
- AnonOps - GeneralActions
Source: Zone-h
Complete item: http://zone-h.org/mirror/id/16416728

Description:
Original Stratfor site at http://stratfor.com/ is currently under mainteanace

Video and Text at hacked Stratfor site containing a message from Anonymous:
// OH STRATFOR. IF YOU ONLY KNEW WHAT ALL IS ABOUT TO GO DOWN.
// 'BUT WAIT', YOU ASK. 'IS THIS IT?' 0H N0, WE GOT MORE IN STORE...
// BUT FOR NOW, SOME INSPIRING WORDS OF WISDOM FROM IT MANAGER FRANK GINAC:

"You do realize how preposterous it is to suggest that stratfor simply shutdown completely for 2 days, right? The plan that you've attached paints a gloom and doom picture claiming no chance that such a move will succeed. Does that really seem a rationale conclusion?"

// YOU DONT EVEN KNOW THE EXTENT OF THE GLOOM AND DOOM WE HAVE PLANNED, FRANK

"Attended the TakeDownCon security conference. Focus of the conference was on wireless and mobile security. No vendors pushing product or service at this conference. Instead, great presentations by renowned white hat hackers (good hackers) and security experts. Bottom line is that no mobile platform is secure, including the Blackberry, but there are best practices that minimize the risk of their use within the enterprise. We will be incorporating these best practices in our operation over the coming months."

// INCORPORATING PRACTICES FROM "GOOD WHITE HAT HACKERS"? HOW'D THAT WORK OUT?

"It blew my mind to discover that our email server backups are being stored on the same physical server. I'm affectionately referring to these little discoveries as 'Mooney turds'."

// SO SAD WE RM'D YOUR MAIL SERVER AND ALL BACKUPS, FRANK

"Most if not all of us use professional and social networking sites like LinkedIn and Facebook. All offer levels of privacy ranging from wide open where everyone can see your profile, activities, and posts to closed allowing

only your immediate connections (or friends) access. As a private intelligence company we must all take extra care to protect our personal information from those who would use that information to exploit us personally or professionally. Although we don't have hard and fast rules on how to set your privacy settings nor do we restrict use of such sites, I suggest that you temper your need to share with prudence and consider the business that we are in. It's also important to check your privacy settings regularly to ensure that the sites you use haven't changed the meaning or scope of privacy settings -- we've all heard or read the news regarding this practice at Facebook. I suggest that you never include any information in your profile -- regardless of privacy setting -- that could be used to compromise your identity. Specifically, never include: your birth date, your exact street address (although this information can usually be found on the web quite easily), your cell phone number, SSN or other government issued ID number (that should be obvious), or any other information that someone could use to compromise your identity if your account were compromised."

// EVEN WITH ALL THE BEST SECURITY PRACTICES LEARNED FROM THE "RENOWNED WHITE // HAT HACKERS" WE STILL MANAGED TO STEAL ALL YOUR PERSONAL INFORMATION. UMAD?
//
// Frank Ginac CC Number: 376792323491009 Expiration: 5/2014

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-25-11 3:34 AM
To: Bendelier, Kenneth
Subject: Important: Stratfor hacked by Anonymous Hackers for AntiSec

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Hacker News
Complete item: http://thehackernews.com/2011/12/stratfor-hacked-by-anonymous-hackers.html

Description:
Stratfor who provides strategic intelligence on global business, economic, security and geopolitical affairs just now has been defaced by Anonymous Group of Hackers.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-24-11 12:55 PM
To: Bendelier, Kenneth
Subject: Important: New York City Public Advocate hacked and database dumped by anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
Source: cyberwar news
Complete item: http://www.cyberwarnews.info/2011/12/24/new-york-city-public-advocate-hacked-and-database-dumped-by-anonymous/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+cwn%2Fall+%28Cyber+War+News+-+All+Articles%29

Description:
Anonymous has been at it again obtaining more data from american government based websites. The site this time belongs to the Office of the New York City Public advocate and the hack was alerted to us via twitter from LuLzOps Account with a funny little message as well as flying it under the Anonymous and Antisec tags.

The leak which is a zipped SQL dump file contains pretty much the complete database for the website and can be found on filebeam.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-23-11 3:01 PM
To: Bendelier, Kenneth
Subject: Information: Tor anonymity will become illegal with SOPA acts ?

Generated by your Alert Subscription on Folder:
- Government US
Source: The Hacker News
Complete item: http://thehackernews.com/2011/12/tor-anonymity-will-become-illegal-with.html

Description:
The Stop Online Piracy Act (SOPA) is the newest attempt by Congress and corporations in the United States to regulate the Internet. SOPA's proponents include the Motion Picture Association of America and the Recording Industry of America. They view SOPA as a means to counter rampant piracy on the Internet, especially sites such as ThePirateBay.org.

A little-noticed section of the Stop Online Piracy Act could make it illegal to distribute Tor and other software that can circumvent attempts by the U.S. government to block pirate Web sites.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-23-11 2:07 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hackers Challenge U.S. Government With Occupy and OpBlackOut 'Protests'

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: ibtimes
Complete item: http://uk.ibtimes.com/articles/271377/20111222/anonymous-hackers-challenge-u-s-government-occupy.htm?

Description:
The hacker cell of Anonymous has issued a new call-to-arms against the U.S. government's "Stop Online Piracy Act" (SOPA), asking all Anons and Occupiers to join its OpBlackOut "protest."

Though announced several weeks ago, OpBlackOut is an active attempt by the collective to voice its disapproval of the U.S. government's SOPA act. Officially designed to combat online piracy, numerous groups have voiced concern about the new powers the act could grant U.S. law enforcement.

A recurring theme in the concerns is the suggestion that the act will allow police to arrest, fine and potentially jail individuals for seemingly minor offences, such as uploading a copyrighted video onto YouTube.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-23-11 12:31 AM
To: Bendelier, Kenneth
Subject: Important: Corporate fraud vs Anonymous Analytics Group

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Hacker News
Complete item: http://thehackernews.com/2011/12/corporate-fraud-vs-anonymous-analytics.html?utm_source=feedburner&utm_medium=twitter&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Daily+Cyber+News+Updates%29

Description:
A new financial research group, Anonymous Analytics has released a report accusing Chinese firm Chaoda Modern Agriculture of 11 years of deceit and corporate fraud. The company is one of Chinas largest fruit and vegetable suppliers. A faction within the online hacking collective Anonymous has moved into an unlikely new area exposing corporate fraud and making money in the aftermath.

The group alleges that Chaodas management has funnelled more than $400 million out of the company through false accounting and payments to shell companies. Hong Kongs government announced an investigation into the company on Monday, shortly before the release of the Anonymous report, leading its shares to fall by 26 per cent before being suspended from trading.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-22-11 10:26 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous faction in new attack on corporate fraud

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://www.realnews24.com/anonymous-faction-attack-corporate-fraud/

Description:
A faction within the online hacking collective Anonymous has moved into an unlikely new area exposing corporate fraud and making money in the aftermath. A new financial research group, Anonymous Analytics, has released a report accusing Chinese firm Chaoda Modern Agriculture of 11 years of deceit and corporate fraud. The company is one of Chinas largest fruit and vegetable suppliers.

The group alleges that Chaodas management has funnelled more than $400 million out of the company through false accounting and payments to shell companies. Hong Kongs government announced an investigation into the company on Monday, shortly before the release of the Anonymous report, leading its shares to fall by 26 per cent before being suspended from trading.

E-Secure-IT
https://www.e-secure-it.com

Dincoy, Rana

From: Bendelier, Kenneth
Sent: December-22-11 8:05 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description: **U.S. Chamber of Commerce details 'sophisticated' 6-month hacking of its computers.** "Hackers in China spent at least six months inside the computers of the U.S. Chamber of Commerce and can still break in despite a massive security update, the lobby group said Wednesday. The Chamber, which lobbies on behalf of almost all major U.S. corporations, described a "sophisticated" hacker attack. "This was clearly somebody very sophisticated, who knew exactly who we are and who targeted specific people and used sophisticated tools to try to gather intelligence," said David Chavern, chief operating office of the Chamber. The *Wall Street Journal* originally reported the security breach and said four Asia specialists at the 3-million-member Chamber were targets. At a daily news briefing in Beijing, foreign minister spokesman Liu Weimin called the report and the Chamber's response "baseless whipping up of so-called hacking. Chinese law bans hacking," Reuters News Agency reported."
Reference: http://www.thestar.com/news/article/1105272

2. Item Description: **Critical holes in Firefox, Thunderbird and SeaMonkey.** "Mozilla developers not only gave the Firefox browser a faster JavaScript engine with their update to version 9.0, but they also closed various critical security holes. One critical flaw in previous versions of the browser allows an embedded OGG video element of "extreme" size to cause a crash that can potentially be exploited to inject malicious code. However, Mozilla is currently keeping the specific details of this confidentially disclosed vulnerability a secret. Mozilla closed a hole that allowed attackers to access out-of-bounds memory areas and inject malicious code via specially crafted SVG files. Another critical issue addressed in Firefox 9.0 is a currently unspecified and potentially exploitable crash in the YARR regular expression library. Mozilla also took the opportunity in 9.0 to close other critical memory bugs. The vulnerabilities also exist in previous versions of SeaMonkey and are addressed in the Seamonkey 2.6 update. The Thunderbird e-mail client is vulnerable, but only the first vulnerability mentioned is rated as critical. Version 9.0 of Thunderbird will fix the issues but has not yet been released."
Reference: http://www.h-online.com/security/news/item/Critical-holes-in-Firefox-Thunderbird-and-SeaMonkey-1399340.html

3. Item Description: **Anonymous aims to make US Senators accountable for their votes.** "A group of Anonymous-affiliated hackers has made public a considerable amount of detailed personal information of the majority of the 86 US Senators that voted for the National Defense Authorization Act (NDAA). The Pastebin entry includes information such as dates of birth, spouse and children names, addresses, phone numbers, Twitter accounts, memberships in various committees, information about education, profession and religion, their staff, previous votes on a number of issues, their campaign contributors, suites filed against them, and more. The hackers don't claim to have stolen the information following a breach, and the document seems to have been compiled from information collected from a variety of sources accessible to the public."
Reference: http://www.net-security.org/secworld.php?id=12125

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-22-11 4:55 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous: A Modern Day Robin Hood?

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Word Press
Complete item: http://silvertailsystems.wordpress.com/2011/12/20/anonymous-a-modern-day-robin-hood/

Description:
According to SC Magazines Dan Raywood, the hacktivist group Anonymous has announced its intention to steal from banks and bring happiness and gratitude to families around the globe with a new campaign called DestructiveSec.

This is a classic Robin Hood scenario stealing from the rich and giving to the poor but the fact that this campaign is being called DestructiveSec is a clear indication that this isnt a heroic action by any means. As weve seen from the data breaches in 2011, its apparent that attacks will become more prevalent as time goes on and organizations need a better way to protect themselves and their counterparts. Various hacking groups around the world are infiltrating computer networks and web properties to expose data, which is ultimately a sign of poor security compliance.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-22-11 2:22 AM
To: Bendelier, Kenneth
Subject: Important: Words of Anonymous

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: Various Sources
Complete item: http://summify.com/story/TvENEy7Xr1SmB1Rz/anoncentral.org/2011/12/words-of-anonymous/?utm_campaign=share&utm_medium=general&utm_source=share

Description:
Gentlemen. We face a threat the likes of which weve never seen. We have only one hope. We must undo decades of divide between the right and the left, using SOPA and NDAA as a rallying cry. The conservatives are livid, as are the liberals. We will manage this by going to every conservative and liberal board we can and forming a new movement combining the best of OWS and the tea party. This will function within the confines of the law with behavioral guidelines. No drum circles, drugs or deliberately fucking with the cops.

That accomplished nothing. Let them face a united America with the left and right standing side by side. We wont find common ground on every issue, but we have enough in common, thanks to these egregious actions by the federal government, to work from.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-22-11 1:57 AM
To: Bendelier, Kenneth
Subject: Important: Arizona Opposition to NDAA 2012 : The Anonymous American Info War Begins

Generated by your Alert Subscription on Folder:
- Government US
- Cyberwar / Cyber conflict / Cyber war
- Anonymous
Source: EXAMINER
Complete item: http://www.examiner.com/paganism-in-phoenix/arizona-oppostion-to-ndaa-2012-the-anonymous-american-info-war-begins

Description:
The National Defense Authorization Act of 2012 is being called the most serious violation of the first Amendment in American history. It follows in suit with the passing of the following legislation. The Stop Online Piracy Act, or (SOPA) and its sister the Protect IP Act of 2011. President Obama even signed it into action, he said he would veto the NDAA 2012 document. He promised many this, all the way until this week.

SOPA act will censor you from accessing certain websites and block all access to other areas of the internet that the United States government does not want you to access.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-22-11 1:09 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hackers Publish Info on U.S. Senators

Generated by your Alert Subscription on Folder:
- Anonymous
Source: eSecurity Planet
Complete item: http://www.esecurityplanet.com/hackers/anonymous-hackers-publish-info-on-u.s.-senators.html

Description:
Members of Anonymous recently leaked personal information on U.S. Senators who had voted in favor of the National Defense Authorization Act (NDAA).

"The large document starts with Republican Senator from the state of Ohio, Robert J. Portman," writes Softpedia's Eduard Kovacs.

"'He has made himself a target as an advocate of the NDAA, but we are truly disturbed by the ludicrous $272,853 (190,000 EUR) he received from special interest groups supporting the NDAA bill that authorizes the indefinite detention of U.S. citizens on U.S. soil. Robert J. Portman, we plan to make an example of you,' said the hackers in a statement," Kovacs writes.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-21-11 2:22 PM
To: Bendelier, Kenneth
Subject: Important: Iowa Republicans concerned about apparent hacker threat from Anonymous group

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: New York Daily News
Complete item: http://www.nydailynews.com/news/politics/iowa-republicans-concerned-apparent-hacker-threat-anonymous-group-article-1.994192

Description:
Taking seriously an apparent threat from a notorious collective of computer hackers, the Iowa Republican Party is boosting the security of the electronic systems it will use in two weeks to count the first votes of the 2012 presidential campaign. Investigators don't know if the threat is authentic, but it has nonetheless led the state party to confront a worst-case scenario. Their fear: an Iowa caucus marred by hackers who corrupt the database used to gather votes and crash the website used to inform the public about results that can shape the campaign for the White House.

"With the eyes of the media on the state, the last thing we want to do is have a situation where there is trouble with the reporting system," said Wes Enos, a member of the Iowa GOP's central committee and the political director for Minnesota Rep. Michele Bachmann's campaign in the state. "We don't want that to be the story."

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-21-11 9:17 AM
To: Bendelier, Kenneth
Subject: Important: In response to SOPA, Anonymous hackers target US government

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: globalpost
Complete item: http://www.globalpost.com/dispatch/news/regions/americas/united-states/111216/anonymous-hackers-sopa-vote-congress

Description:
In response to a bill now before Congress, which opponents say would dramatically erode internet freedom, the free and fair use of copyrighted material and online privacy, hacker groups have begun to publicly threaten to launch attacks on US government workers and websites.

The US House Judiciary Committee debated for a second day on Friday the Stop Online Piracy Act (SOPA), a bill that would bestow the US Department of Justice and individual copyright holders with unprecedented powers to shut down websites and crack down on users for what they deem to be violations of copyrights.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-21-11 9:06 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous: We're Stealing Credit Cards, Funds From Banks for Christmas

Generated by your Alert Subscription on Folder:
- Anonymous
Source: EWeek
Complete item: http://www.eweek.com/c/a/Security/Anonymous-Were-Stealing-Credit-Cards-Funds-from-Banks-for-Christmas-620758/

Description:
In a twisted attempt to play Robin Hood, some Anonymous members say they are hacking into banks to buy items such as iPhones, iPads and iPods requested by random people.

Hacktivist collective Anonymous has announced a new campaign for the holiday season: to steal from the rich.

Dubbed "DestructiveSec," the collective said it will steal virtual credit cards from banks and give "back to the people who had everything taken," according to a statement posted on text-sharing site Pastebin on Dec. 12. The statement did not name any targets or provide any details.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-21-11 8:56 AM
To: Bendelier, Kenneth
Subject: Information: Hacker Group "Anonymous" Threatens to Take Down Iowa Caucuses

Generated by your Alert Subscription on Folder:
- Anonymous
Source: the new american
Complete item: http://www.thenewamerican.com/usnews/politics/10258-hacker-group-qanonymousq-threatens-to-take-down-iowa-caucuses

Description:
As GOP presidential contender Ron Paul is increasingly becoming a threat to the establishment and to big government advocates on both ends of the political spectrum, some members of his opposition are preparing dirty tactics to thwart him. The secretive hacker group Anonymous, for instance, has already vowed to disrupt the January 3 vote in the Iowa caucuses, which Paul seems poised to win.

Though Paul was initially almost wholly ignored by most politicians and the mainstream media, and treated as though he was a fringe, unviable candidate, he has surged in popularity in poll after poll. Now ignoring him is no longer an option.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-21-11 8:50 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Responds to SOPA: We'll Deface The Internet In Protest

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: The Next Web
Complete item: http://thenextweb.com/shareables/2011/12/20/anonymous-responds-to-sopa-well-deface-the-internet-in-protest/

Description:
The Stop Online Piracy Act (SOPA) is a bill that was introduced in the United States House of Representatives on October 26, 2011, by Texan Republican Representative Lamar Smith and a bipartisan group of 12 initial co-sponsors.

The bill, which we describe in great detail here, could signal the end of the Internet as we know it. Its chock full of loose political language thats open to interpretation in the worst way. It essentially expands the ability of U.S. law enforcement and copyright holders to fight online trafficking in copyrighted intellectual property and counterfeit goods.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-21-11 8:45 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous aims to make US Senators accountable for their votes

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: Net-Security
Complete item: http://www.net-security.org/secworld.php?id=12125

Description:
A group of Anonymous-affiliated hackers has made public a considerable amount of detailed personal information of the majority of the 86 US Senators that voted for the National Defense Authorization Act (NDAA).

The Pastebin entry includes information such as dates of birth, spouse and children names, addresses, phone numbers, Twitter accounts, memberships in various committees, information about education, profession and religion, their staff, previous votes on a number of issues, their campaign contributors, suites filed against them, and more.

E-Secure-IT
https://www.e-secure-it.com

Anderson, Windy

From: Anderson, Windy
Sent: December-20-11 9:32 AM
To: Dick, Robert; Hatfield, Adam; Durand, Stéphanie; Weir, Sarah; Anderson, Windy
Subject: FW: follow-up meeting on CCIRC with Comms
Attachments: PS-SP-#522113-R-CCIRC_-_policy_-_Cyber_Awareness_Products_-_details_for_coms_-_November_23__2011.PPT.DRF; PS-SP-#522113-2-CCIRC - policy - Cyber Awareness Products - details for coms - November 23, 2011.PPT

I am sending this information again as we are now closer to the actual meeting (tomorrow).

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

From: Anderson, Windy
Sent: December-02-11 9:52 AM
To: Dick, Robert; Hatfield, Adam; Durand, Stéphanie; Weir, Sarah
Subject: RE: follow-up meeting on CCIRC with Comms

Hi all,

Here is the updated version of our products and clients. I have put both the RDIMS version and a copy (in case you do not have access to the RDIMS version). Please let me know if you require any additional information.

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

From: Dick, Robert
Sent: December-01-11 4:46 PM
To: Anderson, Windy; Hatfield, Adam; Durand, Stéphanie; Weir, Sarah
Subject: follow-up meeting on CCIRC with Comms

I would like to propose that we follow up with a meeting later in the week after next. Sarah will arrange.

Recall that were going to have the following information available, in advance if possible:

- Adam, with Windy: proposed triggers / thresholds for reporting up. Adam, suggest you take a look at the UK incident management doc. Copy on high side from Luc.
- List of people receiving various products, sorted appropriately (Windy)

We would also like to discuss branding for CCIRC – whether / how to proceed.

We will also update on portals.

Robert

Robert Dick
Director General | Directeur général
National Cyber Security | Cybersécurité nationale
Robert.Dick@ps-sp.gc.ca
613-990-2661 fax: 613-990-3287

CCAP: CCIRC Cyber Awareness Products

BUILDING A SAFE AND RESILIENT CANADA

Currently Produced | In Development

Product	Flash	Daily Report	Weekly Technical Report	Information Notes	Technical Report	Advisory	Monthly Statistical Report	Weekly SA Report	Monthly SA Rollup*	Issue of the Month	Annual Report	Ad hoc*
Description	Time sensitive reports for immediate security issues ➢ Security fix unavailable	Daily situation report	Summary of daily reports, CCIRC products / events / activities / indicators / and cyber reporting	Report on significant cyber events ➢for general awareness	Detailed report WRT a cyber security issue ➢Ad hoc	Cyber security advisory on threat and vulnerability ➢ Security fix available	All CCAP products + (1) incidents handled ; (2) take down requests; and (3) victim notifications	Notable cyber events / CCIRC products / open source reports	Summary of weekly SA reports for ADM	Single strategic cyber issue analysis	Yearly status report WRT Canadian cyber security	Strategic cyber issue 1 pagers
Clients	P/T/CI operational contacts	CCIRC / trusted GoC partners	P/T/CI/GoC operational contacts	P/T/CI/GoC ➢Posted on website	P/T/CI operational contacts	P/T/CI operational contacts ➢Posted on website	Public Safety /other Federal departments	GoC managers / executives P/T/CI partners	Public Safety / Senior GoC executives	P/T/CI partners	Public	Public Safety
Release Authority	CCIRC Chief, Operations	CCIRC Chief, Operations	CCIRC Chief, Operations	CCIRC Chief, Operations	CCIRC Chief, Operations	CCIRC Chief, Operations	CCIRC Director	CCIRC Chief, Strategic Initiatives	NCSD Director General	CCIRC Director	ADM NS or Public Safety Minister	NCSD Director General

* Secret

Operational / Technical | Strategic

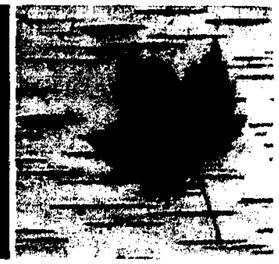
Public Safety Canada | Sécurité publique Canada

Nate Klassen (991-6052)

00708

Detailed Descriptions

Currently Produced Products



BUILDING A SAFE AND RESILIENT CANADA

Product	Description
Flash	Flashes are time sensitive and describe an immediate or active security issue. They are also used to raise awareness of recently identified cyber threats that may impact F/P/T/CI assets. Unlike Advisories, Flashes are not publicly posted. As such, they are ideal for raising awareness and providing detection and mitigation advice, while avoiding unwanted publicity. ➢Examples include: (1) Warnings of imminent threats against F/P/T/CI networks; (2) zero day vulnerability alerts; and (3) advance notification of important patches.
Daily Report	This brief is a daily situation report, which includes: (1) events and actives that are currently being actionned by CCIRC; (2) publicly reported vulnerabilities and threats; (3) noteworthy news items; (4) information from international partners; and (5) a summary of CCIRC products. All events and activities are sanitized (i.e. made anonymous).
Weekly Technical Report	The Weekly Technical Report is geared for the technical F/P/T/CI community. It is a summary of the past week's daily reports along with more technical information.
Information Notes	Information notes are used to draw attention to: (1) changes in CCIRC policy or procedures; and (2) a significant cyber issue. ➢Examples include: (1) notifications of new security tools; and (2) upcoming CCIRC events.
Technical Report	Technical reports explain the technical and operational details of a cyber event impacting F/P/T/CI networks.
Advisory	Advisories communicate security update information regarding vulnerable software. These vulnerabilities could possibly impact F/P/T/CI assets. As such, Advisories may contain information describing the vulnerabilities and informing that updated software has now been made available by the vendor to correct these deficiencies.

Page 710

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

CCIRC Clients

Sector	Client Details	Clients
Government	➢**Federal** – CSEC, RCMP, CSIS, DND ➢**Provincial** – AB, BC, MB, NB, NL, NT, NS, NU, ON, PE, QC, SK, YT ➢**Municipal** – ON, BC, AB	71
Finance	➢**Banks** – Canadian Bankers Association (Canadian bank's focal point), ➢**Financial** – CRA, TBS, OSFI, FINTRAC, CDIC,	30
Energy / Utilities	➢**Energy** – NRCan, NEB, CNSC, Canadian Association of Chemical Distributors, Chemical Industry Association of Canada, Canadian Association of Petroleum Producers, ➢**Utilities** – Canadian Electricity Association – Critical Infrastructure Protection Working Group,	47
Telecom	➢Industry Canada, CRC, CIRA, Canadian Wireless Telecommunications Association,	22
Other Critical Infrastructure Sectors	➢**Transport** ➢**Manufacturing** ➢**Information and Communication Technology** ➢**Education** ➢**International**	28
Total		**198**

* CCIRC focuses on the Finance, Energy / Utility, and Telecom Sectors. With more resources, outreach to the other critical infrastructure sectors could be expanded.

Williston, Sandra

From: Beaudoin, Luc S
Sent: December-20-11 8:26 AM
To: Cameron, Bud; Bendelier, Kenneth; Anderson, Windy
Subject: Re: Anyone ever hear of the RCMP's NCSI?

Probably dave black fusion centre

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: Cameron, Bud
Sent: Tuesday, December 20, 2011 08:21 AM
To: Bendelier, Kenneth; Beaudoin, Luc S; Anderson, Windy
Subject: RE: Anyone ever hear of the RCMP's NCSI?

http://www.rcmp-grc.gc.ca/nsci-ecsn/index-eng.htm

From: Bendelier, Kenneth
Sent: December-19-11 1:54 PM
To: Cameron, Bud; Beaudoin, Luc S; Anderson, Windy
Subject: Anyone ever hear of the RCMP's NCSI?

Credible sources in the
open media have written extensively on the
cyber attacks targeting Finance Canada and
the Treasury Board of Canada Secretariat.
The newly-established RCMP NSCI Cyber
Unit, in partnership with Technological Crime
Branch, reviews cyber incidents reported to
the RCMP for potential criminality. RCMP
NSCI has noted cases involving suspected
foreign intrusion and decentralized cyber
threats (such as ANONYMOUS), either
threatening or actually targeting the cyber
networks of critical infrastructure in the
Canadian Energy, Finance, Government, and
Manufacturing sectors.

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-20-11 1:21 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous takes down Egyptian Websites

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: cyberguerrilla
Complete item: http://www.cyberguerrilla.info/?p=3474

Description:
The hacktivist group Anonymous has taken credit for the attack on at least one Brazilian Operations page. The hackers claim the attacks are in response to the brutal treatment of protesters in the country. The hashtags #Egypt #Solidarity #Anonymous #CabinCr3w were used repeatedly on twitter as the event was being reported live, followed by the familiar phrase, Tango Down. The phrase was used by hackers before after defacing the CIAs website.

Footage was released yesterday that showed images of Egyptian military police firing lethal ammunition into crowds of people. Some officers chased down a woman, beating her repeatedly in the middle of the street.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-20-11 12:48 AM
To: Bendelier, Kenneth
Subject: Important: Top tech stories of 2011: From Jobs to Android, Anonymous to Egypt

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: Computer World
Complete item:
http://www.computerworld.com/s/article/9222632/Top_tech_stories_of_2011_From_Jobs_to_Android_Anonymous_to_Egypt?taxonomyId=17

Description:
In 2011, the increasingly mobile and socially networked world of technology became more intertwined than ever with politics and the law. Patent wars shaped competition in tablets and smartphones, hacktivists attacked a widening array of political and corporate targets, repressive regimes unplugged citizens from the Internet, and the U.S. government moved to block the giant merger of AT&T and T-Mobile USA. With the passing of Steve Jobs, the world lost a technology icon who redefined the computer, entertainment and consumer electronics industries. These are the IDG News Service's picks for the top 10 technology stories of the year:

-- The PlayStation Network hack, Anonymous and the rise of hacktivism

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-19-11 10:54 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous Upcoming US Operations, Impact, and Likelihood

Generated by your Alert Subscription on Folder:
- Anonymous
Source: cyberguerrilla
Complete item: http://www.cyberguerrilla.info/?p=3469

Description:
Though the protests will likely to be peaceful in nature, like any protest, malicious individuals may use the large crowds as cover to conduct illegal activity such as vandalism. Judging based on past behaviors by the group, Anonymous participation in these protests may include malicious cyber activity, likely in the form of DDOS attacks targeting financial institutions and government agencies.

E-Secure-IT
https://www.e-secure-it.com

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-19-11 8:09 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
December 19, 2011 / le 19 décembre 2011

Online media

Parliament site zapped by botched IT upgrade
The Parliament of Australia website, aph.gov.au, was down from Saturday until about lunchtime today due to a botched maintenance upgrade. Alan Thompson, secretary of the Department of Parliamentary Services, said the specific cause of the failure was still a mystery but there was no external attack on the aph.gov.au site. Sydney Morning Herald

Dark side of Net continuing threat to cyber security
Readers get a peek into the dark side of the Internet in this interesting wake-up account of online crime. British journalist Misha Glenny recounts how mostly young, computer-savvy men organized themselves over the worldwide web between 2002 and 2008 to siphon untold millions of dollars from ordinary people through massive credit card fraud and hacking schemes. DarkMarket was the site criminal hackers created to sell skimming machines, pinhole cameras, viruses and stolen credit card and bank account data. It was a members-only club with entry conferred on those approved by wary website administrators always on the lookout for police infiltration. To overcome language barriers they communicated in Globish, a bastardized form of English that changed constantly. Winnipeg Free Press

Hackers invade servers of Indian embassy in Paris
Anonymous cyber hackers allegedly invaded the servers of the Indian embassy office in Paris and walked away with loads of official documents last month. The hackers later posted all the files, including a proposal to rope in Airbus for the indigenous manufacturing of civilian aircraft and visits of senior bureaucrats, ministers and intelligence officials to France, on a website to show how vulnerable the servers are. The hacker on the post claimed these files were stored on computers within the ministry of external affairs' servers worldwide. The government agencies have now launched an investigating into the matter. India Today

La Chine a piraté des dizaines de milliers d'emails d'entreprises occidentales
Dans le monde de l'intelligence économique mondial, tous les yeux sont braqués sur la Chine. Et pour cause: elle est accusée d'espionnage économique. Les victimes principales? Des milliers d'entreprises occidentales. Dotés d'une mine d'or de données relative à la propriété intellectuelle, Google et Intel ont été les principales victimes. Des cibles de choix, pour les hackers situés en Chine, à en croire la cyberattaque dont à été victime IBahn, un prestataire de service internet à destination des hôtels. atlantico; Déplacement Pros

Le cyberespionnage, une arme militaire et économique
Mobilisation générale dans le cyberespace. Ministères, agences gouvernementales, états-majors, mais aussi industriels et prestataires de tous types ont, ces derniers mois, investi de façon significative la cybersécurité et la cyberdéfense. "Nous cherchons où couper dans nos budgets, mais s'il est un domaine pour lequel je suis sûre que nous aurons une progression, c'est celui du cyber", nous a indiqué la secrétaire américaine à la sécurité intérieure, Janet Napolitano, le 2 décembre, à Paris. Pour elle, "le cyberespace est l'endroit où nos intérêts économiques et nos intérêts sécuritaires

peuvent coïncider". En raison de leur sophistication, des attaques récentes sont prises en exemple par les décideurs pour justifier cet effort. Le Monde

Iran boosts cyber war capabilities
Iran has invested $1 billion to boost its offensive and defensive cyber warfare capabilities, The Jerusalem Post said. The Islamic Republic has been plagued with a number of cyber attacks in recent years, including the Stuxnet virus, which is believed to have destroyed 1,000 centrifuges at the Natanz enrichment facility, the daily said Sunday. A new virus called Duqu was recently detected in Iran's computer systems, but the extent of damage is unknown, the newspaper said. Iran's deputy Energy Minister Mohammed Behzad Saturday said electricity production is set to double at the Bushehr nuclear plant, Press TV said. Behzad told the Mehr news agency that the plant is expected to reach the capacity of 1000 megawatts by the end of March 2012. UPI

Fake Gift Cards Masquerading Amazon Traps Users in Scam
Festive season is associated with the gesture of generosity. Taking advantage of this tradition and attacking the expectation of people, scammers have regulated one more phishing campaign in air, as revealed by the security firm AppRiver. The messages are targeting Amazon as evident from the [Gift_Card(dot)exe] attached in the mail. A well planned fake message integrated Trojan downloader that belong "Yakes" (also known as Dofoil).belonging to the virus. A catchy subject line "Your gift card order" is enough to attract recipients to open the mail and further it also entails them with the information that they have received a gift card worth $250, which is valid till December 7. It urges the recipients to take the full advantage of the offer as the shipment will be totally free of cost. The offer of the gift card is totally fraudulent and a click on the fake link in anticipation of the offer, invites the installation of Trojan downloader in their computer. SPAM Fighter

Latest spam campaigns delivering the Zbot Trojan
For a while now, fake messages and warnings from USPS, FedEx and DHL about supposedly undelivered packages have been hitting inboxes, and users have been getting wiser about the danger lurking behind the offered links and attachments. Trying to mix it up and catch the users unawares, Zbot peddlers have put a break on the aforementioned campaigns and have rolled out new ones, with emails offering prepared bills, business meeting notes and payment confirmations. Help Net Security

Malware authors rush to release Java exploit packs
Shift in tactics to getting new exploit kits out quickly could be disastrous for unpatched systems. Researchers at M86 are warning that exploits for a recently-discovered Java vulnerability are already available in the wild, meaning cyber criminals could target unpatched systems. The security firm also warned that this news shows authors are getting much faster at updating their exploit kits when new vulnerabilities are discovered. While it used to take authors a month or more, some authors are now updating their kits before a patch has even been released. Although a patch has been released to fix the Java vulnerability any unpatched systems are still at risk, M86 warns. CBR Online

Dorkbot Malware Continues To Spread On Facebook
Reports have emerged concerning a new worm infiltrating Facebook user accounts by posing as a link sent by compromised friends. According to Security company, Sophos, the malicious worm is continuing to spread through Facebook chat. The company said that the malware disguises itself as a link pretending to point to an image of two women, but, if clicked, it instead launched a malicious screensaver which then ran a code to download further malware. Tech Week Europe

Fresh Phishing E-mail Scam yet again Attacks Gmail Users
According to security researchers, one fresh phishing e-mail posing as a message from Google Mail to its users is presently circulating online, thus published Tech2.in.com dated December 9, 2011. The fake e-mail captioned "Google Account Storage Quota Exhausted on ******@gmail.com," may at a glance appear authentic. The sender's id, which shows no_reply@qmail.com, has alphabets depicted differently that initially can't be detected since the name displays 'Accounts Support,' while within brackets lies the original e-mail. Moreover, similar to a typical e-mail, this particular message lands inside the victim's Gmail account. Additionally, citing Google's mail record, the phishing electronic mail tells the recipient that there isn't enough storage space with ****@gmail.com, therefore, since Google Inc. aims at providing quality service, it suggests users to adopt an upgrade. But for that, they require clicking a given web-link that'll help upgrade the storage space of their Google accounts as also not cause them any difficulty in exchanging e-mails while facilitating them in utilizing other Google features too via ****@gmail.com, the e-mail concludes. SPAM Fighter

Sécurité des Systèmes de contrôle industriels : recommandations pour l'Europe est les États-membres
L'ENISA, l'Agence européenne de cyber-sécurité, a publié aujourd'hui les résultats d'une étude sur la sécurité des Systèmes de contrôle industriels (SCI). Le rapport décrit la situation actuelle de la sécurité des SCI et propose sept recommandations pour l'améliorer. Generation NT

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-19-11 1:23 AM
To: Bendelier, Kenneth
Subject: Information: Anonymous Retaliates: Massive Information dump released on Senators who Passed NDAA

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://freakoutnation.com/2011/12/17/anonymous-retaliates-massive-information-dump-released-on-senators-who-passed-ndaa/

Description:
This years National Defense Authorization Act passed quickly through the Senate and as expected President Obama signed the bill. 86 Senators in a bipartisan move, signed off on this controversial bill, which opens the door to invasive acts against Americans. Almost everyone has felt the effect of Anonymous presence online and off and now, the 86 Senators will feel their ubiquitous presence as well.

The collective activist group just released a massive dump of information, which begins with, Robert J. Portman is a Republican Senator from the state of Ohio.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-18-11 12:28 AM
To: Bendelier, Kenneth
Subject: Important: USA: Massive Anonymous USA Crook Leak!!

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: Various Sources
Complete item: http://www.occupythebanks.com/2011/12/usa-massive-anonymous-usa-crook-leak.html?utm_medium=twitter&utm_source=twitterfeed

Description:
This is a most interesting pastebin we just came across; do note the case-file reference, etc, and see our last post. We're not connecting any dots here AT ALL (that should be taken literally). But Americans might once they understand just what's been going on in the covert (from Americans) war of this past decade, which has now found it's way home, at least smell the roses, and listen up next time the world spends a decade telling them their country has been taken over by BANKSTERS. Next time America, perhaps when the world tells you your government has gone south, it won't take Anons to prove it. ;)

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-17-11 12:52 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous declares war on Congress with #OpAccountable

Generated by your Alert Subscription on Folder:
- Government US
- Cyberwar / Cyber conflict / Cyber war
- Anonymous
- AnonOps - GeneralActions

Source: Rawstory
Complete item: http://www.rawstory.com/rs/2011/12/16/anonymous-declares-war-on-congress-with-opaccountable/

Description:
The National Defense Authorization Act for 2012 has been assailed by civil libertarians for its provisions which allow for the indefinite detention of American citizens without trial. Now the hacktivist collective Anonymous has joined the battle in its own distinctive manner, declaring war on the members of Congress who voted for the legislation under the operation name #OpAccountable. This is an open letter to the US leaders, the operation wrote in a document released on Friday, which cited both the NDAA and attempts to pass so-called anti-piracy legislation that critics fear would amount to preemptive censorship of the Internet.

We have watched as you have violated the very laws that guarantee your power. We have witnessed your fall from Representatives of the People to Representatives of Greed and Corruption. Weve been watching you systematically destroy the rights of your own people, one law at a time.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-17-11 6:35 AM
To: Bendelier, Kenneth
Subject: Information: Operation Green Rights - Anonymous Message

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - Green Rights
Source: Blogspot
Complete item: http://operationgreenrights.blogspot.com/2011/12/comunicado-iberoamerica.html

Description:
This time we are addressing to you as speakers of all of those who suffered injustice, indifference and the consequence of lack of ethical principles; In a world where the power of money can buy the blodiversIty of fragile ocosystems.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-16-11 11:33 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous attacking creators of indefinite detention bill

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: circleof13
Complete item: http://circleof13.blogspot.com/2011/12/anonymous-attacking-creators-of.html

Description:
With President Obama read to sign away the freedoms of Americans by inking his name to the National Defense Authorization Act for Fiscal Year 2012, opponents are already going after the lawmakers that made the legislation possible.

The act, abbreviated as NDAA FY2012, managed to make its way through Congress with overwhelming support in recent days, despite legislation that allows for Americans to be detained indefinitely and tortured by authorities for the mere suspicion of committing a belligerent act." The Obama administration originally decreed that they would veto the bill, only for the White House to announce a change of heart on Wednesday this week.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-16-11 11:30 PM
To: Bendelier, Kenneth
Subject: Information: Operation Green Rights Press Release by Anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - Green Rights
Source: You Tube
Complete item: http://www.youtube.com/watch?v=_jlmI6yTw-4

Description:
#Operation Green Rights Press Release by Anonymous

More Information:
http://www.youtube.com/watch?v=_jlmI6yTw-4

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-16-11 11:24 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous: SOPA passed. We are displeased

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: You Tube
Complete item: http://www.youtube.com/watch?v=qeEcoi8kEuU

Description:
Citizens of the United States.

We are ANONYMOUS.

There is a new bill that the United States government has successfully passed. It is called the Stop Online Piracy Act, or (SOPA) for short. Also known as The Protect IP Act of 2011. The US Congressional Budget Office estimates that implementation of the bill would cost the federal government 47 million dollars through 2016. Translated into plain english, It will cost tax payers 47 million dollars over the next 4 years.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-16-11 11:22 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous declares cyber war on Congress over indefinite detention act

Generated by your Alert Subscription on Folder:
- Government US
- Cyberwar / Cyber conflict / Cyber war
- Anonymous
Source: RT
Complete item: http://rt.com/usa/news/anonymous-congress-ndaa-sopa-013/

Description:
Hacktivists are continuing their mission to take on politicians causing the collapse of constitutional rights in America, with operatives from the online collective Anonymous keeping up a campaign against the signers of controversial legislation.

As RT reported on Thursday, members of Anonymous began a campaign this week to expose information on the lawmakers who voted in favor of the National Defense Authorization Act for Fiscal Year 2012, a bill that will allow for the indefinite detention of American citizens, the reinstating of torture methods and the creation of the United States as a battlefield.

E-Secure-IT
https://www.e-secure-it.com

St-Louis, Danielle

From: St-Louis, Danielle
Sent: December-16-11 12:08 PM
To: [redacted] Champoux, Martin; Coady, Therese; Danaitis, Algis; Dick, Robert; Dole, Natalie; Dvorkin, Corey; Hatfield, Adam; Labelle, Sébastien; Panchyson, Dorian; Selman, Semira
Subject: CCIRC WEEKLY SUMMARY FOR WEEK OF 05 DEC
Attachments: PS-SP-#527919-v1-FEEDBACK_FORM_FOR_WEEKLY_SUMMARY_FOR_EXECS.DOC; PS-SP-#534275-v4-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_5_DEC_2011-TO_SEND_OUT.DOC

Good afternoon,

please find attached the CCIRC Weekly Summary of significant cyber events and incidents reported to and observed by CCIRC, with analysis where required. Please note this product is *not* intended for wide circulation since it is still in the pilot phase. Here are the highlights:

HIGHLIGHTS:

Threat Warnings: Nothing significant to report.

CCIRC Products: CCIRC sent the following Cyber Flashes to stakeholders.

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
- CF11-026: Widespread SQL injection campaign
- CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

Incidents to report:

- Malicious e-mails from threat actors impersonating a Canadian federal agency, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems in the provincial government, financial, health, telecommunications and education sectors
- SQL injection attacks infected thousands of legitimate websites around the world, resulting in re-direction of internet users to a malicious websites. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

Noteworthy Open Source Reports:

- A draft US Bill in cyber security gets support from privacy proponents

- White House announces cloud security "rules of the road" for US federal agencies and contractors

- Hacker groups successfully attack websites of the Portuguese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca <mailto:bud.cameron@ps-sp.gc.ca> .

Danielle St-Louis
Administrative Assistant | Adjointe administrative Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: 613-991-7738 Fax | Téléc.: 613-996-0995 E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca
<blocked::mailto:danielle.st-louis@ps-sp.gc.ca>

Dincoy, Rana

From: St-Louis, Danielle
Sent: December-16-11 12:09 PM
To: [redacted]Champoux, Martin; Coady, Therese; Danaitis, Algis; Dick, Robert; Dole, Natalie; Dvorkin, Corey; Hatfield, Adam; Labelle, Sébastien; Panchyson, Dorian; Selman, Semira
Subject: CCIRC WEEKLY SUMMARY FOR WEEK OF 05 DEC
Attachments: PS-SP-#527919-v1-FEEDBACK_FORM_FOR_WEEKLY_SUMMARY_FOR_EXECS.DOC; PS-SP-#534275-v4-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_5_DEC_2011-TO_SEND_OUT.DOC

Good afternoon,

please find attached the CCIRC Weekly Summary of significant cyber events and incidents reported to and observed by CCIRC, with analysis where required. Please note this product is *__not__* intended for wide circulation since it is still in the pilot phase. Here are the highlights:

HIGHLIGHTS:

Threat Warnings: Nothing significant to report.

CCIRC Products: CCIRC sent the following Cyber Flashes to stakeholders.

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
- CF11-026: Widespread SQL injection campaign
- CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

Incidents to report:

- Malicious e-mails from threat actors impersonating a Canadian federal agency, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems in the provincial government, financial, health, telecommunications and education sectors
- SQL injection attacks infected thousands of legitimate websites around the world, resulting in re-direction of internet users to a malicious websites. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

Noteworthy Open Source Reports:

- A draft US Bill in cyber security gets support from privacy proponents
- White House announces cloud security "rules of the road" for US federal agencies and contractors
- Hacker groups successfully attack websites of the Portuguese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

Danielle St-Louis
Administrative Assistant | Adjointe administrative
Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: 613-991-7738 Fax | Téléc.: 613-996-0995
E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-16-11 10:40 AM
To: Bendelier, Kenneth
Subject: Information: Anonymous - #OpRobinHood (video)

Generated by your Alert Subscription on Folder:
- Anonymous
Source: YouTube
Complete item: http://www.youtube.com/watch?v=NEQ9RhzQ6vg

Description:
Anonymous - #OpRobinHood (video).

E-Secure-IT
https://www.e-secure-it.com

Dincoy, Rana

From: Dincoy, Rana
Sent: December-16-11 10:23 AM
To: Cameron, Bud; Bendelier, Kenneth
Cc: Pitcher Robert; Klassen, Nathan
Subject: CCIRC WEEKLY SUMMARY FOR WEEK OF 5 DEC 2011-TO SEND OUT
Attachments: PS-SP-#534275-3-CCIRC WEEKLY SUMMARY FOR WEEK OF 5 DEC 2011-TO SEND OUT.DOC

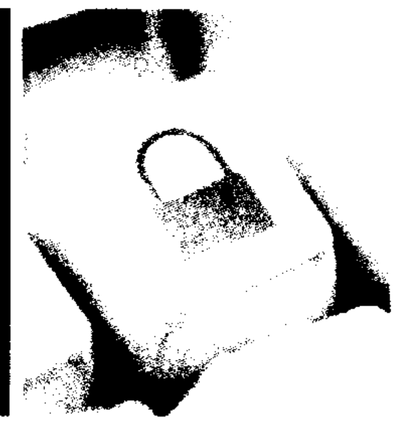
For your review and feedback. I've incorporated everyone's comments to date. Still no word from Luc..

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-008



For the Week of

3 Dec – 9 Dec 2011

Issued: 16 Dec 2011

HIGHLIGHTS:

Threat Warnings: Nothing significant to report.

CCIRC Products: CCIRC sent the following Cyber Flashes to stakeholders.

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
- CF11-026: Widespread SQL injection campaign
- CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

Incidents to report:

- Threat actors impersonating a Canadian federal agency enticing internet users to visit a malicious website
- Potential compromises in computer systems in the provincial government, financial, health, telecommunications and education sectors
- SQL injection attacks, resulting in compromised websites re-directing site visitors to a malicious website. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

Noteworthy Open Source Reports:

- A draft US Bill in cyber security gets support from privacy proponents
- White House announces cloud security "rules of the road" for US federal agencies and contractors
- Hacker groups successfully attack websites of the Portugese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

CCIRC PRODUCTS RELEASED THIS WEEK:

CCIRC sent three Cyber Flashes to key stakeholders – mainly IT professionals and managers in government, critical infrastructure and related sectors.

CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator. CCIRC has been receiving reports of various spear phishing campaigns that may be associated with Advanced Persistent Threat (APT) activity. This Cyber Flash highlighted the technical details of such recent attacks so stakeholders can check if they have been victimized. CCIRC also offered references for additional background information and mitigation advice.

CF11-026: Widespread SQL injection campaign. CCIRC received reports of a recent and broadly distributed SQL injection campaign. This world-wide attack campaign resulted in compromised websites redirecting unsuspecting site visitors to a malicious website, reportedly hosted in Moldova. It is estimated the campaign affected over 160,000 websites in the world, including Canadian ones. SQL injection attacks are a common and effective way to compromise legitimate but vulnerable websites in order to perpetrate malicious acts.

CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products. The purpose of this cyber flash is to raise awareness and offer mitigation for a number of unpatched vulnerabilities affecting versions of Adobe Reader, Adobe Acrobat and Adobe Flash products. CCIRC believes one of these vulnerabilities may have been leveraged in targeted attacks against the defence industrial sector.

NOTABLE INCIDENTS– 3 DECEMBER THROUGH 9 DECEMBER 2011:

Canadian Critical Infrastructure:

Federal Government. Threat actors impersonating a federal agency tried to entice internet users to a malicious website hosted in China. CCIRC notified its Chinese equivalent organization (China CERT) and recommended deactivation of the malicious website. CCIRC also reported the incident to Google as well as the Anti-Phishing Working Group (APWG).

- **Analysis:** CCIRC cooperates with computer incident or emergency response centres around the world, including China CERT. Cyber crime is also a concern in China, where internet

users are targeted quite heavily by criminals. A recently publicized incident was the defrauding of customers of a popular Chinese shopping website.

Threat actors impersonating the same federal agency tried to entice internet users to a malicious website and tried to persuade them to reveal personal information (ex: name, social insurance and credit card numbers). The request was traced to a Romanian website hosted in the U.S. CCIRC notified the internet service provider and informed US CERT (American equivalent of CCIRC). The malicious content had been removed from the website later that week.

Provincial Government. A provincial health organization was one of the victims of the wide-spread, world-wide, SQL injection attack described above for Cyber Flash CF11-026. The impact on the organization and the number of web-site visitors victimized is unknown. CCIRC notified the provincial government contacts and gave mitigation advice.

CCIRC also received infection reports for another provincial government's computer systems. Possible impacts can range from data theft to taking control of those computers to send SPAM. CCIRC notified the provincial contacts and gave mitigation advice. Impact on the organization is unknown.

- **Analysis:** These types of infections, commonly seen by CCIRC, could potentially lead to a compromise of that government's computer system. There is no information to suggest these were targeted attacks on that system.

Financial Sector. CCIRC received infection reports for a Canadian financial institution, which indicates potential computer compromises on the organization's network facing the internet. The impact on the organization and its clients is unknown. CCIRC notified the organization and offered mitigation advice.

- **Analysis:** The infections reported for this institution are commonly found on the internet, probably passed on from an on-line bank client who does not practice good cyber security. In CCIRC's experience, financial institutions pay keen attention to cyber security, because they are aware they are attractive targets to cyber criminals. Cyber security is understood to be a risk mitigation measure that will minimize a bank's financial losses and protect its reputation.

Telecommunications Sector. CCIRC received infection reports for two Canadian internet service providers and notified the organizations. These reports indicate there were likely compromises of computers belonging to internet users subscribing to those providers.

A large telecommunications service provider was one of the victims of the wide-spread, world-wide, SQL injection attack described earlier. This attack resulted in compromised websites redirecting unsuspecting site visitors to malicious websites. It is unknown how many client computers were compromised as a result of this malicious activity. CCIRC notified the service providers and gave mitigation advice. A Cyber Flash was also issued because of the estimated wide-spread impact.

Health. CCIRC received reports on potential compromises for a municipal Canadian health service provider and notified the organization. CCIRC does not have any information to indicate these compromises relate to a targeted attack.

Other Sectors:

CCIRC received reports on potential compromises for a Canadian university and notified the organization. A local real estate board was also the victim of the SQL injection attack described earlier in the report.

Noteworthy Open Source Reports:

A draft US Cyber security bill gets nod from privacy proponents. The House Homeland Security Subcommittee on Cyber security, Infrastructure Protection and Security Technologies held hearings on a draft cyber security bill. This bill proposes cyber-threat information sharing between the public and private sectors via a not-for-profit National Information Sharing Organization. This organization, would be led by DHS and consist of privacy advocates, representatives from critical infrastructure industry sectors, state and local government. The Center for Democracy and Technology, a US civil liberties group, publicly favours this draft bill over the other draft bill (H.R. 3523) because of its "superior information sharing stipulations".

Analysis: The House Intelligence Panel has already approved a competing draft cyber security bill that expands the pilot cyber threat information sharing program between the Defence Department and defence contractors. Privacy groups are concerned would this bill would allow Internet service providers to share private communications with the government. Of particular concern would be any customer data disclosure to the National Security Agency (NSA), who ran the pilot information sharing program.

US agencies and contractors get rules of the road for cloud security approvals. The White House announced that cloud providers to US federal agencies will have to comply with new uniform security requirements, by June 2012. US officials said agencies have shifted 40 IT services, such as email and collaboration software, to the cloud, in the past year. Seventy-nine more services have been identified for transfer to the cloud by June 2012. The newly announced Federal Risk and Authorization Management Program (FedRAMP), is expected to allow for more rapid and cost-effective deployment of cloud services for multiple US government agencies. Reports suggest an estimated $5 billion savings could result.

- **Analysis:** Cloud computing and securing data in a cloud is also a current topic of discussion in Canada. Though there are no specific official guidelines for cloud computing in the Canadian federal government, there are Treasury Board guidelines for outsourcing IT infrastructure and services.

- Cloud computing allows one to store and process one's data in an off-site computer system owned by a third party. This data can be accessible from almost any location. This feature, coupled with the proliferation of smart mobile devices, has brought cloud computing heightened attention. A recent survey by CSC, a US technology company, suggests that allowing employees mobile access to data, rather than saving money, was the reason for moving data to the cloud for many organizations.

Hacker groups successfully attack websites for the Portuguese Government, Columbian Army, Mexican Government and the PR firm for Monsanto. Open sources reported that Lulzsec Portugal, a self-proclaimed activist group, disabled the websites of **Portuguese government**, National Police, House of Parliament and several political parties. Reasons given for the attack were the Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest.

Anonymous, the famous international hacker group, successfully attacked the **Columbian Army**'s website. The motive given was to avenge a recently televised shooting of a seemingly harmless dog by soldiers. Anonymous also took down websites of numerous Mexican transportation and government websites, protesting the "dangerous travelling conditions present in Mexico".

Anonymous also executed a successful attack on a public relations firm working with Monsanto, as part of "Operation End Monsanto". The public relations firm, Bivings, reportedly had its website defaced and data stolen. Shortly after the incident, the firm liquidated their assets, and employees started a new public relations company. Monsanto is a large international producer of genetically engineered seeds and pesticides. It is the target of a number of activist groups and was named "Worst Company of 2011" by an environmental activist group.

- **Analysis:** Even though LulzSec was declared defunct in June 2011, affiliated hacker groups are still operating successfully around the world. Anonymous continues to target and successfully execute attacks around the world against vulnerable targets for activist purposes. Anonymous threatened to attack the Toronto Stock Exchange in support of the "Occupy" movement earlier this year. CCIRC is unaware of any incidents resulting from this threat.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

UNCLASSIFIED
DRAFT

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Dincoy, Rana

From: Dincoy, Rana
Sent: December-16-11 10:23 AM
To: Cameron, Bud; Bendelier, Kenneth
Cc: Pitcher Robert; Klassen, Nathan
Subject: CCIRC WEEKLY SUMMARY FOR WEEK OF 5 DEC 2011-TO SEND OUT
Attachments: PS-SP-#534275-3-CCIRC WEEKLY SUMMARY FOR WEEK OF 5 DEC 2011-TO SEND OUT.DOC

For your review and feedback. I've incorporated everyone's comments to date. Still no word from Luc..

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-008

For the Week of

3 Dec – 9 Dec 2011

Issued: 16 Dec 2011

HIGHLIGHTS:

Threat Warnings: Nothing significant to report.

CCIRC Products: CCIRC sent the following Cyber Flashes to stakeholders.

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
- CF11-026: Widespread SQL injection campaign
- CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

Incidents to report:

- Threat actors impersonating a Canadian federal agency enticing internet users to visit a malicious website
- Potential compromises in computer systems in the provincial government, financial, health, telecommunications and education sectors
- SQL injection attacks, resulting in compromised websites re-directing site visitors to a malicious website. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

Noteworthy Open Source Reports:

- A draft US Bill in cyber security gets support from privacy proponents
- White House announces cloud security "rules of the road" for US federal agencies and contractors
- Hacker groups successfully attack websites of the Portugese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

CCIRC PRODUCTS RELEASED THIS WEEK:

CCIRC sent three Cyber Flashes to key stakeholders – mainly IT professionals and managers in government, critical infrastructure and related sectors.

CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator. CCIRC has been receiving reports of various spear phishing campaigns that may be associated with Advanced Persistent Threat (APT) activity. This Cyber Flash highlighted the technical details of such recent attacks so stakeholders can check if they have been victimized. CCIRC also offered references for additional background information and mitigation advice.

CF11-026: Widespread SQL injection campaign. CCIRC received reports of a recent and broadly distributed SQL injection campaign. This world-wide attack campaign resulted in compromised websites redirecting unsuspecting site visitors to a malicious website, reportedly hosted in Moldova. It is estimated the campaign affected over 160,000 websites in the world, including Canadian ones. SQL injection attacks are a common and effective way to compromise legitimate but vulnerable websites in order to perpetrate malicious acts.

CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products. The purpose of this cyber flash is to raise awareness and offer mitigation for a number of unpatched vulnerabilities affecting versions of Adobe Reader, Adobe Acrobat and Adobe Flash products. CCIRC believes one of these vulnerabilities may have been leveraged in targeted attacks against the defence industrial sector.

NOTABLE INCIDENTS– 3 DECEMBER THROUGH 9 DECEMBER 2011:

Canadian Critical Infrastructure:

Federal Government. Threat actors impersonating a federal agency tried to entice internet users to a malicious website hosted in China. CCIRC notified its Chinese equivalent organization (China CERT) and recommended deactivation of the malicious website. CCIRC also reported the incident to Google as well as the Anti-Phishing Working Group (APWG).

- **Analysis:** CCIRC cooperates with computer incident or emergency response centres around the world, including China CERT. Cyber crime is also a concern in China, where internet

users are targeted quite heavily by criminals. A recently publicized incident was the defrauding of customers of a popular Chinese shopping website.

Threat actors impersonating the same federal agency tried to entice internet users to a malicious website and tried to persuade them to reveal personal information (ex: name, social insurance and credit card numbers). The request was traced to a Romanian website hosted in the U.S. CCIRC notified the internet service provider and informed US CERT (American equivalent of CCIRC). The malicious content had been removed from the website later that week.

Provincial Government. A provincial health organization was one of the victims of the wide-spread, world-wide, SQL injection attack described above for Cyber Flash CF11-026. The impact on the organization and the number of web-site visitors victimized is unknown. CCIRC notified the provincial government contacts and gave mitigation advice.

CCIRC also received infection reports for another provincial government's computer systems. Possible impacts can range from data theft to taking control of those computers to send SPAM. CCIRC notified the provincial contacts and gave mitigation advice. Impact on the organization is unknown.

- **Analysis:** These types of infections, commonly seen by CCIRC, could potentially lead to a compromise of that government's computer system. There is no information to suggest these were targeted attacks on that system.

Financial Sector. CCIRC received infection reports for a Canadian financial institution, which indicates potential computer compromises on the organization's network facing the internet. The impact on the organization and its clients is unknown. CCIRC notified the organization and offered mitigation advice.

- **Analysis:** The infections reported for this institution are commonly found on the internet, probably passed on from an on-line bank client who does not practice good cyber security. In CCIRC's experience, financial institutions pay keen attention to cyber security, because they are aware they are attractive targets to cyber criminals. Cyber security is understood to be a risk mitigation measure that will minimize a bank's financial losses and protect its reputation.

Telecommunications Sector. CCIRC received infection reports for two Canadian internet service providers and notified the organizations. These reports indicate there were likely compromises of computers belonging to internet users subscribing to those providers.

A large telecommunications service provider was one of the victims of the wide-spread, world-wide, SQL injection attack described earlier. This attack resulted in compromised websites redirecting unsuspecting site visitors to malicious websites. It is unknown how many client computers were compromised as a result of this malicious activity. CCIRC notified the service providers and gave mitigation advice. A Cyber Flash was also issued because of the estimated wide-spread impact.

Health. CCIRC received reports on potential compromises for a municipal Canadian health service provider and notified the organization. CCIRC does not have any information to indicate these compromises relate to a targeted attack.

Other Sectors:

CCIRC received reports on potential compromises for a Canadian university and notified the organization. A local real estate board was also the victim of the SQL injection attack described earlier in the report.

Noteworthy Open Source Reports:

A draft US Cyber security bill gets nod from privacy proponents. The House Homeland Security Subcommittee on Cyber security, Infrastructure Protection and Security Technologies held hearings on a draft cyber security bill. This bill proposes cyber-threat information sharing between the public and private sectors via a not-for-profit National Information Sharing Organization. This organization, would be led by DHS and consist of privacy advocates, representatives from critical infrastructure industry sectors, state and local government. The Center for Democracy and Technology, a US civil liberties group, publicly favours this draft bill over the other draft bill (H.R. 3523) because of its "superior information sharing stipulations".

Analysis: The House Intelligence Panel has already approved a competing draft cyber security bill that expands the pilot cyber threat information sharing program between the Defence Department and defence contractors. Privacy groups are concerned would this bill would allow Internet service providers to share private communications with the government. Of particular concern would be any customer data disclosure to the National Security Agency (NSA), who ran the pilot information sharing program.

US agencies and contractors get rules of the road for cloud security approvals. The White House announced that cloud providers to US federal agencies will have to comply with new uniform security requirements, by June 2012. US officials said agencies have shifted 40 IT services, such as email and collaboration software, to the cloud, in the past year. Seventy-nine more services have been identified for transfer to the cloud by June 2012. The newly announced Federal Risk and Authorization Management Program (FedRAMP), is expected to allow for more rapid and cost-effective deployment of cloud services for multiple US government agencies. Reports suggest an estimated $5 billion savings could result.

- **Analysis:** Cloud computing and securing data in a cloud is also a current topic of discussion in Canada. Though there are no specific official guidelines for cloud computing in the Canadian federal government, there are Treasury Board guidelines for outsourcing IT infrastructure and services.

- Cloud computing allows one to store and process one's data in an off-site computer system owned by a third party. This data can be accessible from almost any location. This feature, coupled with the proliferation of smart mobile devices, has brought cloud computing heightened attention. A recent survey by CSC, a US technology company, suggests that allowing employees mobile access to data, rather than saving money, was the reason for moving data to the cloud for many organizations.

Hacker groups successfully attack websites for the Portuguese Government, Columbian Army, Mexican Government and the PR firm for Monsanto. Open sources reported that Lulzsec Portugal, a self-proclaimed activist group, disabled the websites of **Portuguese government**, National Police, House of Parliament and several political parties. Reasons given for the attack were the Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest.

Anonymous, the famous international hacker group, successfully attacked the **Columbian Army**'s website. The motive given was to avenge a recently televised shooting of a seemingly harmless dog by soldiers. Anonymous also took down websites of numerous Mexican transportation and government websites, protesting the "dangerous travelling conditions present in Mexico".

Anonymous also executed a successful attack on a public relations firm working with Monsanto, as part of "Operation End Monsanto". The public relations firm, Bivings, reportedly had its website defaced and data stolen. Shortly after the incident, the firm liquidated their assets, and employees started a new public relations company. Monsanto is a large international producer of genetically engineered seeds and pesticides. It is the target of a number of activist groups and was named "Worst Company of 2011" by an environmental activist group.

- **Analysis:** Even though LulzSec was declared defunct in June 2011, affiliated hacker groups are still operating successfully around the world. Anonymous continues to target and successfully execute attacks around the world against vulnerable targets for activist purposes. Anonymous threatened to attack the Toronto Stock Exchange in support of the "Occupy" movement earlier this year. CCIRC is unaware of any incidents resulting from this threat.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

UNCLASSIFIED
DRAFT

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-16-11 1:25 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Hackers Take Down Child P*** Websites, Leak User's Names

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Opera
Complete item: http://my.opera.com/KellyAFisch/blog/2011/12/15/anonymous-hackers-take-down-child-porn-websites-leak-users-names

Description:
In its statement, the Anonymous members explained their goals and how they aim to achieve them through repeated pressure and consistent online attacks.

"The owners and operators at Freedom Hosting are openly supporting child p***ography and enabling pedophiles to view innocent children, fueling their issues and putting children at risk of abduction, molestation, rape and death," the message said. "For this, Freedom Hosting has been declared #OpDarknet Enemy Number One. By taking down Freedom Hosting, we are eliminating 40+ child p***ography websites, among these is Lolita City, one of the largest child p***ography websites to date containing more than 100 GB of child p***ography. We will continue to not only crash Freedom Hosting's server, but any other server we find to contain, promote, or support child p***ography."

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-15-11 1:18 PM
To: Bendelier, Kenneth
Subject: Information: Anonymous Affiliate Arrested for 2010 DDoS Attack

Generated by your Alert Subscription on Folder:
- Anonymous
Source: infosec island
Complete item: https://www.infosecisland.com/blogview/18703-Anonymous-Affiliate-Arrested-for-2010-DDoS-Attack.html

Description:
While justice may not be swift, federal authorities are finally getting around to charging someone for the October 2010 distributed denial of service (DDoS) attack against the website of rocker Gene Simmons.

The FBI this week arrested Kevin George Poe who was arraigned on charges of conspiracy and unauthorized impairment of a protected computer.

From the FBI press release:

FBI special agents this morning arrested a Connecticut man who is charged with waging a denial of service attack against GeneSimmons.com, a website operated by the frontman for the rock band KISS.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-14-11 3:15 PM
To: Bendelier, Kenneth
Subject: Important: The FBI Nabs Another Alleged Anonymous Member

Generated by your Alert Subscription on Folder:
- Anonymous
Source: National Cyber Security
Complete item: http://nationalcybersecurity.com/2011/12/fbi-nabs-alleged-anonymous-member/

Description:
The number of Anonymous members could be shrinking. Tuesday the FBI announced the arrest of a Connecticut man with ties to the Internet hacking group.

Special agents charged 24-year old Kevin George Poe with waging a denial of service attack against GeneSimmons.com. The website is operated by the front man for the rock band KISS.

Poe allegedly used the screen name spydr101. The FBI took him into custody without incident at the federal courthouse in Hartford. Poe made his initial appearance Tuesday morning in United States District Court, where a judge ordered Poe released on a $10,000 bond and ordered him to appear in federal court in Los Angeles on a date that has yet to be scheduled.

Last week a federal grand jury in Los Angeles returned an indictment accusing Poe of being affiliated with the hacking group Anonymous. The indictment charges Poe with two countsconspiracy and unauthorized impairment of a protected computer.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-14-11 3:07 PM
To: Bendelier, Kenneth
Subject: Important: Florida Family Association: Anonymous Hacked Us Over Lowes Campaign

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Talking points memo
Complete item:
http://tpmmuckraker.talkingpointsmemo.com/2011/12/florida_family_association_anonymous_hacked_us_ove.php

Description:
The Florida Family Association is blaming Anonymous for taking down its website after the social conservative group pressured Lowes to pull its advertising from the TV show All-American Muslim.

David Caton, executive director of the Florida Family Association, said that a hacker claiming to be from the hacktivist collective Anonymous took down the website Monday night in retaliation for the Lowes campaign, only leaving up the message that the group was destroying our free speech, the St. Petersburg Times reports.

At the time of writing the FFA site was just one page that referenced the attack in a message from Caton: No further proof is needed of the potential for vicious action then [sic] exactly what these folks are trying to do to this web site!

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-14-11 3:04 PM
To: Bendelier, Kenneth
Subject: Information: Gene Simmons Hacker Suspect Kevin George Poe Arrested (Bummer): FBI Says He's a Member of 'Anonymous'

Generated by your Alert Subscription on Folder:
- Anonymous
Source: laweekly
Complete item: http://blogs.laweekly.com/informer/2011/12/gene_simmons_hacker_anonymous_arrest.php

Description:
You see, the L.A.-based rocker and reality show "star" uttered a death-to-file sharers proclamation ("Take their homes, their cars," he said) last year, and, in response, hackers took down his website.

(Lulz, right?).

Well the law has caught up with one of the alleged online pranksters, unfortunately:

The FBI today announced the arrest of 24-year-old Kevin George Poe in connection with the "denial of service attack" on genesimmons.com.

FBI agents got him at his Manchester, Connecticut home this morning, according to a statement from the U.S. Attorney's Office in L.A.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-14-11 2:14 PM
To: Bendelier, Kenneth
Subject: Information: Alleged Anonymous Affiliate Accused of DDoS on Gene Simmons Site Arrested

Generated by your Alert Subscription on Folder:
- Anonymous
Source: threat post
Complete item: http://threatpost.com/en_us/blogs/anonymous-affiliate-accused-hacking-gene-simmons-arrested-121411?utm_source=Newsletter_121411&utm_medium=Email+Marketing&utm_campaign=Newsletter&CID=&CID=

Description:
An alleged member of the Anonymous hacker collective was arrested Tuesday in connection with an attack on the Website of KISS front-man and reality television star Gene Simmons.

Reuters identifies the suspect as a 24 year-old Connecticut man named Kevin George Poe. Poe is accused of orchestrating a denial-of-service attack against Simmonss website back in October 2010.

Poe is ordered to appear in a court in Los Angeles at a yet-to-be determined date. He is charged with conspiracy and unauthorized impairment of a protected computer and could face up to the 15 years if convicted.

E-Secure-IT
https://www.e-secure-it.com

s.15(1) - Subv
s.16(2)(c)

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-14-11 8:15 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary - 2011-12-14

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
December 14, 2011 / le 14 décembre 2011

Print media

Man arrested for hacking site
A Connecticut man affiliated with the Anonymous hacking group was arrested Tuesday on federal charges for an attack on a website belonging to Kiss bassist Gene Simmons, authorities said. Red Deer Advocate, D6

Encore arrête
Accusé en juillet d'avoir frauduleusement utilisé des ordinateurs, Joseph Mercier fait de nouveau face à la justice, notamment pour menaces et possession de pornographie juvénile. De son côté, la Gendarmerie royale du Canada (GRC), en collaboration avec la police de Laval, l'a arrêté pour les mêmes raisons qu'en juillet, soit l'utilisation non autorisée d'ordinateur et méfaits aux données. À l'aide d'un réseau zombie (botnet), il aurait infecté des ordinateurs d'un virus pour les contrôler à distance. Journal de Montréal, 10

Les enfants manquent d'encadrement
Tous les parents s'entendent: l'internet représente une importante source de danger pour les enfants. Paradoxalement, la moitié d'entre eux ne fait pourtant rien pour les protéger. C'est ce qui ressort du tout premier sondage jamais réalisé au Québec sur la question, rendu public hier par la fondation Marie-Vincent et cyberaide.ca, en présence du Service de police de la Ville de Montréal, de la Sûreté du Québec et de la Gendarmerie royale du Canada. La Voix de l'Est, 18

Online media

China-based hacking offers evidence of global cyber war
Google Inc. and Intel Corp. were logical targets for China-based hackers, given the solid-gold intellectual property data stored in their computers. An attack by cyber spies on iBahn, a provider of Internet services to hotels, takes some explaining. Bloomberg

12 hacking groups are behind most Chinese cyber attacks
Eastern European and Russian hackers mostly steal financial information, while Chinese ones are mainly after intellectual propriety or other sensitive data, say security analysts and US officials, and the great majority of the attacks believed to be originating from China can be tied to as few as 12 distinct hacking groups. Help Net Security

Hacks of municipal water, power services prompts DHS warning
Hackers using "readily available and generally free search tools" can gain access to municipal power and water systems via the Internet, a problem that can be exacerbated by the fact that plant operators might not know their systems are

Internet-connected, the Homeland Security Department says. An FBI official recently said services in three U.S. cities have been hit. Government Computer News

Russian security council chief wants web regulation
The Internet must be subject to "reasonable regulation", the head of Russia's Security Council said in remarks published on Wednesday, a fresh sign of Kremlin concern about the use of social networks to promote anti-government protests. Reuters

Prime Minister Gillard Takes Control Of Cyber Security
Prime Minister Julia Gillard appears set to take personal control of cyber security as part of the ministerial reshuffle she announced yesterday. In a line published in the Prime Minister's press speech distributed to media, but not actually read by Gillard to the cameras – but quickly picked up by SC business intelligence magazine – she announced that "responsibility for cyber security policy will move from the Attorney-General's portfolio to my portfolio" of Prime Minister and Cabinet (PM&C). Channel News

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-14-11 8:03 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
December 14, 2011 / le 14 décembre 2011

MINISTER / MINISTRE

Quebec to sue for long-gun data

Quebec wants to create its own long-gun registry, using data already collected for the federal registry, and is prepared to go to court to stop Ottawa destroying gun ownership records. Public Security Minister Robert Dutil announced Tuesday that Quebec would take legal action to recover the data once Ottawa's Bill C-19, abolishing the federal longgun registry, becomes law. Dutil wrote to his federal counterpart **Vic Toews** on Dec. 2 appealing for him to save the registry. Dutil also asked **Toews** to require gun sellers to verify whether buyers have a valid gun permit. **Michael Patton, communications director for Toews**, said in a telephone interview the Conservative government has a mandate to repeal the long-gun registry. He said the government's commitment includes destroying the data, which he added are not always up to date, and that Ottawa will not transfer its registry to Quebec. "***It's just a difference of philosophy***," he said. **Patton** added police can still track weapons ownership through gun permits. "***You have to have a licence to purchase ammunition***," he noted. Montreal Gazette, A12; Ottawa Citizen; The Province; Toronto Star; Journal de Montréal

Would-be leaders absent for most votes

The federal politicians in the races to lead the NDP and the Bloc Quebecois are also leading the pack of MPs who missed the most votes in this session of Parliament, according to the latest investigation of House of Commons attendance by The Globe and Mail. Seven Tory cabinet members were among the top 25 most absent MPs in 2011, including Finance Minister Jim Flaherty, **Public Safety Minister Vic Toews** and Foreign Affairs Minister John Baird. Globe and Mail, A12

Getting ruff on drugs

Ruby is a bundle of energy and bounds through the visiting room at Collins Bay Institution. Always sniffing, she pulls at her leash, leading her handler around the room. When Ruby finds what she is looking for, she is trained to sit and await her chew toy reward. What is fun for the dog is also part of an expanded federal government anti-drug prison detector dog program. In November, **Minister of Public Safety Vic Toews** announced an expansion of the detector dog program in federal prisons. Kingston Whig-Standard, 1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

* Flood packs $815

This year's flood has turned out to be a $343-million budgetary headache for Manitoba's finance minister. Stan Struthers told the Free Press on Tuesday the tally for flood compensation in the province this year is a whopping $815 million, of which $472 million is expected to be recovered from the federal government. Although Ottawa covers as much as 90 per cent in disaster financial assistance costs, some of the agricultural support programs necessitated by the flood were more equally cost-shared by the two levels of government. And the cost of one livestock feed plan was borne by the province alone, Stan Struthers said. Winnipeg Free Press, A3

* Fuite d'eau lourde radioactive

De l'eau lourde radioactive a fui de la centrale nucléaire de Point Lepreau au Nouveau-Brunswick. Kathleen Duguay, une porte-parole pour Énergie NB, a indiqué que la fuite était survenue mardi soir dans le bâtiment du réacteur. Mme Duguay ne connaissait pas la quantité exacte d'eau lourde qui s'était échappée, mais a dit que le volume était "minime". Selon elle, personne n'a été blessé. La fuite a eu lieu alors que le système de régulation du réacteur était rempli d'eau lourde, dans le cadre du redémarrage de l'unité de production électrique, qui a été remise à neuf à grands frais. Le Quotidien, 15

*** 'Gaps' found in pipeline safety**
The public safety of Canadians is increasingly at risk because the federal government is failing to monitor and enforce its regulations on dangerous goods and decades-old oil and gas pipelines, Canada's environment watchdog warns in a new report. Calgary Herald, A1 (Montreal Gazette, Leader-Post, Windsor Star, Edmonton Journal, Times & Transcript, Vancouver Sun)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Sweeping detention measures added to bill
Even American citizens arrested in the United States could face perpetual detention in military prisons without charge or trial under draconian new presidential powers unless Barack Obama vetoes a massive Pentagon spending bill. The sweeping new "antiterrorist" measures could also ensnare Canadians or other foreigners picked up in the United States or overseas. Canadians have already suffered the long reach of enhanced U.S. counterterrorism powers, abetted sometimes by Canadian agents. For instance, Maher Arar was intercepted changing planes in New York, shipped to Syria and tortured. Under the new provisions, he could have been imprisoned in Guantanamo indefinitely. Similarly, secret Canadian CSIS documents show that the CIA wanted another Canadian, Abousfian Abdelrazik, sent to Guantanamo Bay, the U.S. offshore prison on a leased naval base in Cuba. Globe and Mail, A17

Hezbollah aided by drug king pin, U.S. says
U.S. authorities have accused a Lebanese drug kingpin with alleged links to the Hezbollah terrorist group of helping to smuggle huge amounts of cocaine into the United States. Ayman Joumaa, 47, was accused of conspiring with others to help ship some 85,000 kilograms of cocaine from Colombia from 2005 to 2007. He was also accused of helping launder more than US$250-million in drug money for the Los Zetas drug cartel. Washington blacklisted the Beirut-based Lebanese Canadian Bank - which had an office in Montreal - alleging it was a money-laundering front for Mr. Joumaa. It was alleged his network was moving hundreds of millions of dollars in drug money. National Post, A16

Terror label doesn't fit
A letter to the editor states, "How can an Iraqi-Canadian citizen, whose homeland was illegally invaded by foreign armies in 2003 in the opinion of the secretary general of the United Nations and most legal experts, and occupied for eight years in blatant violation of international law, be labelled a terrorist for allegedly resisting what U.S. officials at Nuremberg declared the quintessential war crime, an unsanctioned war of aggression?...Would Canada extradite Americans who resisted or encouraged the resistance to such a lawless invasion to the invading country?" Edmonton Journal, A26

Refugees or terrorists? They'll soon be dead
An opinion piece states, "They are half-a-world away and there are only seven of them, but the members of Parliament on a House of Commons human rights committee are doing whatever they can for the 3,400 refugees at Camp Ashraf, north of Baghdad, who, the MPs believe, are in imminent danger. There are two Canadians among the refugees. They remain at Ashraf voluntarily despite offers from Canadian consular officials to get them out of what could, within days, become a dicey situation...So why doesn't the U.S. or its allies in the West save these 3,400 refugees? We won't because officially the MeK are all terrorists. Officially, we think they're the bad guys because of those violent acts committed a generation or more ago. Canada has designated the MeK as a terrorist organization since 2005 and just reaffirmed that status in 2010. The U.S. has had them on the list since 1997..." Calgary Sun, 15 (Edmonton Sun, Toronto Sun, London Free Press, Kingston Whig-Standard, Winnipeg Sun)

*** Special forces keep terror threat at bay**
Jamaican commandos storm the Tivoli Gardens slum in May 2010, hunting down an alleged trafficker and drug baron wanted in the United States. One year later on the other side of the world, a little-known squad of Afghan police officers fend off volleys of Taliban bombs and bullets during a siege of the governor's palace in Kandahar City. Tying the two events together are small groups of Canadian Special Forces who travel the world training foreign militaries on how to fight terrorism. It's a modest investment of foreign ministry money and Canadian Forces personnel meant to halt threats of violence and instability before they spread to Canadian shores. Toronto Star, A4

*** Canada invited to nuclear summit**
Fighting the threat of "radiological terrorism" will once again preoccupy Canada and 50 other countries and groups at a major summit next year on nuclear security. South Korea has high ambitions for the March meeting it is hosting, the followup to last year's inaugural nuclear security summit that was chaired by U.S. President Barack Obama. Hamilton Spectator, A14

CYBER SECURITY / CYBERSÉCURITÉ

*** Man arrested for hacking site**
A Connecticut man affiliated with the Anonymous hacking group was arrested Tuesday on federal charges for an attack on a website belonging to Kiss bassist Gene Simmons, authorities said. Red Deer Advocate, D6

*** Encore arrête**
Accusé en juillet d'avoir frauduleusement utilisé des ordinateurs, Joseph Mercier fait de nouveau face à la justice, notamment pour menaces et possession de pornographie juvénile. De son côté, la Gendarmerie royale du Canada (GRC), en collaboration avec la police de Laval, l'a arrêté pour les mêmes raisons qu'en juillet, soit l'utilisation non autorisée d'ordinateur et méfaits aux données. À l'aide d'un réseau zombie (botnet), il aurait infecté des ordinateurs d'un virus pour les contrôler à distance. Journal de Montréal, 10

*** Les enfants manquent d'encadrement**
Tous les parents s'entendent: l'internet représente une importante source de danger pour les enfants. Paradoxalement, la moitié d'entre eux ne fait pourtant rien pour les protéger. C'est ce qui ressort du tout premier sondage jamais réalisé au Québec sur la question, rendu public hier par la fondation Marie-Vincent et cyberaide.ca, en présence du Service de police de la Ville de Montréal, de la Sûreté du Québec et de la Gendarmerie royale du Canada. La Voix de l'Est, 18

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Raids crack down on street gangs
What began as an investigation into a shooting in Toronto's gritty Jane-Finch neighbourhood last spring turned into a major bust of street gang members in four provinces. The case gained a national scope as investigators tracked local gang associates who had relocated and committed crimes in cities across central and Western Canada, Toronto police Chief Bill Blair said on Tuesday. "It revealed a level of mobility among street gangs not yet witnessed before in this city," he said. In predawn operations, hundreds of police officers arrested 60 people - 10 of them minors - and searched dozens of locations in Ontario, Quebec, Alberta and British Columbia. Police seized guns, ammunition, drugs and money in the raids, and Superintendent Chris White, the officer in charge of the Toronto police's Organized Crime Enforcement Unit, said more than 300 charges are expected. Globe and Mail, A15; The Record; (The Guardian); * Le Droit; * National Post; * Calgary Sun; * Edmonton Sun; * Toronto Sun; * Ottawa Sun (Whig-Standard); * London Free Press; * Vancouver Sun; * L'Acadie Nouvelle; * Toronto Star

*** PM unmoved by Quebec court challenge**
Prime Minister Stephen Harper is refusing to delay the destruction of the long-gun registry data even as the Quebec government launches a last-ditch court challenge that could take years to decide. Brushing off attacks from Quebec and the opposition, Mr. Harper and his ministers said they will not wait for the court ruling to fulfill a campaign promise to get rid of the registry and its unreliable data. Globe and Mail, A9; National Post; Edmonton Journal (Calgary Herald); Edmonton Sun; Le Quotidien (La Voix de l'Est, Le Soleil); Le Devoir; The Telegram

*** Québec annonce un recours juridique contre Ottawa**
Si Québec ne réussit pas à empêcher la destruction des données du registre des armes à feu, il devrait investir pour en créer un nouveau, même si cela coûterait au moins 35 millions. C'est ce que croient Yves Francoeur et Pierre Veilleux, présidents de la Fraternité des policiers et policières de Montréal et de l'Association des policières et policiers provinciaux du Québec. La Presse, A16 (La Tribune)

*** Beneath Chrétien's dignity**
An editorial states, "...With or without the long-gun registry, Canada already has one of the strictest gun-control policies of any nation on Earth. And to the extent the registry is on its way out, the blame goes almost entirely to the Liberal-created bureaucratic apparatus that managed to burn through $2-billion without making Canada any safer. No doubt, Mr. Chrétien and the man who led the gun-registry file - mid1990s-era justice minister Allan Rock - were genuinely moved by the massacre at École Polytechnique, and wanted to do something to prevent another tragedy. But their signature gun-control project was executed so incompetently that it actually damaged the cause. All the Tor-ies did was clean up their mess..." National Post, A12

*** Ex-Mountie guilty of child porn**
A former RCMP officer who had more than 20,000 images of child pornography on his computer and sexually assaulted a 14-year-old boy should receive a seven-to 10-year jail term, a prosecutor says. Edmonton Journal, A9 (The Province, Times Colonist); Times Colonist

*** Burnout threatens Kelowna Mounties**
New statistics show Kelowna has the fewest police officers per capita in Canada, and a police official says the result is officer burnout and a relatively high crime rate for a city its size. Kelowna officers receive among the most calls per member of any detachment in B.C., said Supt. Bill McKinnon, who is in charge of the local RCMP detachment. Vancouver Sun, A1 (Times Colonist)

*** Cop fetishist accused of playing mountie again**
A Manitoba man recently freed from jail for impersonating an RCMP officer at crime scenes is accused of mimicking one again -- this time in writing. Thomas David Hanaway, 54, made a first appearance on a charge of impersonating a peace officer in a Winnipeg courtroom Tuesday afternoon. Winnipeg Sun, 7(Whig-Standard)

*** Legal grow ops act as magnets for illegal activities, city officials worry**
The situation in the small B.C. community underscores a growing trend being played out across Canada, where 12,000 licences have been issued by Health Canada to allow people to grow medicinal weed. The permits allow people with certain conditions - such as glaucoma, spinal cord injuries, pain or nausea from cancer or HIV - to grow medical pot in their homes or designate some-one else to grow it for them. But many municipalities, especially those in B.C. where close to 3,000 medical marijuana permits have been issued, argue the program is rife with abuse. A proliferation of grow operations has led to house fires, violent home invasions and black-market dealing - with some sanctioned growers growing far more than they need. Vancouver Sun, A6

*** G20 activist to be back in court next month**
G20 activist Julian Ichim was ready for his day in court Tuesday, but the same couldn't be said for the Crown. Ichim appeared Tuesday at Old City Hall after he refused an OPP request last month to remove a blog post that contained the pseudonym of an undercover officer who had befriended him for more than a year before the Toronto summit in 2010. The Record, B3

*** Kensington man faces weapons charges**
A Kensington man faces weapons charges after allegedly threatening others with a shotgun Dec. 7. A 12-gauge single-barrel shotgun and ammunition were seized. The Guardian, A4

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

'Canada failed to take any action'
The brother of a woman believed to have been murdered by serial killer Robert Pickton welcomes a United Nations committee's plan to probe the allegation that 600 aboriginal women have been murdered or have gone missing over the last 20 years. Vancouver Sun, B3

*** Missing native women spark UN inquiry**
The United Nations is set to conduct an inquiry into Canada's cases of missing and murdered aboriginal women, two Canadian groups lobbying for the action announced on Tuesday. The UN Committee on the Elimination of Discrimination against Women - which is made up of 23 independent experts on women's issues - will hold the inquiry. The investigation was announced by the Native Women's Association of Canada (NWAC) and the Canadian Feminist Alliance for International Action (FAFIA). NWAC said it has "documented the disappearances and murders of more than 600 aboriginal women and girls in Canada over about 20 years," and believes there are more cases. Montreal Gazette, A15; National Post (Times Colonist, Starphoenix, Leader-Post); The Province; Winnipeg Free Press

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

U.S. fugitive ordered held after hearing
An American fugitive sought in the U.S. for allegedly trying to kill a police officer will enjoy Canadian hospitality for at least another week, albeit behind bars. James Louis Whittlesey, 51, had a hearing before the Immigration and Refugee Board on Tuesday during which he denied his identity, despite the fact his fingerprints confirmed otherwise. Whittlesey was taken to the Rivière des Prairies Detention Centre after his arrest on Sunday by a Montreal police tactical squad after investigators with the Canada Border Services Agency tracked him down here. The Gazette, A4

Ottawa girds for legal battle over Windsor-Detroit bridge

The Canadian government is considering the extraordinary step of using an act of Parliament to shield the new Windsor-Detroit bridge project from lawsuits launched by owners of an existing crossing. Canada and the United States last week signalled a new era of co-operation on their joint border with a deal on perimeter security, but the agreement unveiled was light on details of how much new crossing infrastructure would be built to expedite two-way trade. Globe and Mail, A5

$10M in coke plucked from Pearson
Police at the largest airport in Canada suspect corrupt workers became nervous and fled leaving behind a guitar case filled with a record 100 kilos of high-grade cocaine that was being smuggled into the country. The haul, which is worth more than $10 million, is one of the largest coke seizures found in an unclaimed item at Toronto's Pearson International Airport in recent years, investigators said. Most major organized crime gangs, including the Hells Angels, have foot-soldiers working at the airport who are involved in the smuggling of contraband, a Senate National Security Committee has found. London Free Press, B3 (Whig-Standard, Toronto Star)

Tories give value to citizenship
An editorial states, "'Canadians are generous people, but have no tolerance or patience for people who don't play by the rules and who lie or cheat to become a Canadian citizen. The government will apply the full strength of Canadian law to those who have obtained citizenship fraudulently." With those blunt words, Citizenship and Immigration Minister Jason Kenney announced last Friday that his department and the RCMP have gathered evidence on as many as 6,500 new citizens or permanent residents who acquired their immigration status fraudulently. Kenney intends to strip them of their status and deport them, if they are still in the country..." Vancouver Sun, A12

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Cowansville hostage-taking ends peacefully
A hostage-taking at a penitentiary in Cowansville ended peacefully on Tuesday evening when an inmate who had barricaded himself in a room with a staff member surrendered to a negotiating team. The nearly nine-hour ordeal began at about 10: 45 Tuesday morning. Two separate investigations will take place: one by Correctional Service Canada and the other by the Sûreté du Québec, said Abergel, who noted the latter may lead to new charges being laid against the inmate. The Gazette, A12

Theo Fleury
A letter states, "Fleury is absolutely right to attack the Canadian justice system. It is the Canadian system that "enabled" James. It is the Canadian system that gave James a pitiful sentence the first time around, and it is the Canadian system that granted him a pardon. It is the Canadian system that will hand James another pitiful sentence in this case..." The Gazette, A24

Cowansville hostage-taking ends peacefully
A hostage-taking at a penitentiary in Cowansville ended peacefully on Tuesday evening when an inmate who had barricaded himself in a room with a staff member surrendered to a negotiating team. The nearly nine-hour ordeal began at about 10: 45 Tuesday morning. Two separate investigations will take place: one by Correctional Service Canada and the other by the Sûreté du Québec, said Abergel, who noted the latter may lead to new charges being laid against the inmate. The Gazette, A12 (Edmonton Journal), * The Windsor Star, * The Record, * Le Nouvelliste (La Tribune, Le Soleil), * La Voix de l'Est, Le Journal de Montréal

Theo Fleury
A letter states, "Fleury is absolutely right to attack the Canadian justice system. It is the Canadian system that "enabled" James. It is the Canadian system that gave James a pitiful sentence the first time around, and it is the Canadian system that granted him a pardon. It is the Canadian system that will hand James another pitiful sentence in this case..." The Gazette, A24

*** Cult of ignorance**
A letter states, "Our federal government seems to think that ignorance is a virtue... On the subject of crime, it's pushing through the costly Bill C-10, whose measures have already been proven elsewhere to increase crime rather than decrease it. The government is doing this despite the advice of legal experts, and has even had the gall to question the credentials of criminologists...It is now up to our Senate to save us. Senators have their appointments until 75 and are under no obligation to toe party lines. They will still have their jobs when Harper loses his. It's time for senators to stand up to Harper's cult of ignorance and demonstrate some 'sober second thought.'" The Star Phoenix, A10

*** Dealer found dead in penitentiary cell**

A drug dealer who was found unresponsive in his cell at the Drumheller Institution has died. Officials from the federal penitentiary say he was found by correctional officers during a regular check on Monday. They tried to revive the man and he was taken to hospital by ambulance. Dang Akays Dang, 27, was serving a two-year sentence for possession for the purpose of trafficking. Calgary Herald, B3

*** Uplifting initiative**
A letter states, "My sincere congratulations to Justice Colin Westman and Crown attorneys Lynette Fritzley and Kathleen Nolan for the drug court they have initiated and developed in Kitchener. It is so uplifting and inspiring at this cold and wintry time of the year. This court, which offers help and encouragement to addicts, is a ray of hope to these people. Westman,and others, are to be congratulated and supported for this type of humane justice by treating addiction as more of an illness instead of simply a crime..." The Record, A10

*** You can't complain to your senator if there isn't one**
An opinion piece states, "...For the first time, I've noticed how removed we are from Parliament's place of sober second thought. The Canadian Senate has always seemed to me to be a pretty useless thing, like government's equivalent of the appendix. But suddenly it has found itself in the spotlight. That's because of Prime Minister Stephen Harper's controversial omnibus crime bill, which will put a lot more people in jail. It easily passed through the House of Commons thanks to the Conservative majority there. Now the only way to stop the bill is if the Senate rejects it..." The Record, B1

*** Harper majoritaire**
Sous le gouvernement Harper, la session a déjà connu 13 étapes limitées sur seulement 21 projets de loi déposés, et cela en seulement 66 jours depuis la rentrée. Selon les calculs des libéraux, la proportion des étapes législatives touchées par le bâillon atteint 61 %. Les conservateurs ont limité le temps des débats de façon considérable «pour éviter le débat sur des projets de loi controversés», croit le député libéral Marc Garneau. Parmi les projets de loi qui ont été étouffés par le bâillon, on note le projet omnibus en matière de justice criminelle (à trois différentes étapes législatives), celui pour l'abolition de la Commission canadienne du blé et même un projet de loi budgétaire. L'Acadie Nouvelle, 15, Toronto Star

*** Tories reject consideration of mental illness in major new crime bill**
Justice Minister Rob Nicholson ignored questions Thursday about how a massive new crime bill will deal with Canadians living with mental illness, including young offenders who find themselves being sentenced as adults. The Canadian Council of Criminal Defence Lawyers told MPs who were studying the bill this fall that if they only made one change to the bill, it should be to recognize people with mental illnesses need treatment before they are put in jail. The Telegram, D6

*** Libération sous quelles conditions?**
Mythes : La plupart des délinquants commettent des crimes quand ils sont en liberté conditionnelle; Un délinquant obtient automatiquement la libération conditionnelle lorsqu'il y devient admissible. Faits : 98,1% n'ont pas commis d'infraction avec violence durant leur période de liberté conditionnelle; La libération conditionnelle est un privilège et non un droit pour la personne incarcérée. Elle n'est jamais sûre de l'obtenir. Le Journal de Montréal, 19

PUBLIC SERVICE / FONCTION PUBLIQUE

*** It's not the time to gut Fisheries**
An opinion piece states, "With declining salmon stocks and concerns about fish farms and the impact of climate change, we are going to need to more knowledge than ever before. This is not the time for a dumbing-down of Fisheries and Oceans Canada. Yet the federal government has sent letters to 400 DFO employees, including about 200 scientists, warning them that they could be affected by a pending "workforce adjustment," the usual term for a large-scale termination of employees..." Times Colonist, A12

*** Integrity czar appointee faces scrutiny**
The Conservatives' nominee to become the next Public Sector Integrity Commissioner told MPs Tuesday that he had the independence and courage to investigate the possible wrongdoings of his former bureaucratic colleagues - only to find himself accused of the same issues that dogged his disgraced predecessor. Mario Dion, who has been interim commissioner for a year, found himself on the hot seat at the Commons government operations committee. He was required to explain how a career bureaucrat with his legal experience is ideal for the job and won't be swayed to protect his former colleagues. Ottawa Citizen, A6

*** Ottawa $80-billion short in pension estimate: report**
The federal government is understating the liability for its employee pension plans by $80-billion because it does not use "real world" investment returns in its calculation, a new report says. A C.D. Howe Institute study has concluded that the

federal liability for pension plans now totals $227-billion, which is $80-billion more than the government reports in its Public Accounts. Globe and Mail, B3; National Post; Toronto Star

OTHER / AUTRE

Raging imam cites Hitler
A Calgary-based imam says Muslims are being attacked in the same way Jews were before Hitler ordered their extermination. Syed Soharwardy, founder of the Islamic Supreme Council of Canada, says a regulation change requiring Muslim women to remove their niqabs and burkas when swearing the oath to become a Canadian amounts to Muslim-bashing. From intimidating and bad-mouthing the Muslim faith and belittling the Qur'an and Muslim beliefs, he drew a parallel with the treatment of Jews in Germany. Edmonton Sun, 12 (London Free Press, Winnipeg Sun, Kingston Whig-Standard)

*** More education needed to fight abuse, Kennedy tells senators**
Kennedy, a former NHL player who was sexually abused by disgraced junior coach Graham James, told U.S. lawmakers Tuesday it's OK to be angry. But it's also vital, he said, that government and sporting authorities take dramatic steps to educate adults in how to identify and prevent more abusers from finding new victims. Testifying before a U.S. Senate committee, Kennedy urged sports groups and governments to require mandatory training for any adult who signs up to work with kids. Actions taken in Canada can serve as a model, Kennedy told a U.S. Senate subcommittee on children and families. The Gazette, A2 (The Star Phoenix, National Post, Calgary Herald), Calgary Sun, The Record (Chronicle Herald, Toronto Star)

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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-14-11 6:37 AM
To: Bendelier, Kenneth
Subject: Information: 'Anonymous' hacker charged in breach of KISS' Gene Simmons' website

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Latimes
Complete item: http://latimesblogs.latimes.com/lanow/2011/12/man-feds-say-connected-to-anonymous-hackers-man-charged-in-kiss-hacking-case.html

Description:
A Connecticut man who federal authorities say is linked to the hacking group anonymous has been charged with trying to shut down the website operated by KISS frontman Gene Simmons.

Kevin George Poe, 24, of Manchester, Conn., was taken into custody without incident by FBI agents at the federal courthouse in Hartford.

Poe allegedly used the screen name spydr101 to a make denial of service attack against GeneSimmons.com. He was charged in a federal grand jury indictment in Los Angeles with one count each of conspiracy and unauthorized impairment of a protected computer.

If convicted of the two counts in the indictment, Poe would face a statutory maximum penalty of 15 years in federal prison. The case against Poe originated with an investigation by the Los Angeles field office of the Federal Bureau of Investigation.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-14-11 5:41 AM
To: Bendelier, Kenneth
Subject: Information: Anonymous computer hacker charged with cyber attack on Gene Simmons' web site

Generated by your Alert Subscription on Folder:
- Anonymous
Source: NYDailyNews
Complete item: http://www.nydailynews.com/gossip/anonymous-computer-hacker-charged-cyber-attack-gene-simmons-web-site-article-1.991137

Description:
A Connecticut man affiliated with the Anonymous hacking group was arrested Tuesday on federal charges for an attack on a website belonging to Kiss bassist Gene Simmons, authorities said.

Kevin Poe, of Manchester, Conn., made his initial appearance Tuesday in federal court in Hartford, Conn., and was released on $10,000 bond. An email message left for deputy federal public defender Deirdre Murray was not immediately returned.

Poe was indicted in Los Angeles on two counts: conspiracy and unauthorized impairment of a protected computer. If convicted of both, he faces up to 15 years in prison.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-13-11 10:49 AM
To: Bendelier, Kenneth
Subject: Important: ANTI-LGBT password dump by @ANONOPSWORLD

Generated by your Alert Subscription on Folder:
- AnonOps - GeneralActions
Source: pastebin
Complete item: http://pastebin.com/aBKf6jU4

Description:
"westwood","zhouxiaoxu@hotmail.co.uk"
"Felix1","youcanreachray@gmail.com"
"pL5ksMb3","yuji.takahara@googlemail.com"
"426hemi","yann.balastrier@gadz.org"
"m1keyboy","xsportmotorsport@gmail.com"
"johnmag","xavbiz1@yahoo.fr"
"nownT41Sp","wybijokno@yahoo.com"
"pulse17","wwebber@havering-college.ac.uk"
"Poleposition","wlwh_rich@ymail.com"
"harley","wjohnston700@gmail.com"
"voxpsil","www.bertwithane@yahoo.co.nz"
"jpayne","wolfgang.lindner@telia.com"

E-Secure-IT
https://www.e-secure-it.com

s.16(2)(c)

St-Louis, Danielle

From: Bendelier, Kenneth
Sent: December-13-11 8:55 AM
To: [redacted]
Subject: First Portugal - Now Mexico.....

http://www.examiner.com/anonymous-in-national/anonymous-mexico-strikes-operation-saferoads-a-success

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-13-11 8:53 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Mexico strikes - Operation SafeRoads a success

Generated by your Alert Subscription on Folder:
- Major Site Security Breaches - Hack / DDos Attacks
- Anonymous
Source: EXAMINER
Complete item: http://www.examiner.com/anonymous-in-national/anonymous-mexico-strikes-operation-saferoads-a-success

Description:
#OpCarreterasSeguras (Operation SafeRoads)

On Saturday, December 10, a global cadre of Anonymous hacktivists launched a number of successful strikes against numerous Mexican transportation and government websites, protesting the dangerous travelling conditions present in Mexico.

Government agencies and bus companies were targeted for being complicit in allowing the dangerous traveling conditions in Mexico to exist. At least a dozen Mexican institutional portals, among them the Federal Roads and Bridges Access and Related Services, as well as several natioal bus companies, were the subject of Anonymous cyber attacks.

Websites were taken down via well orchestrated DDoS (distributed denial of service) attacks as well as defaced by Anonymous hacktivists. For an accounting of the many strikes, with links of verification, go to Blog.AtHack.Net and/or el5antuario.org. Also, see video.

The following is an excerpt from a press release announcing demands for #OpCarreterasSeguras (Operation SafeRoads):

Government of Mexico and bus companies that provide transportation on Mexican highways, we direct ourselves to you so that you may solve a grave injustice that you have allowed for several years.

In Mxico we have two classes of citizens, those that have and those that do not have. Only five percent of Mexicans travel by airplane for economic reasons. This five percent receives from the Mexican government, and the airlines, each and every safety and security guarantee accorded by law. It is for this reason that passengers on Mexican airlines are not kidnapped, raped or robbed since every security procedure has been implemented.

However when it comes to Mexicans that cannot afford air travel, but must travel by bus through our highways, these same safety and security procedures are non existent. Therefore, the Mexican bus passenger faces kidnapping, rape and robbery on his own highways.

The bus companies as well as the Mexican authorities have decided to pursue a strategy of silence in order to avoid financial losses and minimize a tarnished image in other countries

But this must end.

We have five demands for the bus companies and the Mexican government:

1. All buses, regardless of company, route, or line, should travel on toll highways. This should reduce criminal acts directed against bus passengers, providing a safer environment.

2. All buses should install a GPS locator system that will aid in locating the bus at any time in the event of a kidnapping.

3. All buses should install a real-time camera and silent alarm with a double backup system, one which transmits in real time and which will be constantly monitored, and the other which records all activity within the bus at all time. In the event of a kidnapping or unauthorized stop, the silent alarm can be activated and the camera will show and record the person or persons responsible.

4. A bus marshal will be placed on each bus, whether a specially trained security guard or a member of the Armed Forces, to aid in keeping passengers safe and as a deterrent to possible criminal activity.

5. We demand that as unarmed civilians, in a declared war between the government and criminal factions, all citizens of Mexico and those foreigners traveling on Mexican soil, be held under the articles of the Geneva Convention, and as non-combatants, be granted the immunities and humanitarian treatment so outlined in said treaties.

On Facebook, Chihuahua Anonymous thanked the following Anonymous collectives for participating in the wide ranging cyber attack:

Anonymous Mexico and the respective pages of the states in which stand Mexico Anonymous Tamaulipas, Anonymous Chihuahua, Guanajuato Anonymous, Anonymous Coahuila Mexico, DF Mexico Anonymous, Anonymous Veracruz, American Hackers, Anonymous EUA, anonymous El Salvador, Anonymous Argentina, Colombia Anonymous, Anonymous Germany, Spain Anonymous, Anonymous Europe, Ibero Anonymous and Anonymous Asia.

While the successful attacks are sure to gain media attention in Mexico and other locations in Latin America, it remains to be seen if government and transportation authorities will get the message, and take further precautions to safeguard travel by bus in Mexico.

E-Secure-IT
https://www.e-secure-it.com

Anderson, Windy

From: Bendelier, Kenneth
Sent: December-13-11 8:55 AM
To: * NCSD-CCIRC
Subject: First Portugal - Now Mexico.....

http://www.examiner.com/anonymous-in-national/anonymous-mexico-strikes-operation-saferoads-a-success

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

s.16(2)(c)
s.15(1) - Subv

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: December-13-11 8:06 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Salas, Anik; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
December 13, 2011 / le 13 décembre 2011

Print media

Trojan virus could download child porn
Somebody could have used a Trojan virus to hack into security expert Daniel Clayton's laptop, downloaded child pornography and exited without a trace, a computer expert testified on Monday. Gerald Vaselenak, systems adviser for the department of computer sciences at the University of Calgary, said such viruses may not easily be traceable but could have attached themselves to one or more files. Calgary Herald

Online media

Speculation rife as Gillard gobbles cyber security
Julia Gillard will take command of cyber security policy away from the Attorney-General's Department (AGD) under a sweeping cabinet reshuffle that also claimed the scalp of Federal Attorney-General, Robert McClelland. In a single line buried within the Prime Minister's press speech, but not read by Gillard, the Federal Government announced that "responsibility for cyber security policy will move from the Attorney-General's portfolio to my portfolio". SC Magazine; Computerworld

U.S. Homes In on China Spying
U.S. intelligence agencies have pinpointed many of the Chinese groups responsible for cyberspying in the U.S., and most are sponsored by the Chinese military, according to people who have been briefed on the investigation. Armed with this information, the U.S. has begun to lay the groundwork to confront China more directly about cyberspying. Wall Street Journal

Website knows what you've illegally downloaded
A new website that keeps track of everything you download from file-sharing sites could spell trouble for the scores of people who steal copyrighted music and movies. The site, Youhavedownloaded.com, does exactly what its name implies: It keeps a huge database of millions of media files that have been downloaded to tens of millions of Internet Protocol (IP) addresses from file-sharing websites and services such as BitTorrent. MSNBC

Most China-based hacking carried out by 'select few'
U.S. cybersecurity analysts believe that as few as 12 different Chinese groups could be responsible for the majority of cyberattacks on the United States. Experts suggest that this 'select' set of hacking groups may be backed, or directed by the Chinese government itself. ZDNet

Cyber attacks could wreck world oil supply

Hackers are bombarding the world's computer controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil supply disruption. Oil company executives warned that attacks are becoming more frequent and more carefully planned. Vancouver Sun; BBC News

Microsoft Releases Windows Defender Offline for Systems That Can't Go Online
Software giant Microsoft has unleashed the beta version of a new tool which allows users to remove pesky rootkits and other dangerous malware from the system. The Windows Defender Offline has been designed for computer systems that are infected with malware to the point of not being able to boot and connect to the internet properly. ITProPortal

Google pulls fraudulent apps from Android Market
Google has recently removed 22 fraudulent apps from Android Market that rack up hidden charges for unsuspecting users who downloaded seemingly innocent services, such as horoscopes, wallpapers and games. Apparently, these forecasts and other apps have been ploys for criminals to lure consumers into clicking on options that led to premium charges tied to SMS usage. MSNBC

Android Malware Found in Fake 'Angry Birds,' 'Cut the Rope,' and More
Over the weekend more premium rate SMS Trojans surfaced in the Android Market, this time within legitimate-looking versions of popular games like Angry Birds and Cut the Rope. When downloaded, the games install a premium rate SMS Trojan that sends text messages to premium line numbers, leaving you with the bill. PC Magazine

The new age of malware
Smart devices, social media and increased online activity through app stores and other transaction-based websites are coming together in what one researcher says is a scary combination of factors that have dire implications for national security. Network World

New malware could knock out antivirus systems
A dangerous new breed of malware or malicious software could knock out computer security systems, leaving them exposed to cyber attacks or hostile governments, warn researchers. Murray Brand, senior lecturer in computer science at Australia's Edith Cowan University, says the processing power needed to scan for and delete malware may soon outstrip the capacity of most computers. Economic Times

'Duqu' zero-day Windows flaw patched this week
Microsoft will tomorrow patch the zero-day kernel Word vulnerability exploited by the mysterious Duqu malware, more than a month after its existence was first made public. In a pre-release draft covering the 13 December Patch Tuesday release that excluded helpful security bulletin numbers, Microsoft appears to have slipped in a fix for the elevation of privilege flaw (CVE-2011-3402) in Win32k TrueType font parsing engine hijacked by Duqu. TechWorld

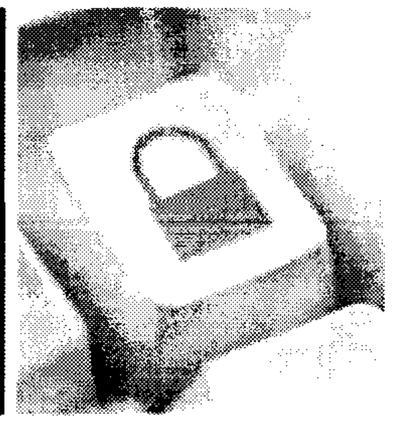
Lulzlover Hacked Coalition of Law Enforcement, Data Dumped for 2,400 cops and feds
In support of OWS, an AntiSec hacker chose to lock and load on C.L.E.A.R. (Coalition of Law Enforcement and Retail), hack the website, and dump the entire member database. Passwords, phone numbers, email and home addresses, and other digital dirt was posted for over 2,400 law enforcement, feds, military, loss prevention professionals, and big corporations like Microsoft. Network World

The academics of Anonymous
If the word "doxing" makes you think of puppies, and the word "hacker" has you imagining a zit-faced, social outcast eating junk food in his or her parents' basement, it's time to head to the anthropology section of your local library or bookstore and start reading up on "hacktivism," or online activism. Washington Post

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-008



For the Week of

3 Dec – 9 Dec 2011

Issued: 16 Dec 2011

HIGHLIGHTS:

Threat Warnings: Nothing significant to report.

CCIRC Products: CCIRC sent the following Cyber Flashes to stakeholders.

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
- CF11-026: Widespread SQL injection campaign
- CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

Incidents to report:

- Malicious e-mails from threat actors impersonating a Canadian federal agency, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems in the provincial government, financial, health, telecommunications and education sectors
- SQL injection attacks infected thousands of legitimate websites around the world, resulting in re-direction of internet users to a malicious websites. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

Noteworthy Open Source Reports:

- A draft US Bill in cyber security gets support from privacy proponents
- White House announces cloud security "rules of the road" for US federal agencies and contractors
- Hacker groups successfully attack websites of the Portuguese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

CCIRC PRODUCTS RELEASED THIS WEEK:

CCIRC sent three Cyber Flashes to key stakeholders – mainly IT professionals and managers in government, critical infrastructure and related sectors.

CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator. CCIRC has been receiving reports of various spear phishing campaigns that may be associated with Advanced Persistent Threat (APT) activity. This Cyber Flash highlighted the technical details of such recent attacks so stakeholders can check if they have been victimized. CCIRC also offered references for additional background information and mitigation advice.

CF11-026: Widespread SQL injection campaign. CCIRC received reports of a recent and broadly distributed SQL injection campaign. This world-wide attack campaign resulted in compromised websites redirecting unsuspecting site visitors to a malicious website, reportedly hosted in Moldova. It is estimated the campaign affected over 160,000 websites in the world, including Canadian ones. SQL injection attacks are a common and effective way to compromise legitimate but vulnerable websites in order to perpetrate malicious acts.

CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products. The purpose of this cyber flash is to raise awareness and offer mitigation for a number of unpatched vulnerabilities affecting versions of Adobe Reader, Adobe Acrobat and Adobe Flash products. CCIRC believes one of these vulnerabilities may have been leveraged in targeted attacks against the defence industrial sector.

NOTABLE INCIDENTS– 3 DECEMBER THROUGH 9 DECEMBER 2011:

Canadian Critical Infrastructure:

Federal Government. E-mails from threat actors impersonating a federal agency tried to entice internet users to a malicious website located in China. CCIRC notified its Chinese equivalent organization (China CERT) and recommended deactivation of the malicious website (still pending). CCIRC also reported the incident to Google as well as the Anti-Phishing Working Group (APWG).

Threat actors impersonating the same federal agency tried to entice internet users to a malicious website and tried to persuade them to reveal personal information (ex: name, social insurance and credit card numbers). The request was traced to a Romanian website hosted in the U.S. CCIRC

notified the internet service provider and informed US CERT (American equivalent of CCIRC). The malicious content had been removed from the website later that week.

- **Analysis:** CCIRC cooperates with computer incident or emergency response centres around the world, including US and China CERT. This type of incident for this agency occurs on a weekly basis. CCIRC works with the organization as well as the Canadian Antifraud Centre to have these malicious websites deactivated as quickly as possible.

Provincial Government. A provincial health organization was one of the victims of the wide-spread, world-wide, SQL injection attack described above for Cyber Flash CF11-026. The impact on the organization and the number of web-site visitors victimized is unknown. CCIRC notified the provincial government contacts and gave mitigation advice.

CCIRC also received infection reports for another provincial government's computer systems. Possible impacts can range from data theft to taking control of those computers to send SPAM. CCIRC notified the provincial contacts and gave mitigation advice. Impact on the organization is unknown.

- **Analysis:** These types of infections, commonly seen by CCIRC, could potentially lead to a compromise of that government's computer system. There is no information to suggest these were targeted attacks on that system.

Financial Sector. CCIRC received infection reports for a Canadian financial institution, which indicates potential computer compromises on the organization's network facing the internet. The impact on the organization and its clients is unknown. CCIRC notified the organization and offered mitigation advice.

- **Analysis:** The infections reported for this institution are commonly found on the internet, probably passed on from an on-line bank client who does not practice good cyber security. In CCIRC's experience, financial institutions pay keen attention to cyber security, because they are aware they are attractive targets to cyber criminals. Cyber security is understood to be a risk mitigation measure that will minimize a bank's financial losses and protect its reputation.

Telecommunications Sector. CCIRC received infection reports for two Canadian internet service providers and notified the organizations. These reports indicate there were likely compromises of computers belonging to internet users subscribing to those providers.

A large telecommunications service provider was one of the victims of the wide-spread, world-wide, SQL injection attack described earlier. This attack resulted in compromised websites redirecting unsuspecting site visitors to malicious websites. It is unknown how many client computers were compromised as a result of this malicious activity. CCIRC notified the service providers and gave mitigation advice. A Cyber Flash was also issued because of the estimated wide-spread impact.

Health. CCIRC received reports on potential compromises for a municipal Canadian health service provider and notified the organization. CCIRC does not have any information to indicate these compromises relate to a targeted attack.

Other Sectors:

CCIRC received reports on potential compromises for a Canadian university and notified the organization. A local real estate board was also the victim of the SQL injection attack described earlier in the report.

Noteworthy Open Source Reports:

A draft US Cyber security bill gets nod from privacy proponents. The House Homeland Security Subcommittee on Cyber security, Infrastructure Protection and Security Technologies held hearings on a draft cyber security bill. This bill proposes cyber-threat information sharing between the public and private sectors via a not-for-profit National Information Sharing Organization. This organization, would be led by DHS and consist of privacy advocates, representatives from critical infrastructure industry sectors, state and local government. The Center for Democracy and Technology, a US civil liberties group, publicly favours this draft bill over the other draft bill (H.R. 3523) because of its "superior information sharing stipulations".

Analysis: The House Intelligence Panel has already approved a competing draft cyber security bill that expands the pilot cyber threat information sharing program between the Defence Department and defence contractors. Privacy groups are concerned would this bill would allow Internet service providers to share private communications with the government. Of particular concern would be any customer data disclosure to the National Security Agency (NSA), who ran the pilot information sharing program.

US agencies and contractors get rules of the road for cloud security approvals. The White House announced that cloud providers to US federal agencies will have to comply with new uniform security requirements, by June 2012. US officials said agencies have shifted 40 IT services, such as email and collaboration software, to the cloud, in the past year. Seventy-nine more services have been identified for transfer to the cloud by June 2012. The newly announced Federal Risk and Authorization Management Program (FedRAMP), is expected to allow for more rapid and cost-effective deployment of cloud services for multiple US government agencies. Reports suggest an estimated $5 billion savings could result.

- **Analysis:** Cloud computing and securing data in a cloud is also a current topic of discussion in Canada. Though there are no specific official guidelines for cloud computing in the Canadian federal government, there are Treasury Board guidelines for outsourcing IT infrastructure and services.

- Cloud computing allows one to store and process one's data in an off-site computer system owned by a third party. This data can be accessible from almost any location. This feature, coupled with the proliferation of smart mobile devices, has brought cloud computing heightened attention. A recent survey by CSC, a US technology company, suggests that allowing employees mobile access to data, rather than saving money, was the reason for moving data to the cloud for many organizations.

Hacker groups successfully attack websites for the Portuguese Government, Columbian Army, Mexican Government and the PR firm for Monsanto. Open sources reported that Lulzsec Portugal, a self-proclaimed activist group, disabled the websites of **Portuguese government**, National Police, House of Parliament and several political parties. Reasons given for the attack were the Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest.

Anonymous, the famous international hacker group, successfully attacked the **Columbian Army**'s website. The motive given was to avenge a recently televised shooting of a seemingly harmless dog by soldiers. Anonymous also took down websites of numerous Mexican transportation and government websites, protesting the "dangerous travelling conditions present in Mexico".

Anonymous also executed a successful attack on a public relations firm working with Monsanto, as part of "Operation End Monsanto". The public relations firm, Bivings, reportedly had its website defaced and data stolen. Shortly after the incident, the firm liquidated their assets, and employees started a new public relations company. Monsanto is a large international producer of genetically engineered seeds and pesticides. It is the target of a number of activist groups and was named "Worst Company of 2011" by an environmental activist group.

- **Analysis:** Even though LulzSec was declared defunct in June 2011, affiliated hacker groups are still operating successfully around the world. Anonymous continues to target and successfully execute attacks around the world against vulnerable targets for activist purposes. Anonymous threatened to attack the Toronto Stock Exchange in support of the "Occupy" movement earlier this year. CCIRC is unaware of any incidents resulting from this threat.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-13-11 7:45 AM
To: Bendelier, Kenneth
Subject: Information: Anonymous attack didn't harm HBGary's business, says CEO

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: TechWorld
Complete item: http://news.techworld.com/security/3324397/anonymous-attack-didnt-harm-hbgary-federals-business-says-ceo/?olo=rss

Description:
When HBGary Federal, had its website hacked and sensitive e-mail exposed by hacktivist group Anonymous last February, it became a question of how Sacramento, California-based security firm HBGary could survive the damage to its reputation.

In spite of the bruising, HBGary not only didn't lose business customers in the course of the past year, but "we ended up getting additional business," claimed Greg Hoglund, founder and CEO of HBGary.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-13-11 7:05 AM
To: Bendelier, Kenneth
Subject: Important: Retrospective Video by Anonymous Includes Ominous Warning

Generated by your Alert Subscription on Folder: - Anonymous
Source: Mashable
Complete item: http://mashable.com/2011/12/11/retrospective-video-by-anonymous/

Description:
The controversial Internet hacking group known as Anonymous created this retrospective video commemorating a tumultuous year in the world of anarchy and subversive activism. Its LulzXmas video is a complicated and picture-packed montage of mayhem, where the groups point of view doesnt exactly come into sharp focus, but you can get an idea of what sort of year some of its members think weve just gone through.

The group doesnt speak with one voice. It consists of many free spirits who want to change the world and are willing to employ a variety of digital methods both constructive and destructive, and often just mischievous to make that happen. Heres how the group announced the video in a tweet:

@YourAnonNews: ANONYMOUS LULZXMAS VIDEO: http://t.co/rSqwQ3Gg We made a list, checked it twice. Gonna find out what companies have been naughtynot nice.

From the videos eerie beginning with its We do not forgive and we do notforget motif, to the tweet with its ominous warning to companies that havent been nice, to its final admonition to prepare yourself for 2012, Anonymous has certainly enshrouded itself in mystery and foreboding.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-13-11 7:03 AM
To: Bendelier, Kenneth
Subject: Important: The academics of Anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Washington Post
Complete item: http://www.washingtonpost.com/blogs/innovations/post/the-academics-of-anonymous/2011/12/11/gIQA1F8jpO_blog.html

Description:
If the word doxing makes you think of puppies, and the word hacker has you imagining a zit-faced, social outcast eating junk food in his or her parents basement, its time to head to the anthropology section of your local library or bookstore and start reading up on hacktivism, or online activism.

Academics have been studying the very non-academic undertakings of hacktivists, predominantly groups such as Anonymous, for years. These include the repeated hacking of the Church of Scientology Web site, the infamous online message board 4Chan, and the philosophy of doing it for the Lulz. Their findings, while not your average classroom fare, are helping to paint a picture for policy makers of a leaderless, geographically and socio-economically diverse and powerfully disruptive group.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-13-11 6:53 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous warns of Lulzxmas

Generated by your Alert Subscription on Folder:
- Anonymous
Source: The Inquirer
Complete item: http://www.theinquirer.net/inquirer/news/2131741/anonymous-warns-lulzxmas

Description:

HACKTIVIST GROUP Anonymous has posted a video that celebrates its year to date and suggests more activity over the Christmas period such as attacks on naughty businesses. "Epic year isnt [it]?" says a caption about half-way through a video that features most of the activities of the group to date and the headlines it has gathered. "And it was just the beginning. Please fasten your seat belts for this Lulz Xmas".

In cuts between videos, Oprah opens the show and there are screengrabbed headlines and articles - the INQUIRER makes an appearance - and the video then borrows from the Charlie Chaplin classic The Great Dictator, specifically a polemic scene that rails against dictatorships and the machine and supports universal brotherhood.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-12-11 11:55 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous - OpRobinHood - Anonymous and TeaMp0isoN have joined forces to fight censorship

Generated by your Alert Subscription on Folder:
- Anonymous
Source: You Tube
Complete item: http://www.youtube.com/watch?v=Hrvo5SEYk6E&feature=share

Description:
Anonymous and TeaMp0isoN have joined forces to fight censorship in the name of OpCensorThis. There is a new operation that has been taking place over the actions of Banks in response to the Occupy Movement. We have watched our brothers and sisters being refused their hard earned money by the banks on top of being beaten and brutalized by officers during peaceful demonstrations. Congratulations banks, you have gotten our attention.

You ignore your customers and use authorities to censor their voices. Operation Censor This will not stand for such acts and is spawning another operation under Operation Cash Back which already removed well over 500,000 accounts from banks and put them into credit unions. This is the next step. Banks have stolen millions from its customers as well as lacked the security to protect them. We give you Operation Robin Hood.

E-Secure-IT
https://www.e-secure-it.com

St-Louis, Danielle

From: Hatfield, Adam
Sent: December-12-11 4:48 PM
To: Anderson, Windy; Labelle, Sébastien
Cc: St-Louis, Danielle
Subject: FW: As requested. For Adam's questions
Attachments: FW: ERWG Introductory letter; Government of Canada Cyber Security Incident Reporting Trigger Criteria.xls; FW: For your reading pleasure; vulnerability assessment.xls; cvss-blank-scoring-1.0-sr.xls

Hi Windy,

Thanks for this, it is helpful to know. On the issue of when an issue gets escalated to Robert, I really think Robert needs CCIRC to state in plain English what the current protocol would be so that he can understand and react.

Sébastien, a number of the comments from Luc below are related to engagement with key partners – CSTAC, CIRA (the Canadian Internet Registration Authority), the Industry Canada Spam Centre, etc. Happy to decode acronyms as needed.

Thanks,
Adam

From: Anderson, Windy
Sent: December-06-11 3:46 PM
To: Hatfield, Adam
Cc: St-Louis, Danielle
Subject: FW: As requested. For Adam's questions

Adam,

After our conversation yesterday, I came back and asked Luc tons of questions. He has attempted to address all the questions in this email. Can you let me know if you require anything further from us or if this is sufficient – or at least a good start? Thanks.

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

From: Beaudoin, Luc S
Sent: December-06-11 3:43 PM

To: Anderson, Windy
Cc: St-Louis, Danielle
Subject: As requested. For Adam's questions

1. ERWG, under CSTAC. Update and situation attached.
2. RCMP SIR: We do not have access and do not think we need to or should. The SIR is mostly physical events related. We trust RCMP will share with us events of interest that are Cyber and require our attention.
3. CIRA: we have a working relationship with CIRA. They are our DNS experts and we like to solicit their opinion on issues such as DNSsec and BIND vulnerabilities. We have no MOUs with them at this time but Bud's team had started working on that front. We have had a number of meetings with CIRA in the past 20 months. They are a key strategic asset for CCIRC.
4. Spam Centre: Meetings with CRTC and IC have taken place over the last 12 months. Specifically, CCIRC is hosting a recurrent Ops-meeting with them and IC, RCMP TCB, Antifraud centre, and CTEC. One took place in Sept, and one in Nov. The Spam Centre contract is on MERX and the law is not expected to come into force before next summer. Our next meeting with CRTC will be in Jan.
5. Escalation to the GOC: Any incidents having a significant impact on Canadian CI sector may be reported to the GOC provided it is ***not*** associated with an on-going investigation and/or caveated not for distribution. Sensitive matters will be escalated using existing executive reporting. CCIRC provides routine reporting to the GOC on a daily basis.
6. Escalation: How is risk assessment performed at CCIRC ? Every morning at 0830h, we review and assess cyber issues. This process draws from expertise from CCIRC team members. Risk Asessment in Cyber Space is an unsolved problem, so we rely on expertise and experience to judge criticality. Some guidelines include: (from some of our SOPs)

1) For Vulnerabilities: use CVSS methodology as a starting point (tools attached) . CVSS of 9+ minimum can be candidates, as per NIST NVD; zero-days on any of the following products common versions can be candidate: CISCO, MS Office, Windows, BlackBerry, Linux, Mac, ie, firefox, Apache, Oracle, MySQL, JavaVM, other significantly used plateforms in ISPs, government and large corporations - critical infrastructure owners, and general users (due to second order impact of having a very large number of devices affected).
2) For Threats: many reports of use in the wild with tool-integration (like metasploit), or affecting largely popular canadian websites (ex: cbc.ca), or theme (ex: G20)
3) For News, threats and vulnerabilities: High media attention (ex: government website being hacked), potential for significant impact on security (ex: Anonymous targeting, SCADA, etc), main stream media pick up (GhostNet, Mariposa, TBS), etc.
4) For incidents: actual and significant impact on one or many Canadian CI.

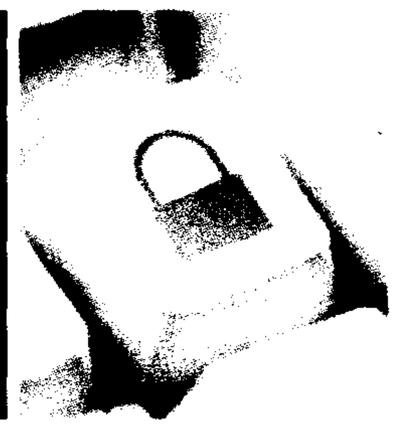
7) TOR for U5: the latest version was produced by Andrew. Attached. I have hand written comments not included. A rapid review took place in London but it was decided if I recall to look into this further at future opportunities (next U5).

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

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-007



For the Week of

26 Nov – 2 Dec 2011

Issued: 8 Dec 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released:** Nothing to report.

- **Incidents to report:**
  - A provincial government's computers potentially infected
  - A compromised Canadian website redirecting visitors to a malicious website in Russia
  - Threat actors impersonating reputable Canadian financial and telecommunications organizations, luring internet users to malicious websites (phishing)
  - Distribution of malicious software that steals passwords traced to a Canadian Internet Protocol Address
  - Canadian credentials compromised in the UN Development Program website hack

- **International:** Foreign government officials' e-mail accounts and passwords compromised

- **Noteworthy Open Source Reports:**
  - Chinese cyber spies sought Potash deal secrets
  - Spoof Health Canada E-mail offers shovelling credit
  - Carrier IQ snoops on US cell users
  - Cybersecurity bill approved by U.S. House panel

UNCLASSIFIED
DRAFT

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and other noteworthy open source reports.

NOTABLE INCIDENTS– 19 NOVEMBER THROUGH 25 NOVEMBER 2011:

Canadian Critical Infrastructure:

Multi Sector Event Update. CCIRC notified 147 organizations in multiple sectors that were victims of Operation "Ghostclick", the massive DNS changer fraud exposed by the FBI two weeks ago and reported in the last two CCIRC Weekly Summary reports. Canadian organizations that were notified this week included internet service providers, information technology companies, post-secondary schools, health and media organizations.

- **Analysis:** This was a world-wide fraud where victims are still being notified by CCIRC and its international equivalents around the world. It is estimated that this fraud went on for four years.

Financial Sector.

Threat actors impersonating well known financial entities attempted to steal personal information by persuading internet users to click on links to malicious websites (phishing). CCIRC found one malicious website still in operation and notified the entity being impersonated. CCIRC also notified Google phishing, and the Anti-Phishing Working Group so internet users may be alerted if they encounter these specific malicious websites. The number of victims is unknown.

- **Analysis:** This type of malicious activity is commonly seen by CCIRC and continues to cause financial losses for Canadians. It is known that the malicious website is hosted in Seoul, Korea.

CCIRC also learned that the website of a financial institution was vandalized. CCIRC notified the organization of this website defacement and offered mitigation advice.

- **Analysis: This type of** malicious activity usually does not put a financial institution's operations in jeopardy but could threaten the visitors to that website. Website defacement does, however, indicate the vulnerability of the website to malicious activity by threat actors. A common malicious activity is placement of malicious software on the website that would be passed on to any visitor to that website, and compromise his/her computer, then steal information or use it to send SPAM e-mails anonymously.

Telecommunications Sector – an Update.

Last week CCIRC reported that a Canadian domain name registrar was victim a of a cyber-attack, and that its stolen customer contact list was then used by criminals to persuade customers to provide their credit card numbers. These credit card numbers were used in recent purchases. **A federal agency is now leading the investigation.**

- **Analysis:** While CCIRC regularly sees threat actors impersonating trusted entities to persuade internet users to give their personal and financial information, this is the first time in recent memory an internet registration authority in Canada has been successfully targeted. The impact of a trusted entity's compromise can be much greater than an individual or an organization. **This matter is considered of national interest because of the significance of this registrar.**

Public. CCIRC discovered that the user credentials for a Canadian newspaper website's special section were stolen. The loss of these credentials could lead to the users' personal information being compromised. CCIRC is not aware of the number of victims.

- **Analysis:** The newspaper's special section is aimed at a specific reader group, which is a small subset of this newspaper's regular readership. However, the stolen user credentials were posted on the internet and could allow any threat actor to gain access to these users' personal information such as their name, address, phone number and workplace. Unfortunately, this type of compromise is being seen on a regular basis in Canada.

CCIRC Products: Nothing to report

International:

UK releases updated Cyber Security Strategy. The UK government released an update to its Cyber Security Strategy, which was published two years ago. There is an increased emphasis on information sharing between the public and private sector, reaching out to industry sectors previously not considered as part of UK's critical infrastructure, and increased military capability in cyber security to gain comparative advantage. Increased efforts to improve the public's cyber security include working with internet service providers to develop a voluntary code of conduct for situations where customers suspect their computer has been compromised. In addition, a new Cyber Crime Unit within the National Crime Agency will be created. UK Government intends to continue working internationally to help improve cyber security in the UK and in the world. The National Cyber Security Programme based on this strategy has been allocated £650m over the next four years.

- **Analysis:** The UK sees cyber security in terms of national security and economics. The UK government publicly stated that their aim was to make UK a safe place to do business online, and gave warning that it intended to deter and defend itself against advanced threats by

nation-states. The Government of Canada released its own cyber security strategy in 2010, which, similarly, focuses on protecting government systems, working with the private sector to protect critical infrastructure systems and helping Canadians to be secure online. These initiatives have been allocated $90M over five years. Canada is a strong partner of the UK in helping determine the global "rules of the road" for cyber security.

Noteworthy Open Source Reports:

UK banks set for cyber security 'stress test'. Eighty-seven British banks, including major institutions such as Barclays, HSBC and Royal Bank of Scotland, took part in a simulation exercise that tested their defences against a cyber-attack. The test scenarios included automated teller machines (ATMs) being down due to a cyber-attack. The exercise also examined how financial institutions would cope if there was a major disruption to the transport infrastructure during the London 2012 Olympic Games. An Exercise Report discussing the results of the test is expected to be published in early 2012. The Financial Services Authority stated there would also be a Post Exercise Conference.

Analysis: The London 2012 Olympic Games were featured in a test scenario and were likely a factor in prompting this cyber security exercise. The Olympic Games could have an impact on a bank's response to a cyber attack if less bank staff is available for duty where many could be watching or attending the games. There could also be an impact if there were a major disruption to the transport infrastructure at the same time as a cyber attack, and there were difficulties in physically mobilizing staff to respond to this attack. The UK Government has made it clear that cyber security is a national priority. The updated UK Cyber Security Strategy was released publicly on November 25, 2011.

More Facebook scams reported. Open sources reported two separate scams targeting Facebook users. In the first instance, threat actors reportedly impersonated Facebook administrators and sent e-mails to users charging them with violating policy regulations. Users were then asked to pass along their account details, which included personal and financial information.

In the second instance, which occurred during American thanksgiving weekend, Facebook users were lured to give up their personal information by an offer of a program that would allow watching live streaming video of football games. The number of victims in both instances is unknown, though many Facebook users did report these spams to the legitimate Facebook support site.

- **Analysis:** Facebook is one of the world's most popular social networking websites. There are reportedly 16.6 Million Facebook users in Canada. Federal public servants were recently encouraged by the President of Treasury Board to use social media in the course of their work and government guidelines have just been released on the subject. Accordingly, a compromise or SPAM campaign in social media websites in the future may also affect federal departments as well as other workplaces. This risk will need to be managed by appropriate departmental officials.

Public Safety Canada | Sécurité publique Canada

Canada

UNCLASSIFIED
DRAFT

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-12-11 12:09 PM
To: Bendelier, Kenneth
Subject: Important: Florida Family Association hacked and warned by Anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
Source: cyberwar news
Complete item: http://www.cyberwarnews.info/2011/12/12/florida-family-association-hacked-and-warned-by-anonymous/

Description:
A hacker going under the Anonymous/antisec flag has spent a bit of time on the Florida Family Association servers, grabbed some data and left a nice warning with the leak of data.

The dump of information and warning was first posted via ihazcAnNONz twitter account and dumped on pastebin.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-12-11 7:13 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous: OpEndMonsanto claims first victim

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - Green Rights
Source: TGDaily
Complete item: http://www.tgdaily.com/security-features/60126-anonymous-opendmonsanto-claims-first-victim

Description:
Cyber activists associated with Anonymous are claiming credit for the ostensible demise of a PR firm that once represented Monsanto, the US-based multinational agricultural biotechnology corporation. The Bivings Group recently fell victim to a team of Anonymous hackers, which extracted and publicly posted the contents of a site database, along with hundreds of stolen emails. The group also rooted a number of servers and defaced the company website.

Shortly after the incident, Bivings shut down all servers, liquidated company assets and officially closed its doors. A number of former Bivings employees then opened a new PR company known as The Brick Factory. "This is after 15+years of running marketing campaigns and helping some of the most corrupt corporations on the planet, as well as several governmental agencies, cover up their dirt," Anonymous wrote in a communiqu.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-11-11 12:03 PM
To: Bendelier, Kenneth
Subject: Important: OpTylerDox1 - Message from Anonymous

Generated by your Alert Subscription on Folder:
- Anonymous
Source: pastebin
Complete item: http://pastebin.com/u33YCLEz

Description:
Video Upload @ http://www.mediafire.com/?lobuck363392ndy
Basic Dox @ http://pastebin.com/u33YCLEz

Citizens of the United States.

We are Anonymous.

In recent months press and Occupy protesters have had their first amendment rights infringed upon, as members of the house and senate continue efforts to subvert your constitutional rights. As if the Patriot Act weren't unconstitutional enough, the National Defense Authorization Act threatens to declare the United States a war zone and allow indefinite detention of Occupy protesters. The National Defense Authorization Act passed the U.S. Senate with 93 Yay votes and only 7 Nay votes, the bill was sent back to the House and is now known as H.R.1540, it is being sponsored by Rep. Howard P. McKeon and co-sponsored by Rep. Adam Smith.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-11-11 12:28 AM
To: Bendelier, Kenneth
Subject: Information: Anonymous' LulzXmas(video)

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: YouTube
Complete item: http://www.youtube.com/watch?v=BdqoSWtYpHE&feature=youtu.be

Description:
Anonymous' LulzXmas (video)

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-10-11 3:45 PM
To: Bendelier, Kenneth
Subject: Information: AnonOps Turns One: Anonymous' Three Best Hacks to Date

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: ibtimes
Complete item: http://uk.ibtimes.com/articles/263923/20111209/anonops-turns-anonymous-best-hacks-date.htm

Description:
Anonymous is one today, celebrate or weep the collective has survived a full year.
With Anonymous AnonOps site being born exactly one year ago, the International Business Times UK takes you through three of the collective's best moments to date.

1) Anonymous Hackers Release Evidence of Brazilian Government Corruption

Back in August, Anonymous released a series of files allegedly proving corruption within the Brazilian Government.

Links to the data were posted alongside a statement on the pastebin website on Wednesday 10 Aug, 2010. In its accompanying statement Anonymous claimed to have released "evidence revealing government cover-up of a corruption investigation involving the CIA, the Brazilian telecom industry, and multiple US corporations."

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-10-11 3:31 PM
To: Bendelier, Kenneth
Subject: Information: Anonymous and LulzSec accused will stand trial in November 2012

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://the-anonymous-daily.com/2011/12/anonymous-and-lulzsec-accused-will-stand-trial-in-november-2012/

Description:
Peter David Gibson, Ashley Rhodes, Christopher Weatherhead and 17-year-old student given provisional trial date

Josh Halliday guardian.co.uk, Friday 18 November 2011 13.26 EST

The accused were arrested earlier this year by police investigating online attacks by the hacking groups Anonymous and LulzSec.

Four British men charged with computer hacking in connection with online groups LulzSec and Anonymous will not stand trial before November next year.

The four Peter David Gibson, 22, Ashley Rhodes, 26, Christopher Weatherhead, 20 and a 17-year-old student were given a provisional trial date of 7 November 2012 at a short hearing at Southwark crown court in London on Friday.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-10-11 10:09 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous'' threatening a cyber attack on Mexican agencies, bus companies

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: My sanantonio
Complete item: http://www.mysanantonio.com/news/local_news/article/Anonymous-threatening-a-cyber-attack-on-2391932.php

Description:
The group Anonymous, whose members are sometimes called hactavists for using cyber attacks to promote causes, has said it is targeting Mexican government agencies and bus companies for failing to protect citizens traveling on the country's dangerous highways.

Drug cartel members or other outlaws taking advantage of the lack of security brought on by the Mexican government's war against the cartels have taken to hijack motorists and assaulting commercial bus passengers.

The group says it will launch attacks on the agencies' and companies' websites Saturday if they do not meet demands laid out by one of the Anonymous factions.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-10-11 1:58 AM
To: Bendelier, Kenneth
Subject: Information: OpRobinHood And His NOT So Merry (Anonymous) Men...

Generated by your Alert Subscription on Folder:
- Anonymous
Source: IT Proportal
Complete item: http://www.itproportal.com/2011/12/07/oprobinhood-and-his-not-so-merry-anonymous-men/

Description:
The hacking groups TeaMp0isoN and Anonymous have been busy over the last week, with their latest Operation "OpRobinHood" -

"Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks. Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people there money back."

E-Secure-IT
https://www.e-secure-it.com

St-Louis, Danielle

From: St-Louis, Danielle
Sent: December-09-11 1:47 PM
To: [redacted] Champoux, Martin; Coady, Therese; Danaitis, Algis; Dick, Robert; Dole, Natalie; Dvorkin, Corey; Hatfield, Adam; Labelle, Sébastien; Panchyson, Dorian; Selman, Semira
Subject: CCIRC WEEKLY SUMMARY FOR WEEK OF 28 NOV
Attachments: PS-SP-#527919-v1-FEEDBACK_FORM_FOR_WEEKLY_SUMMARY_FOR_EXECS.DOC; PS-SP-#529606-v3-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_28_NOV_2011.doc

Good afternoon,

please find attached the CCIRC Weekly Summary of significant cyber events and incidents reported to and observed by CCIRC, with analysis where required. Please note this product is *not* intended for wide circulation due to the nature of some of the information in the Summary. Here are the highlights:

HIGHLIGHTS:

· Threat Warnings: Nothing significant to report.

· CCIRC Products Released: Technical Report TR11-002: Mitigation Measures for Advanced Persistent Threats published on Public Safety Canada's website

· Incidents to report:

· Canadian federal official and university related credentials compromised in the UN Development Program website hack

· Three provincial governments' computers potentially infected

· Threat actors impersonating reputable Canadian financial institutions and a telecommunications company, enticing internet users to malicious websites (phishing)

· A compromised Canadian website redirecting visitors to a malicious website in Russia

· Distribution of malicious software that steals passwords traced to a Canadian source

· International: Foreign government officials' e-mail accounts and passwords compromised

· Noteworthy Open Source Reports:

· Foreign hackers targeted Canadian institutions during Potash bid last year

- Spoof Health Canada E-mail offers shovelling credit
- Carrier IQ snoops on US cell users
- Cybersecurity bill approved by U.S. House Panel

This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca <mailto:bud.cameron@ps-sp.gc.ca> .

Danielle St-Louis
Administrative Assistant | Adjointe administrative Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada
257 rue Slater St | Ottawa ON K1A 0P9
Telephone | Téléphone: 613-991-7738 Fax | Téléc.: 613-996-0995 E-mail | Courriel: danielle.st-louis@ps-sp.gc.ca
<blocked::mailto:danielle.st-louis@ps-sp.gc.ca>

Klassen, Nathan

From: Bendelier, Kenneth
Sent: December-08-11 7:57 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description: **Cross-site scripting flaws plague Web apps, report says.** "Cross-site scripting flaws are the most prevalent vulnerabilities found in Web applications, posing a risk to data and intellectual property, according to a study of thousands of applications by vendor Veracode released December 7. Veracode analyzed more than 9,900 applications that were submitted to its cloud-based scanning service over the last 18 months. For Web applications, 68 percent contained cross-site scripting flaws, Veracode found in its study. Cross-site scripting is an attack in which a script drawn from another Web site is allowed to run even though it should not, and it can be used to steal information or potentially cause other malicious code to run. Veracode also found that 32 percent of Web applications contained a SQL injection problem, a type of issue where commands entered into Web-based forms are executed, potentially returning sensitive data. Other prevalent flaws Veracode found were CRLF (Carriage Return Line Feed) injection issues, which can allow an attacker to control a Web application or steal information, the report said."
Reference:
http://www.computerworld.com/s/article/9222474/Cross_site_scripting_flaws_plague_web_apps_report_says?taxonomyId=17

2. Item Description**: Anonymous hacks Monsanto PR firm Bivings Group.** "Tango down: Operation End Monsanto claims first victim. The Bivings Group, a public relations firm associated with Monsanto, has been permanently shut down after a devastating attack by those claiming to represent the nebulous and notorious international Internet hacktivist collective known as Anonymous. According to the Anonymous hacktivists, The Bivings Group website was defaced, their database was hacked and dumped, hundreds of emails were stolen and are now viewable, and a database of Monsanto documents were acquired."
Reference: http://www.examiner.com/anonymous-in-national/anonymous-hacks-monsanto-pr-firm-bivings-group
http://pastebin.com/UZTcLMGT

3. Item Description **Inside the latest issue of (IN)SECURE Magazine.**
Reference http://www.net-security.org/dl/insecure/INSECURE-Mag-32.pdf

4. Item Description: **Spam run frightens with fake news about epidemic.** "The time has come again for users to be targeted with spam emails alerting them to an epidemic raging in some part of the world. The subject line contains a simple "Fwd/Re: Epidemic in X" - X being variety of countries around the world including Afghanistan, Australia, Syria, Taiwan, Venezuela or some of the United States of America - and the email says that in order to avoid getting infected the recipient should take the precautions supposedly hosted on a page to which a link is offered. Of course, the page is far from helpful and, according to Symantec, actually hosts a malicious script file that can exploit certain vulnerabilities in the target's system if downloaded and run."
Reference: http://www.net-security.org/secworld.php?id=12074

5. Item Description: **Information: Threat Trends in 2011 - The Signals and the Noise**.
Reference http://regmedia.co.uk/2011/11/29/jwalter_mcafee_labs_threatbrief112011_v3.pdf

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Klassen, Nathan

From: Bendelier, Kenneth
Sent: December-07-11 11:15 AM
To: [redacted]
Subject: Recent Events Claimed by LulzSec/Anonymous

1. Portuguese Under Massive Cyber Attack From Lulzsec
   http://www.voiceofgreyhat.com/2011/12/portuguese-under-massive-cyber-attack.html

2. International hackers Anonymous shut down Colombian Army website
   http://colombiareports.com/colombia-news/news/20878-anonymous-hacks-colombian-army-website-video.html

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-08-11 7:00 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous hacks Monsanto PR firm Bivings Group

Generated by your Alert Subscription on Folder:
- Anonymous
Source: EXAMINER
Complete item: http://www.examiner.com/anonymous-in-national/anonymous-hacks-monsanto-pr-firm-bivings-group

Description:
The Bivings Group, a public relations firm associated with Monsanto, has been permanently shut down after a devastating attack by those claiming to represent the nebulous and notorious international Internet hacktivist collective known as Anonymous.

According to the Anonymous hacktivists, The Bivings Group website was defaced, their database was hacked and dumped, hundreds of emails were stolen and are now viewable, and a database of Monsanto documents were acquired.

On Monday, Anonymous hacktivists released a statement via Pastebin announcing the successful attack. The following is an excerpt from that release:

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-07-11 3:18 PM
To: Bendelier, Kenneth
Subject: Important: OpRobinHood And His NOT So Merry (Anonymous) Men..

Generated by your Alert Subscription on Folder:
- Anonymous
Source: itproportal.com
Complete item: http://www.itproportal.com/2011/12/07/oprobinhood-and-his-not-so-merry-anonymous-men/

Description:
The hacking groups TeaMp0isoN and Anonymous have been busy over the last week, with their latest Operation "OpRobinHood" - "Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks. Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people there money back."

The first National bank of Long Island was attacked last week, and then over the weekend, the BCD credit union in the UK was also targeted- http://legionnet.wordpress.com/2011/12/03/842/. Anonymous's attack vector of choice is not really that sophisticated, it is just SQL injection, still if banks are not going to sanitize dangerous characters (like " ' ") and validate user input then Anonymous will have easy pickings.

E-Secure-IT
https://www.e-secure-it.com

St-Louis, Danielle

From: Bendelier, Kenneth
Sent: December-07-11 11:15 AM
To: [redacted]
Subject: Recent Events Claimed by LulzSec/Anonymous

1. Portuguese Under Massive Cyber Attack From Lulzsec
   http://www.voiceofgreyhat.com/2011/12/portuguese-under-massive-cyber-attack.html

2. International hackers Anonymous shut down Colombian Army website
   http://colombiareports.com/colombia-news/news/20878-anonymous-hacks-colombian-army-website-video.html

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-07-11 9:33 AM
To: Bendelier, Kenneth
Subject: Important: International hackers Anonymous shut down Colombian Army website

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Colombia Reports
Complete item: http://colombiareports.com/colombia-news/news/20878-anonymous-hacks-colombian-army-website-video.html

Description:
Hacker group Anonymous attacked the Colombian Army's website Monday morning, forcing the site to go offline.

According to the Anonymous Twitter page, the DDoS attack - a term referring to an operation which shuts down a website - had a planned launch time of 8:30AM.

There were no official reports about the attack or the culprits - but using Twitter, Anonymous claimed responsibility and explained their motive - to avenge animal cruelty by the Colombian Army, following a broadcast on Colombian television news depicting soldiers shooting a seemingly harmless dog in cold blood with a high-powered rifle.

Anonymous tweeted late night Sunday, "Anonymous Colombia launches an emergency operation tomorrow in defense of animals... They will punish those soldiers."

E-Secure-IT
https://www.e-secure-it.com

Dincoy, Rana

From: Cameron, Bud
Sent: December-07-11 9:18 AM
To: Bendelier, Kenneth; Dincoy, Rana; Pitcher Robert
Subject: FW: Some free training resources

Some good sources for future products.

From: Robert Rodriguez [mailto:resources@infosecinstitute.com]
Sent: December-06-11 3:08 PM
To: Cameron, Bud
Subject: Some free training resources

Here are some of the highlights from InfoSec Resources Fall 2011. Now that it is the last month of the year, we have launched our ever popular free Kindle promotion, register for (almost) any class and get a Kindle included.

You'll notice we've had a lot more focus on mobile and social media security as a result of your requests. Please keep them coming. Be sure to bookmark us, because our new Editor-in-Chief, Robert Rodriguez, has some great new features coming soon.

The 10+1 most frequently read articles in October and November:

1. Attacking IPv6 Enabled Routers with a Reflection Tunnel
2. Hacking Web Services - SOAP Injection
3. Auditing Public API Security with FXCop
4. A History of Anonymous
5. Facebook Connect and OAuth Vulnerabilties
6. Hacking Electronic Voting Machines
7. Reverse Engineering Android Malware - DroidDream
8. Poisoning Web Servers with the HTTP Response Splitting Attack
9. Egghunter Shellcode Exploitation Tutorial
10. Blind SQL Injection Tutorial-
11. 2012 CISSP Exam Changes - Find out everything you'll need to know for the new version of the CISSP exam that begins in January 2012. InfoSec Institute courses are here: http://www.infosecinstitute.com/courses/CISSP

These popular articles and videos are just a few of our recently posted articles. There is much more to read, watch, and learn at http://resources.infosecinstitute.com. If you'd like to write for Resources.InfoSecInstitute.com and be featured in industry publications (and here) please contact Robert at rob.rodriguez@infosecinstitute.com with an article or video topic idea.

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-07-11 5:54 AM
To: Bendelier, Kenneth
Subject: Important: NCCIC DHS Bulletin (Sep 1): "#Anonymous Upcoming US Operations, Impact and Likelihood"

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: public intelligence
Complete item: http://publicintelligence.net/nccic-anonops/

Description:
Public Intelligence [http://twitter.com/PublicIntel] has released an alleged unclassified / for official use only National Cybersecurity and Communications Integration Center (NCCIC) Bulletin dated September 1st assessing four areas of interest to the DHS:

1) Occupy Wall Street
2) Operation Facebook
3) Project Mayhem
4) Operation Halliburton

Alleged tool development (#RefRef) and exploitation vectors ("Apache Killer") are explored in a section on "Tactics, Techniques, and Procedures".

Public Intelligence The loosely organized hacking collective known as Anonymous has announced through several mediums that they plan on conducting cyber attacks, peaceful protests, and other unspecified activity targeting a variety of organizations. The purpose of this product is to judge the likelihood of occurrence for these events, as well as the potential impact.

E-Secure-IT
https://www.e-secure-it.com

Williston, Sandra

From: Beaudoin, Luc S
Sent: December-06-11 3:43 PM
To: Anderson, Windy
Cc: St-Louis, Danielle
Subject: As requested. For Adam's questions
Attachments: FW: ERWG Introductory letter; Government of Canada Cyber Security Incident Reporting Trigger Criteria.xls; FW: For your reading pleasure; vulnerability assessment.xls; cvss-blank-scoring-1.0-sr.xls

1. ERWG, under CSTAC. Update and situation attached.
2. RCMP SIR: We do not have access and do not think we need to or should. The SIR is mostly physical events related. We trust RCMP will share with us events of interest that are Cyber and require our attention.
3. CIRA: we have a working relationship with CIRA. They are our DNS experts and we like to solicit their opinion on issues such as DNSsec and BIND vulnerabilities. We have no MOUs with them at this time but Bud's team had started working on that front. We have had a number of meetings with CIRA in the past 20 months. They are a key strategic asset for CCIRC.
4. Spam Centre: Meetings with CRTC and IC have taken place over the last 12 months. Specifically, CCIRC is hosting a recurrent Ops-meeting with them and IC, RCMP TCB, Antifraud centre, and CTEC. One took place in Sept, and one in Nov. The Spam Centre contract is on MERX and the law is not expected to come into force before next summer. Our next meeting with CRTC will be in Jan.
5. Escalation to the GOC: Any incidents having a significant impact on Canadian CI sector may be reported to the GOC provided it is ***not*** associated with an on-going investigation and/or caveated not for distribution. Sensitive matters will be escalated using existing executive reporting. CCIRC provides routine reporting to the GOC on a daily basis.
6. Escalation: How is risk assessment performed at CCIRC ? Every morning at 0830h, we review and assess cyber issues. This process draws from expertise from CCIRC team members. Risk Asessment in Cyber Space is an unsolved problem, so we rely on expertise and experience to judge criticality. Some guidelines include: (from some of our SOPs)

1) For Vulnerabilities: use CVSS methodology as a starting point (tools attached) . CVSS of 9+ minimum can be candidates, as per NIST NVD; zero-days on any of the following products common versions can be candidate: CISCO, MS Office, Windows, BlackBerry, Linux, Mac, ie, firefox, Apache, Oracle, MySQL, JavaVM, other significantly used plateforms in ISPs, government and large corporations - critical infrastructure owners, and general users (due to second order impact of having a very large number of devices affected).
2) For Threats: many reports of use in the wild with tool-integration (like metasploit), or affecting largely popular canadian websites (ex: cbc.ca), or theme (ex: G20)
3) For News, threats and vulnerabilities: High media attention (ex: government website being hacked), potential for significant impact on security (ex: Anonymous targeting, SCADA, etc), main stream media pick up (GhostNet, Mariposa, TBS), etc.
4) For incidents: actual and significant impact on one or many Canadian CI.

7) TOR for U5: the latest version was produced by Andrew. Attached. I have hand written comments not included. A rapid review took place in London but it was decided if I recall to look into this further at future opportunities (next U5).

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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-06-11 2:58 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous: Operation Horizon - Dec. 17th (video)

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: YouTube
Complete item: http://www.youtube.com/watch?v=SoKIBW4keeQ

Description:
Anonymous: Operation Horizon - Dec. 17th (video)

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-06-11 1:27 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Took Responsibility Of Hacking Into 50+ Toronto Websites (#OccupyToronto)

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Various Sources
Complete item: http://www.voiceofgreyhat.com/2011/12/anonymous-took-responsibility-of.html

Description:
Anonymous took responsibility of hacking into 50+ Toronto websites. In a YouTube video anon said "We have been receiving plenty of complaints that Toronto business based websites have been hacked. People quickly assumed that OccupyTO was behind this, but luckily Anonymous stepped up to the plate for taking responsibilities for their actions. At this moment we do not know why the websites were redirect to OccupyTOs website (www.occupyto.org).

Although, this seemed to be a response to the first video that threatened to remove Toronto from the internet. All we can say at this point is that Anonymous, is stating a point that this occurred because of the cities actions to evict the protesters. A video is claiming that Anonymous attacked 50+ Toronto business based website, took down Canadian Craigslist website, and gained access to a valuable email account. We hope everything comes down to a peaceful agreement."

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-06-11 12:09 AM
To: Bendelier, Kenneth
Subject: Information: DHS Bulletin: Anonymous Upcoming U.S. Operations Overview

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: public intelligence
Complete item: http://publicintelligence.net/nccic-anonops/

Description:
This DHS National Cybersecurity and Communications Integration Center (NCCIC) bulletin was released by Anonymous as a teaser ahead of an upcoming leak. The date of the bulletin is believed to be September 1, 2011 due to the documents metadata and references made in other NCCIC bulletins. For other NCCIC bulletins regarding Anonymous and LulzSec, please see our collection.

The loosely organized hacking collective known as Anonymous has announced through several mediums that they plan on conducting cyber attacks, peaceful protests, and other unspecified activity targeting a variety of organizations. The purpose of this product is to judge the likelihood of occurrence for these events, as well as the potential impact.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-05-11 1:05 PM
To: Bendelier, Kenneth
Subject: Information: 2011 The Year of the Hacktivist: When Anonymous Finally Grew-Up

Generated by your Alert Subscription on Folder:
- Anonymous
Source: ibtimes
Complete item: http://uk.ibtimes.com/articles/261403/20111205/2011-year-hacktivist-anonymous-finally-grew.htm

Description:
Read through the International Business Times hind-sight look at hacktivism in the year 2011, as it runs through the key points that changed Anonymous from a "hacktivist" collective into a global political movement. In a year plagued by cyber-crime, the name Anonymous has been at the forefront of nearly every debate, with what was originally taken as little more than a small group of tantruming teenagers, growing into, debatably, one of the most powerful political movements in the world.

Hacktivist Origins

Though the exact details of Anonymous' origin remain as mysterious as its moniker, the collective is believed to be an off-shoot of the older 4Chan online community. Unlike its brother group, LulzSec, which operated on a more anarchistic ideology, targeting random organisations and companies "just for lulz" -- internet jargon for laughs -- Anonymous portrayed itself as a hacktivist collective, picking its targets for perceived crimes against the world.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-05-11 1:00 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous Wages Cyber War in South America

Generated by your Alert Subscription on Folder:
- Cyberwar / Cyber conflict / Cyber war
- Anonymous
Source: ibtimes
Complete item: http://uk.ibtimes.com/articles/261418/20111205/anonymous-wages-cyber-war-south-america.htm

Description:
While this year will be remembered as the year of the hacktivist, it was in South America that cyber activists sprang up to protest against human rights violations, corruption and restrictions on internet freedoms.Although the international internet collective Anonymous achieved renown for its attacks on Scientology, the application of legal procedures and big banks, its operations were more overtly political in Latin America, where it raised public awareness of crucial issues, such as the manipulation of information, the murders of bloggers and journalists by drug cartels and freedom of expression.

Cyber crime has been prevalent in Latin America since the birth of the World Wide Web. But the proliferation of computers and online access in the region, which has grown more than 1,000 percent over the past decade, according to the Miami Herald, has led to a surge in South American cyber activism.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-04-11 3:24 PM
To: Bendelier, Kenneth
Subject: Important: A Message From Anonymous: #OpHorizon

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps - GeneralActions
Source: Various Sources
Complete item: http://inewp.com/?p=9953

Description:
Greetings from Anonymous,
On December 17th, we invite every Occupy protester, Anon, and Citizen to march in a day of solidarity and remembrance.

December 17 will mark the anniversary of many historic events: three months since the beginning of the Occupy movement; the one-year anniversary of the death of Mohamed Bouazizi, the Tunisian man whose self-immolation initiated the first of protests which became the Tunisian Revolution, and eventually cascaded into the Arab Spring; and 24 years since the birth of Bradley Manning, the army private accused of leaking classified information to Wikileaks.

Mannings first hearing is scheduled for Dec 16, 586 days after his arrest, where he will face a military panel who decide if will go to trial.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-04-11 7:06 AM
To: Bendelier, Kenneth
Subject: Critical: LulzSec: Anonymous hacktivists strike Portugal after police brutality

Importance: High

Generated by your Alert Subscription on Folder:
- Major Site Security Breaches - Hack / DDos Attacks
- Anonymous
Source: EXAMINER
Complete item: http://www.examiner.com/anonymous-in-national/lulzsec-anonymous-hacktivists-strike-portugal-after-police-brutality

Description:
Anonymous hacktivists in Portugal are on a rampage, driven by austerity measures, social inequalities and recent police violence against demonstrators during a protest on November 24.

On Friday, LulzSec Portugal launched a successful DDoS (distributed denial of service) attack against the website of Banco de Portugal (Bank of Portugal), making the site inaccessible.

In addition to taking down the Bank of Portugal website, LulzSec Portugal has been credited with successful attacks on numerous state services. Earlier this week LulzSec disabled the websites of the Portugal House of Parliament, several political parties and the national police.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-04-11 6:55 AM
To: Bendelier, Kenneth
Subject: Information: Raids target computers suspected in 'Anonymous' cyber-attack

Generated by your Alert Subscription on Folder:
- Anonymous
Source: STL Today
Complete item: http://www.stltoday.com/news/local/crime-and-courts/raids-target-computers-suspected-in-anonymous-cyber-attack/article_933b13fa-9d03-580f-9f62-d607332ed95c.html

Description:
The sound of keys in his lock and the jangling of the security chain on his door awakened Chris Sudlik.

It was 6 a.m. July 19, and the University of Missouri-St. Louis student had fallen asleep just a few minutes before.

At his door were FBI agents and police who suspected him of being a member of the "Anonymous" hacker group thought to have brought down a business website with a flood of attacks.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-04-11 6:52 AM
To: Bendelier, Kenneth
Subject: Critical: Anonymous warns Mexico over OpRoadSafe

Importance: High

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: TGDaily
Complete item: http://www.tgdaily.com/security-features/59982-anonymous-warns-mexico-over-oproadsafe

Description:
Cyber activists associated with Anonymous have published a list of demands aimed at the Mexican government and local bus companies.

The group said it would halt a mass cyber attack planned for December 10 under the banner of Op Carreteras Seguras (OpRoadSafe) if their demands were met.

Anonymous launched its latest digital campaign in an effort to publicize the fact that the Mexican government and bus companies are failing to stop kidnappings, rapes and robberies of passengers on the countrys lawless highways.

Indeed, a mass grave containing 293 bodies was recently discovered in San Fernando, Tamauilpas just 90 miles south of the Rio Grande Valley.  Authorities believe the victims were bus passengers abducted and murdered by members of the Zetas drug cartel.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-04-11 6:45 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Takes From The Rich, Gives To... The Cyber Security Industry?

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Forbes
Complete item: http://www.forbes.com/sites/parmyolson/2011/12/02/anonymous-takes-from-the-rich-gives-to-cyber-security-market/

Description:
Cyber activists supporting Anonymous have passionately sought to punish the corruption they see in authority from digital security firms to big corporations to, now, banks themselves. A hacker splinter group called TeaMp0isoN says it has partnered with supporters of the extremely loose-knit network of hacktivists and pranksters, to steal credit cards from several banks including Chase, Bank of America and CitiBank and give the money to charities and the 99%. The project, announced yesterday, is called Operation Robin Hood and in response to the Occupy Movement.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-03-11 5:13 PM
To: Bendelier, Kenneth
Subject: Information: Anonymous news blogs - antisec teampoison teamp0ison oprobinhood ophorizon opblackout

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Wordpress
Complete item: http://gnudarwin.wordpress.com/2011/12/02/anonymous-news-blogs-antisec-teampoison-teamp0ison-oprobinhood-ophorizon-opblackout/

Description:
I am looking for high quality Anonymous News blogs. If you know of any good ones, please feel free to post them in the comments section. There is a high possibility that I will publish good links on all the GNU-Darwin spectrum blogs and social network sites. In due course, links may appear on the GNU-Darwin site itself. Reader accessible RSS feeds and current news would be a minimal requirement. Here are a few that I know about already. I try to consult these blogs on a daily basis. Like many people, I am eager for more such news, and a good list would likely be widely appreciated. Please submit in the following format, if possible. Also, feel free to submit more than one. Self-promotion is discouraged I understand.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-03-11 4:58 PM
To: Bendelier, Kenneth
Subject: Information: I love Anonymous, the great equalizers who are on the side of the oppressed - The Shutter of Mouths - OpRobinHood

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Blogspot
Complete item: http://accesstoinfo.blogspot.com/2011/12/system_02.html?spref=tw

Description:
I am a populist, with libertarian and leveller flourishes all my own. I hold no truck with wealth or power, or with authority in general. My target is elitist hierarchy, and I don't care the source. It is irrelevant to me whether establishment insiders and front men happen to work in Ottawa or Beijing, on Wall Street or Hollywood Boulevard, in a law office or the Oval Office. I will do my bit here to expose the venality and ineptitude of the self-satisfied classes in society, as well as to discredit those institutions which they have worked so diligently to force on the rest of us. To that end, I resolve to publish anything on this blog I can get away with, including (unless we agree otherwise) any emails you send me.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-03-11 8:00 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous and TeaMp0isoN Target Banks to Help Those "Cheated" by the System

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Security Week
Complete item: https://www.securityweek.com/anonymous-and-teamp0ison-target-banks-help-those-cheated-system

Description:
p0isAnon, a name representing the merger between Anonymous and TeaMp0isoN, has launched a campaign which includes the possibility of wearing green tights, caps with matching feathers, and a guaranteed felony charge for those involved, should they be caught.

The campaign, aptly named OpRobinHood, aims to take from the rich and then force the rich to eat the charges as the poor benefit from compromised credit accounts.

Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people their money back, a statement from p0isAnon explains.

We have already taken Chase, Bank of America, and Citibank credit cards with big breaches across the map. We have returned it to the poor (the TRUE 99%) who deserve it.... We have donated thousands to many protests around the world.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-03-11 4:35 AM
To: Bendelier, Kenneth
Subject: Important: Raids target computers suspected in 'Anonymous' cyber-attack

Generated by your Alert Subscription on Folder:
- Anonymous
Source: STL Today
Complete item: http://www.stltoday.com/news/local/crime-and-courts/raids-target-computers-suspected-in-anonymous-cyber-attack/article_933b13fa-9d03-580f-9f62-d607332ed95c.html

Description:
The sound of keys in his lock and the jangling of the security chain on his door awakened Chris Sudlik.

It was 6 a.m. July 19, and the University of Missouri-St. Louis student had fallen asleep just a few minutes before.

At his door were FBI agents and police who suspected him of being a member of the "Anonymous" hacker group thought to have brought down a business website with a flood of attacks.

"It was pretty terrifying," Sudlik told a reporter in a recent interview. While "they didn't quite kick down the door," he said, he was forced to the floor after he let the officers into his ground-floor apartment on Marietta Drive, just east of the university.
The officials forced his fiance to wait outside as he was questioned, and agents grabbed and carted away computers, CDs and other equipment.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-02-11 1:00 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous Takes From The Rich, Gives To Cyber Security Market

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Forbes
Complete item: http://www.forbes.com/sites/parmyolson/2011/12/02/anonymous-takes-from-the-rich-gives-to-cyber-security-market/?

Description:
Cyber activists supporting Anonymous have passionately sought to punish the corruption they see in authority from digital security firms to big corporations to, now, banks themselves. A hacker splinter group called TeaMp0isoN says it has partnered with supporters of the extremely loose-knit network of hacktivists and pranksters, to steal credit cards from several banks including Chase, Bank of America and CitiBank and give the money to charities and the 99%. The project, announced yesterday, is called Operation Robin Hood and in response to the Occupy Movement.

Also announced yesterday: the cyber security market is (surprise) booming. This is the industry making money from companies and governments who want to defend and attack digital threats like Operation Robin Hood.

E-Secure-IT
https://www.e-secure-it.com

Cameron, Bud

From: Cameron, Bud
Sent: December-02-11 12:13 PM
To: Anderson, Windy
Subject: RE: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication

Ken is our open-source watchdog. Just because he sends stuff to cyberdo for SA, or for possible investigation, does not mean he wants it escalated, in fact normally that is NOT the case. He would send it to Luc or me or you if he thought it was something big that needed higher up attention.
(Ken is speaking with Cyberdo about not sending these things on to everybody...) As far as a process, Luc will say that he owns the escalation process, and I agree up to a point (certainly for cyber incidents impacting Canadian CI) but there are many cases where cyber event information or concerns over cyber events arrives from other sources, top-down or sideways in the GC, and there is a role for CCIRC management outside of ops to assess the strategic impact and to manage any Executive Overreaction!

If an email like the one Frank prepared this morning feeds the beast, then let's stick with that. Luc will only produce things that are technically complete and accurate and will not give a timely response sometimes for this reason. And as Luc says we shouldn't stop the ops train while we answer questions!

-----Original Message-----
From: Bendelier, Kenneth
Sent: December-02-11 11:53 AM
To: Anderson, Windy
Subject: RE: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication

Nope, this is tactical.

Within reason, yep.

-----Original Message-----
From: Anderson, Windy
Sent: December-02-11 11:44 AM
To: Bendelier, Kenneth
Subject: Fw: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication
Importance: High

Can I ask you to let me know which of these items I need to get to Robert until we figure out the right way to do it.

And if important, send me the note to send to Robert?

Windy

----- Original Message -----
From: CYBERDO
Sent: Friday, December 02, 2011 11:34 AM
To: [redacted]
Subject: FW: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication

FYI

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: Bendelier, Kenneth
Sent: December-02-11 11:33 AM
To: CYBERDO; Turbide, Frank; Beaudoin, Luc S
Subject: FW: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication
Importance: High

FYI

-----Original Message-----
From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: December-02-11 11:23 AM
To: Bendelier, Kenneth
Subject: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication
Importance: High

Generated by your Alert Subscription on Folder:
- Scam / Fraud / Hoax Alerts
- - Global Business ICT Risks
Source: Bank Information Security
Complete item: http://ffiec.bankinfosecurity.com/articles.php?art_id=4295&pg=1

Description:
The Federal Bureau of Investigation has issued a warning about a new Zeus malware attack targeting commercial bank accounts, ultimately leading to incidents of corporate account takeover. The Zeus variant used: a malware called Gameover, which the FBI says is able to defeat several forms of dual-factor authentication.

To protect themselves, the FBI suggests consumers and businesses pay attention to suspicious e-mails. In the case of the Gameover attacks, e-mails purporting to come from NACHA-The Electronic Payments Association contained malicious links. NACHA does not traditionally send e-mails directly to businesses or consumers. Receipt of a direct e-mail from an organization such as NACHA should raise a red flag.

But according to the FBI's Denver Cyber Squad, it's not just phishy e-emails and dual-factor get-arounds that have made the Gameover attacks forces to be reckoned with. As it turns out, the fraudsters behind this scheme combined a number of tactics, including the use of money mules and denial of service attacks, to con businesses and banks out of funds.

"After the accounts are compromised, the perpetrators conduct a distributed denial of service (DDos) attack on the financial institution," the FBI states. "The belief is the DDoS is used to deflect attention from the wire transfers, as well to make them unable to reverse the transactions."

Over the past two weeks, since the Gameover scheme was discovered, the FBI has tracked fraudulent wire transfers routed to high-end jewelry stores. And here is where the scheme takes its twist. Money mules, which've been hired to visit these stores, where funds have been fraudulently transferred, go to pick up jewels worth the amount of the fake wire.

"A money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as pending and releases the merchandise to the mule," the FBI states. "Later on, the transaction is reversed or cancelled ... and the jeweler is out whatever jewels the money mule was able to obtain."

Connecting the Dots
Fraudsters' ingenuity in the Gameover scheme is concerning.

"We've gotten fairly good at the Red Flag rules and detecting money mules, so the attackers are now figuring out they need to stall for time to get the cash," says Mike Smith, an online security expert with Akamai Technologies.

To do that, fraudsters are launching DDoS attacks against the banking institutions, just to distract them long enough to get the money and run.

"These attacks kill the interface that the customers are used to seeing, as well as the interface the banks use, like the APIs they use to do their transfers between each other," Smith says.

Cybercriminals have figured out how to connect the dots. They are committing cross-channel fraud.

The scam relies on traditional phishing and spear-phishing tactics to get in the door. Spear-phishing e-mails are sent to executives, who oftentimes are identified via social networking channels like LinkedIn and corporate databases. Additionally, the fraudsters send massive phishing e-mails to every employee in an organization, just waiting for one with access to the corporate online banking account to click a link.

Once the malware is launched, the fraudsters can monitor keystrokes and the online bank sites those infected PCs visit.

But it's the DDoS and money mule additions that bring the fraud full circle.

"You usually see one of three things in a DDoS attack," Smith says:

A protection racket scam, which involves an attack against an ecommerce site that blackmails the site into paying a few to stop the attack;

An activist threat, like the ones the industry has seen waged by groups such as Anonymous against entities for social reasons;

A political threat, which could be waged against a corporation or country by a nation state.

"This is an entirely different scenario," Smith says. "What you're seeing is that the attack is designed to slow down the businesses being defrauded and slow down the bank's response."

Dave Jevans of the Anti-Phishing Working Group says financial institutions have two theories about the reasoning behind the attacks: to shut down access and distract bank security and IT. For large institutions, the attacks likely only serve as distractions.

E-Secure-IT
https://www.e-secure-it.com

s.16(2)(c)

Klassen, Nathan

From:
Sent: December-02-11 11:35 AM
To:
Subject: FW: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication

Importance: High

FYI

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: Bendelier, Kenneth
Sent: December-02-11 11:33 AM
To: Turbide, Frank; Beaudoin, Luc S
Subject: FW: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication
Importance: High

FYI

-----Original Message-----
From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: December-02-11 11:23 AM
To: Bendelier, Kenneth
Subject: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication
Importance: High

Generated by your Alert Subscription on Folder:
- Scam / Fraud / Hoax Alerts
- - Global Business ICT Risks
Source: Bank Information Security
Complete item: http://ffiec.bankinfosecurity.com/articles.php?art_id=4295&pg=1

Description:
The Federal Bureau of Investigation has issued a warning about a new Zeus malware attack targeting commercial bank accounts, ultimately leading to incidents of corporate account takeover. The Zeus variant used: a malware called Gameover, which the FBI says is able to defeat several forms of dual-factor authentication.

To protect themselves, the FBI suggests consumers and businesses pay attention to suspicious e-mails. In the case of the Gameover attacks, e-mails purporting to come from NACHA-The Electronic Payments Association contained malicious links. NACHA does not traditionally send e-mails directly to businesses or consumers. Receipt of a direct e-mail from an organization such as NACHA should raise a red flag.

But according to the FBI's Denver Cyber Squad, it's not just phishy e-emails and dual-factor get-arounds that have made the Gameover attacks forces to be reckoned with. As it turns out, the fraudsters behind this scheme combined a number of tactics, including the use of money mules and denial of service attacks, to con businesses and banks out of funds.

"After the accounts are compromised, the perpetrators conduct a distributed denial of service (DDos) attack on the financial institution," the FBI states. "The belief is the DDoS is used to deflect attention from the wire transfers, as well to make them unable to reverse the transactions."

Over the past two weeks, since the Gameover scheme was discovered, the FBI has tracked fraudulent wire transfers routed to high-end jewelry stores. And here is where the scheme takes its twist. Money mules, which've been hired to visit these stores, where funds have been fraudulently transferred, go to pick up jewels worth the amount of the fake wire.

"A money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as pending and releases the merchandise to the mule," the FBI states. "Later on, the transaction is reversed or cancelled ... and the jeweler is out whatever jewels the money mule was able to obtain."

Connecting the Dots
Fraudsters' ingenuity in the Gameover scheme is concerning.

"We've gotten fairly good at the Red Flag rules and detecting money mules, so the attackers are now figuring out they need to stall for time to get the cash," says Mike Smith, an online security expert with Akamai Technologies.

To do that, fraudsters are launching DDoS attacks against the banking institutions, just to distract them long enough to get the money and run.

"These attacks kill the interface that the customers are used to seeing, as well as the interface the banks use, like the APIs they use to do their transfers between each other," Smith says.

Cybercriminals have figured out how to connect the dots. They are committing cross-channel fraud.

The scam relies on traditional phishing and spear-phishing tactics to get in the door. Spear-phishing e-mails are sent to executives, who oftentimes are identified via social networking channels like LinkedIn and corporate databases. Additionally, the fraudsters send massive phishing e-mails to every employee in an organization, just waiting for one with access to the corporate online banking account to click a link.

Once the malware is launched, the fraudsters can monitor keystrokes and the online bank sites those infected PCs visit.

But it's the DDoS and money mule additions that bring the fraud full circle.

"You usually see one of three things in a DDoS attack," Smith says:

A protection racket scam, which involves an attack against an ecommerce site that blackmails the site into paying a few to stop the attack;

An activist threat, like the ones the industry has seen waged by groups such as Anonymous against entities for social reasons;

A political threat, which could be waged against a corporation or country by a nation state.

"This is an entirely different scenario," Smith says. "What you're seeing is that the attack is designed to slow down the businesses being defrauded and slow down the bank's response."

Dave Jevans of the Anti-Phishing Working Group says financial institutions have two theories about the reasoning behind the attacks: to shut down access and distract bank security and IT. For large institutions, the attacks likely only serve as distractions.

E-Secure-IT
https://www.e-secure-it.com

Klassen, Nathan

From: Cameron, Bud
Sent: December-01-11 8:12 AM
To: Bendelier, Kenneth; [redacted]
Subject: RE: Noteworthy and Not Worthy

Further to #6, a dissenting view:

*** 'Jailbreak' of PlayBook no emergency**
An opinion piece states, "A group of U.S.-based computer hackers claim to have found a vulnerability within Research In Motion Ltd.'s BlackBerry PlayBook that allows the tablet computer to be "jail-broken," giving users the ability to access and alter core features of the device. The announcement set off alarm bells in the technology world, prompting some observers to fret that the jailbreak had dealt a damaging blow to RIM's reputation for iron clad mobile security…" National Post, FP14

From: Bendelier, Kenneth
Sent: December-01-11 8:06 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description **Google researchers propose fix for ailing SSL system.** "Security researchers from Google proposed an overhaul to improve the security of the Secure Sockets Layer encryption protocol that millions of Web sites use to protect communications against eavesdropping and counterfeiting. The changes are designed to fix a structural flaw that allows any one of the more than 600 bodies authorized to issue valid digital certificates to generate a Web site credential without the permission of the underlying domain name holder. The consequences of fraudulently issued certificates was underscored in late August when hackers pierced the defenses of Netherlands-based DigiNotar and minted bogus certificates for Google and other high-profile Web sites. One of the fraudulent credentials, for Google mail, was used to snoop on as many as 300,000 users, most of them from Iran. Under changes proposed November 29 by Google security researchers, all certificate authorities would be required to publish the cryptographic details of every Web site certificate to a publicly accessible log that has been cryptographically signed to guarantee its accuracy. The overhaul, they said, is designed to make it impossible –- or at least much more difficult –- for certificates to be issued without the knowledge of the domain name holder."
Reference: http://www.theregister.co.uk/2011/11/29/google_proposes_ssl_fix/

2. Item Description: **Anonymous launches new operation targeting big banks.** "Hacktivist collective Anonymous and hacking group Teamp0ison have announced that they will be joining their forces once again and starting another operation against banks. They call it OpRobinHood, and apparently it will consist of stealing credit card details from big banks in order to use it to make donations to charities and others. "In regards to the recent demonstrations and protests across the globe, we are going to turn the tables on the banks," they state. "Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks. Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people there money back." The operation is meant to damage the banks' financial standing as well as their reputation, and as such it should continue the work initiated by the Operation Cash Back, with which bank users were urged to close their accounts and transfer the money to accounts opened with credit unions. "Operation Robin Hood urges YOU, to now move your accounts into secure credit unions, before it's too late while we hit them from the inside," they say, but don't reveal whether the stolen information will be used by them or made public for the "99%" to use. Allegedly, Chase, Bank of America, and CitiBank have already been hit with big breaches, and credit cards issued by them have been used to make donations."
Reference: http://www.net-security.org/secworld.php?id=12024
http://www.itworld.com/security/229141/team-poison-anonymous-campaigners-claim-first-victims-oprobinhood

3. Item Description: **Carrier IQ snoops on US cell users - Spyware or service monitoring tool?.** "Last week a very scary piece of research was published by Trevor Eckhart about spyware that is being included on cellular phones in the United States. The commercial software application is called Carrier IQ and is reportedly being used by Verizon, Sprint and potentially other carriers. Carrier IQ was unhappy with Eckhart publishing public copies of their training materials and proceeded to send a cease and desist letter to Mr. Eckhart. Fortunately Eckhart worked with the EFF to explain things to Carrier IQ and their CEO responded with an apology promising to work with the EFF and Eckhart. Eckhart analyzed the software that was running on his Android-based HTC phone (Carrier IQ also supports Blackberry, Nokia and others) and discovered it was doing some rather sneaky things. It was installed in such a manner as to be largely invisible, it was logging his location even when he had location services disabled and keeping track of every key press and URL he visited (including HTTPS urls). The software ignored the "Force stop" button and was nearly impossible to remove from the device for non-Android hackers."
Reference: http://nakedsecurity.sophos.com/2011/12/01/carrier-iq-snoops-on-us-cell-users-spyware-or-service-monitoring-tool/

4. Item Description: **Cyber security bill promotes sharing of threat data** "The House Intelligence Committee introduced legislation Wednesday designed to knock down the barriers that interfere with the federal government and the private sector sharing critical information about cyber security threats. The bill would enable the intelligence community to share classified information with the private sector while at the same time addressing the concerns private companies have with providing information about attacks on their systems to the government. Communications between the two sides has been problematic and difficult. The government has limited the amount of information it provides private industry about cyber attacks for fear of compromising secrets."
Reference: http://security.blogs.cnn.com/2011/11/30/cyber-security-bill-promotes-sharing-of-threat-data/

5. Item Description: **Obama Invokes Cold-War Security Powers to Unmask Chinese Telecom Spyware**. "The U.S. is invoking Cold War-era national-security powers to force telecommunication companies including AT&T Inc. and Verizon Communications Inc. (VZ) to divulge confidential information about their networks in a hunt for Chinese cyber-spying. In a survey distributed in April, the U.S. Commerce Department asked for a detailed accounting of foreign-made hardware and software on the companies networks. It also asked about security-related incidents such as the discovery of unauthorized electronic hardware or suspicious equipment that can duplicate or redirect data, according to a copy of the survey reviewed by Bloomberg News. The survey represents very high-level concern that China and other countries may be using their growing export sectors to develop built-in spying capabilities in U.S. networks, said a senior U.S. intelligence official who asked not to be named because he wasnt authorized to speak on the matter."
Reference: http://www.bloomberg.com/news/2011-11-30/obama-invokes-cold-war-security-powers-to-unmask-chinese-telecom-spyware.html?utm_source=dlvr.it&utm_medium=twitter

6. Item Description: **Hackers say they broke BlackBerry PlayBook security**. "Three hackers say they have broken the security on the BlackBerry PlayBook tablet, allowing them to run unauthorized applications and control hardware components that users can't normally access. "We've done it. We've broken RIM's fancy security," said a hacker who goes by the alias "neuralic" in a demonstration video posted on Youtube. He said he collaborated on the project with two other hackers, known as Xpvqs and Chris "cmw" Wade. In a statement, Playbook-maker Research in Motion said it was aware of "a claim made on Twitter" by security researchers "that suggests the ability to 'jailbreak' a BlackBerry PlayBook tablet." Jailbreaking a device means altering it to gain access to systems or applications that aren't authorized by the manufacturer. RIM added that it is investigating the claim and has been in contact with one of the security researchers to discuss it."
Reference: http://www.cbc.ca/news/technology/story/2011/11/30/technology-blackberry-playbook-security.html

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-02-11 6:04 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous and ANTISEC: Mixing Metaphors Can Lead to Trouble

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
- AnonOps - GeneralActions
Source: Wordpress
Complete item: http://krypt3ia.wordpress.com/2011/12/01/anonymous-and-antisec-mixing-metaphors-can-lead-to-trouble/

Description:
The Steady March Toward Anonymous Jihad

The picture above showed up on the internet attached to a right wing site. Edited I assume with the text The left has *declared jihad on capitalism* This image and the connotation of it should be of concern to Anonymous at large because of its potential for swaying thought. I can only assume that this image and more like it coming from the OWS movement sites will only proliferate as the right wing candidates vie for the position of President and in the process, make the Anons and the OWS movement seem to be a terrorist movement or groups.

I am sorry to say though, that unless this person photographed was a shill for the right, then someone or more than a few people have got the wrong idea and are wearing the typical shemagh in tandem with the Anon mask and have thus started the ball rolling on this themselves. I for one actually wore the same together back before Anon and the OWS movement began to really pick up steam, and I did so tongue in cheek.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-01-11 11:56 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous and Team Poison Join Forces For OpRobinHood to Target Banks and Give to Charities

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Gizmodo
Complete item: http://gizmodo.com/5863679/anonymous-and-team-poison-join-forces-for-oprobinhood-to-target-banks-and-give-to-charities

Description:
Two hacking groups, Anonymous and Team Poison, have joined forces to take on the banks, steal money and donate it to charities and protests. Reclaiming the "99 per cent's money back".

Apparently the plan is to swipe money from stolen credit card and bank details and donate it to charities and protest movements:

PoisAnon is relying on the fact that the banks will reimburse stolen cash from victim's credit cards, which is probably a safe bet, but would backfire horribly if that doesn't actually happen. Both hacker teams have had success in the past hacking into banks and are confident they can do it again. The thought of internet Robin Hoods running around helping out the poor is a noble proposition, but I can't see this not impacting your average Joe on the street. The money they intend to steal has to come from somewhere and almost everything ends up landing with the customer. [YouTube via The Inquirer via Gizmodo UK]

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-01-11 11:27 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous: Operation Robin Hood (opRobinHood) We Want our Money Back

Generated by your Alert Subscription on Folder:
- Anonymous
Source: You Tube
Complete item: http://www.youtube.com/watch?v=DKNUKP5hal4&feature=youtu.be

Description:
Anonymous and TeaMp0isoN have joined forces to fight censorship in the name of OpCensorThis. There is a new operation that has been taking place over the actions of Banks in response to the Occupy Movement. We have watched our brothers and sisters being refused their hard earned money by the banks on top of being beaten and brutalized by officers during peaceful demonstrations. Congratulations banks, you have gotten our attention.

You ignore your customers and use authorities to censor their voices. Operation Censor This will not stand for such acts and is spawning another operation under Operation Cash Back which already removed well over 500,000 accounts from banks and put them into credit unions. This is the next step. Banks have stolen millions from its customers as well as lacked the security to protect them. We give you Operation Robin Hood.

E-Secure-IT
https://www.e-secure-it.com

Dincoy, Rana

From: Dincoy, Rana
Sent: December-01-11 4:01 PM
To: Cameron, Bud
Cc: Dincoy, Rana
Subject: CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_NOV_21_2011
Attachments: PS-SP-#527055-v1-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_NOV_21_2011.DOC.doc

Tracking:

Recipient	Recall
Cameron, Bud	Failed: 02/12/2011 7:26 AM
Dincoy, Rana	Failed: 01/12/2011 4:08 PM

Hi Bud,

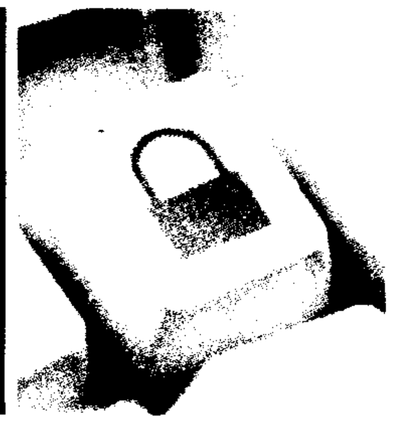
Please find attached the almost final Weekly Summary. I would appreciate it if you could e-mail me the revised/commented document also as an attachment. Please let me know what you think about the watermark – I'm not sure it really works but I think jazzing up the Top Header (CCIRC bigger and bolder) on first page, plus unbolding Unclassified and DRAFT work well.

Rana

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-006



For the Week of

19 Nov – 25 Nov 2011

Issued: 1 Dec 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released/Activities:** CCIRC notified 147 Canadian organizations that were affected by Operation "Ghostclick"and offered mitigation advice.

- **Incidents to report:** (1)User credentials stolen for a newspaper website; (2) An update on the massive on-line fraud and cybercrime reported last week; (3) Financial institution's website vandalized; and (4) Threat actors impersonating a Canadian financial institution, luring internet users to malicious websites (phishing);

- **International:** UK Government releases updated Cyber Security Strategy, which will invest £650m over four years to strengthen the UK's cyber capabilities.

- **Noteworthy Open Source Reports:** (1) UK banks undergo cyber security 'stress test'; and (2) More Facebook scams.

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and other noteworthy open source reports.

NOTABLE INCIDENTS– 19 NOVEMBER THROUGH 25 NOVEMBER 2011:

Canadian Critical Infrastructure:

Multi Sector Event Update. CCIRC notified 147 organizations in multiple sectors that were affected by Operation "Ghostclick", the massive DNS changer fraud exposed by the FBI two weeks ago and reported in the last two CCIRC Weekly Summary reports. Canadian organizations that were notified this week included internet service providers, information technology companies, post-secondary schools, health and media organizations.

- **Analysis:** This was a world-wide fraud where victims are still being notified by CCIRC and its international equivalents around the world. It is estimated that this fraud went on for four years.

Financial Sector.

Threat actors impersonating well known financial entities attempted to steal personal information by persuading internet users to click on links to malicious websites (phishing). CCIRC found one malicious website still in operation and notified the entity being impersonated. CCIRC also notified Google phishing, and the Anti-Phishing Working Group so internet users may be alerted if they encounter these specific malicious websites. The number of victims is unknown.

- **Analysis:** This type of malicious activity is commonly seen by CCIRC and continues to cause financial losses for Canadians. It is known that the malicious website is hosted in Seoul, Korea.

CCIRC also learned that the website of a financial institution was vandalized. CCIRC notified the organization of this website defacement and offered mitigation advice.

- **Analysis:** This type of malicious activity usually does not put a financial institution's operations in jeopardy but could threaten the visitors to that website. Website defacement does, however, indicate the vulnerability of the website to malicious activity by threat actors. A common malicious activity is placement of malicious software on the website that would be passed on to any visitor to that website, and compromise his/her computer, then steal information or use it to send SPAM e-mails anonymously.

Telecommunications Sector – an Update.

Last week CCIRC reported that a Canadian domain name registrar was victim of a cyber-attack, and that its stolen customer contact list was then used by criminals to persuade customers to provide their credit card numbers. These credit card numbers were used in recent purchases. **A federal agency is now leading the investigation.**

- **Analysis:** While CCIRC regularly sees threat actors impersonating trusted entities to persuade internet users to give their personal and financial information, this is the first time in recent memory an internet registration authority in Canada has been successfully targeted. The impact of a trusted entity's compromise can be much greater than an individual or an organization. **This matter is considered of national interest because of the significance of this registrar.**

Public. CCIRC discovered that the user credentials for a Canadian newspaper website's special section were stolen. The loss of these credentials could lead to the compromise of these users' personal information. CCIRC is not aware of the number of victims.

- **Analysis:** The newspaper's special section is aimed at a specific reader group, which is a small subset of this newspaper's regular readership. However, the stolen user credentials were posted on the internet and could allow any threat actor to gain access to these users' personal information such name, address, phone number and workplace. Unfortunately, this type of compromise is being seen on a regular basis in Canada.

CCIRC Products/Activities: Nothing to report

International:

UK releases updated Cyber Security Strategy. The UK government released an update to its Cyber Security Strategy, which was published two years ago. There is an increased emphasis on information sharing between the public and private sector, reaching out to industry sectors hitherto not considered as part of UK's critical infrastructure, and increased military capability in cyber security to gain comparative advantage. Increased efforts to improve the public's cyber security include working with internet service providers to develop a voluntary code of conduct to help their customers when they suspect their computer has been compromised. In addition, a new Cyber Crime Unit within the National Crime Agency will be created.UK Government intends to continue working internationally to help improve cyber security in the UK and the world. The National Cyber Security Programme based on this strategy has been allocated £650m over the next four years.

- **Analysis:** The UK sees cyber security in terms of national security and economics. The UK government publicly stated that their aim was to make UK a safe place to do business online, and gave warning it intended to deter and defend itself against advanced threats by nation-states. The Government of Canada released its own cyber security strategy in 2011, which,

similarly, focuses on protecting government systems, working with the private sector to protect critical infrastructure systems and helping Canadians to be secure online. These initiatives have been allocated $90M over five years. Canada is a strong partner of the UK in helping determine the global "rules of the road" for cyber security.

Noteworthy Open Source Reports:

UK banks set for cyber security 'stress test'. 87 British banks, including major institutions such as Barclays, HSBC and Royal Bank of Scotland, took part in a simulation exercise that tested their defences against a cyber-attack. The test scenarios included automated teller machines (ATMs) being down due to a cyber-attack. The exercise also examined how financial institutions would cope if there was a major disruption to the transport infrastructure during the London 2012 Olympic Games. An Exercise Report discussing the results of the test is expected to be published in early 2012. The Financial Services Authority stated there would also be a Post Exercise Conference.

Analysis: The London 2012 Olympic Games were featured in a test scenario and were likely a factor in prompting this cyber security exercise. The Olympic Games could have an impact on a bank's response to a cyber attack if less bank staff is available for duty where many could be watching or attending the games. There could also be an impact if there were a major disruption to the transport infrastructure at the same time as a cyber attack, and there were difficulties in physically mobilizing staff to respond to this attack. The UK Government has made it clear that cyber security is a national priority. The updated UK Cyber Security Strategy was released publicly on November 25, 2011.

More Facebook scams reported. Open sources reported two separate scams targeting Facebook users. In the first instance, threat actors reportedly impersonated Facebook administrators and sent e-mails to users charging them with violating policy regulations. Users were then asked to pass along their account details, which included personal and financial information.

In the second instance, which occurred during American thanksgiving weekend, Facebook users were lured to give up their personal information by an offer of a program that would allow watching live streaming video of football games. The number of victims in both instances is unknown, though many Facebook users did report these spams to the legitimate Facebook support site.

- **Analysis:** Facebook is one of the world's most popular social networking websites. There are reportedly 16.6 Million Facebook users in Canada. Federal public servants were recently encouraged by the President of Treasury Board to use social media in the course of their work and government guidelines have just been released on the subject. Accordingly, a compromise or SPAM campaign in social media websites in the future may also affect federal departments as well as other workplaces. This risk will need to be managed by appropriate departmental officials .

UNCLASSIFIED
DRAFT

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-01-11 7:59 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous' Robin Hood credit card fraud campaign could hurt more than just banks

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Network World
Complete item: http://www.networkworld.com/news/2011/113011-anonymous-robin-hood-credit-card-253592.html?hpg1=bn

Description:
Hacktivist groups Anonymous and TeaMp0isoN have joined together in a new campaign that involves compromising credit card details and using them to donate money to charities, homeless people and anti-government protesters around the world. The two hacker outfits, who call their alliance p0isAnon, have named the new credit card fraud campaign "Operation Robin Hood" in reference to the famous English outlaw who, according to folklore, stole money from the rich and gave it to the poor.

Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks," p0isAnon said in a statement released on Monday. "Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe," it added.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-01-11 4:45 AM
To: Bendelier, Kenneth
Subject: Critical: Heads-Up - Team Poison, Anonymous campaigners claim first victims of OpRobinHood

Importance: High

Generated by your Alert Subscription on Folder:
- Anonymous
Source: itworld
Complete item: http://www.itworld.com/security/229141/team-poison-anonymous-campaigners-claim-first-victims-oprobinhood

Description:
Team Poison and Anonymous AKA PoisAnon when referring to the portion of each group working in cooperation to hack and harass commercial banks have counted coup in the campaign they call Operation Robin Hood, but didn't actually draw blood.

The alliance of a subset of Anonymous and Team Poison (which spells itself TeaMp0isoN, keeps a fan page on Facebook) announced yesterday they were launching Operation Robin Hood (#OpRobinHood).

OpRobinHood is a campaign to attack and, where possible, defraud large commercial banks for the benefit of the same mass of non-rich, non-powerful majority the Occupy Wall Street movement protests were organized to represent against what organizers called the economic injustice and exploitation by the banks, brokers and investment houses that make up the global financial industry.

Though both TeamPoison and Anonymous have attacked banks and financial-services companies in the past, neither has overtly tried to steal from or defraud the banks.

The first two successes touted by PoisAnon sticks to the hacktivist ethic that allows sabotage against large corporations but frowns on outright theft.

In two updates unconfirmed by the victims, PoisAnon claims to have found the weakness of two banks: The First National Bank of Long Island and the National Bank of California.

TeamPoison member or affiliate Phantom~, claimed to have found a flaw in the security of National Bank of California and that SQL injection and XSS exploits cracked the first line of security at the First National Bank of Long Island's main site, according to a description posted on PasteBin by Phantom~.

Neither bank has publicly admitted any damage or even illicit access.

According to Phantom's writeup of what the description referred to as 'research,' both banks were cracked, but none of the databases or customer information were touched.

"Why? Because innocent people could get money lost if I did, so this is just [a] warning for you to withdraw your money from banks," Phantom~ wrote.

That's more in line with the fair-play principles the Occupy movement advocated and the more traditional hacker ethic of harrying the rich and powerful while ignoring or protecting the little guy.

Hacktivists aren't always so careful. The reign of annoyance Anonymous-affiliates LulzSec conducted this summer frequently hurt the little guy by exposing personally identifiable private data from the hacks of members. So did the serial hacks of various Sony networks.

The PoisAnon announcement of OpRobinHood warned that the attacks would extract money from banks using credit cards and other means, but didn't say how.

It did warn those belonging to what the Occupy movement refers to as "the 99%" of society to move their money out of large banks and into credit unions, where it would be safe from attacks by PoisonAnon or other groups.

However they accomplish extortion, fraud or extraction, PoisonAnon does not intend to damage the little guys they claim to represent.

"The only ones to be victimized in this Operation is the rich," according to tweets from OpRobinHood leader _f0rsaken. "Stop complaining & worrying 99%! Donations to Shelters start soon #OpRobinHood."

Attacks or claims to have penetrated banks in California and Long Island, however, are designed to make the point that defacing web sites, stealing passwords and camping out in public parks aren't the only ways populist hacktivist groups can cause trouble for big companies.

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: December-01-11 4:31 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous Threatens Robin Hood Attacks Against Banks

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Slashdot
Complete item: http://it.slashdot.org/story/11/12/01/0049204/anonymous-threatens-robin-hood-attacks-against-banks

Description:
"Just in time for the holidays, hacktivist collective Anonymous has announced that it has teamed up with like-minded group TeaMp0isoN to donate to charity. The catch: they're using stolen credit data from big banks to make donations, in a campaign they're calling Operation Robin Hood. Is the #OpRobinHood campaign for real, or like previous threats against Wall Street and Facebook, just another hoax? Aesthetically, at least, the OpRobinHood video ticks all of the traditional Anonymous aesthetic requirements: a mashed-up 'p0isoaNoN' logo (green on black), a liberal dose of swelling choral music (via that movie trailer staple 'Europa,' by Globus), together with selected clips of Kevin Costner as Robin Hood: Prince of Thieves."

E-Secure-IT
https://www.e-secure-it.com

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: November-30-11 2:30 PM
To: Bendelier, Kenneth
Subject: Important: Anonymous launches new operation targeting big banks

Generated by your Alert Subscription on Folder:
- Anonymous
Source: Net-Security
Complete item: http://www.net-security.org/secworld.php?id=12024

Description:
Hacktivist collective Anonymous and hacking group Teamp0ison have announced that they will be joining their forces once again and starting another operation against banks.

They call it OpRobinHood, and apparently it will consist of stealing credit card details from big banks in order to use it to make donations to charities and others.

"In regards to the recent demonstrations and protests across the globe, we are going to turn the tables on the banks," they state. "Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks. Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people there money back."

E-Secure-IT
https://www.e-secure-it.com

Klassen, Nathan

From: Bendelier, Kenneth
Sent: November-30-11 7:58 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description: **Foreign hackers targeted Canadian firms.** "A leading cyber-crime expert says foreign hackers who launched a massive attack on Canadian government computers last fall also broke into the data systems of prominent Bay Street law firms and other companies to get insider information on an attempted $38-billion corporate takeover. Daniel Tobok, whose international cyber-sleuthing company was called in by a number of the firms hit by the attacks, says the hacking spree from computers in China were all connected to last year's ultimately unsuccessful takeover bid for Potash Corporation of Saskatchewan. "All those different attacks on companies, law firms and government were all interconnected — they weren't isolated incidents," he said in an interview with CBC News. Tobok said hackers penetrated the computer systems of at least seven of Canada's leading law firms in what experts believe was an attempt to mask the real target of the attacks — the few firms directly involved in the aborted Potash deal. The foreign hack-attack on Canadian law firms was "very sophisticated and highly targeted," he said. The hackers appeared to have been hunting exclusively for information on the Potash deal, and there was no evidence they had penetrated the confidential files of other clients of the firms affected."
Reference: http://www.cbc.ca/news/canada/story/2011/11/29/pol-weston-hacking-firms.html

2. Item Description: **United Nations agency 'hacking attack' investigated.** A group of hackers posted more than 100 e-mail addresses and log-in details it claimed to have extracted from the United Nations. Many of the e-mails involved appear to belong to members of the United Nations Development Programme (UNDP). The group, which identifies itself as Teampoison, attacked the UN's behavior and calledit a "fraud". A spokeswoman for the UNDP said the agency believed "an old server which contains old data" had been targeted. "UNDP is taking action to close any vulnerabilities on our Web site," she said. "Please note that UNDP.org was not compromised." The details were posted on the Web site Pastebin under the Teampoison logo. Many of the e-mail addresses gend in undp.org, but others appear to belong to members of the Organization for Economic Cooperation and Development, the World Health Organization, and the United Kingdom's Office for National Statistics. The poster noted that several of the accounts had "no passwords".
Reference: http://www.bbc.co.uk/news/technology-15951883

3. Item Description: **HP printers may be remotely set on fire, researchers say.** "Researchers at Columbia University in New York City found a HP LaserJet printer vulnerability that could allow a hacker to remotely control the device to launch cyberattacks, steal data that is being printed, and even instruct its mechanical components to overload until it catches fire. According to MSNBC, the researchers revealed the flaw they found does not affect only HP printers, but also other devices utilized by millions of individuals and companies that so far were considered to be safe. In the case of the HP printers which they thoroughly tested, the researchers relied on the fact remote software updates are not checked for signatures or certificates when they are being installed. In another demonstration, by sending a specially crafted print job, they were able to inject a code that would automatically scan printed documents for sensitive information, transmitting the data to a Twitter feed. They showed an infected computer could instruct the printer's fuser, the one used to dry off the paper, to continuously heat up until the device self-destructs or, if it lacks a fuse, to set itself on fire. They also proved a hijacked printer could act as a gate-opener for a full-effect attack on a company network. They even made a demo from computers running Mac and Linux operating systems. HP representatives argue the situation might not be all that disastrous, claiming their newer models check for signatures while performing firmware updates. However, they are currently investigating the issue to determine exactly what is affected and what can be done about it. Even though later printer models should be more secure, the researchers claim one of the printers used in their tests was purchased not long ago."
Reference: http://news.softpedia.com/news/HP-Printers-May-Be-Remotely-Set-On-Fire-Researchers-Say-237254.shtml

4. Item Description: **Targeted attacks steal credit cards from hospitality and educational institutions.** "A little more than a week ago SophosLabs became aware of a resurgence of an attack against the education and hospitality industries. In at least one case the malware has shown up at a financial services company. One thing important to note is that it has only been seen at moderate to small size organizations. These criminals aren't targeting Walmart. They are

after organizations with less investment in defensive counter-measures. The goal of this Trojan is to target credit card processing and point of sale (PoS) equipment and make off with all of the card details. It installs itself as a service in Windows and the filename is typically rdasrv.exe, while the service is called rdasrv. More recent samples have changed their name to be A#######.exe, where the # is a random number."
Reference: http://nakedsecurity.sophos.com/2011/11/30/targeted-attacks-steal-credit-cards-from-hospitality-and-educational-institutions/

5. Item Description: **Anonymous launches OpRobinHood against banks**. "Anonymous and other hacktivists have joined together to launch an attack on banks in response to recent crackdowns against the Occupy protest movement.TeaMp0isoN and Anonymous are joining forces to run OpRobinHood, which will involve using stolen credit details to donate to charities and others, supposedly at the expense of banks."
Reference: http://www.theregister.co.uk/2011/11/30/anon_oprobinhood/

6. Item Description: **Recent SPAM Reports.**

a. FBI Denver Cyber Squad advises citizens to be aware of a new phishing campaign.:
http://www.fbi.gov/denver/press-releases/2011/fbi-denver-cyber-squad-advises-citizens-to-be-aware-of-a-new-phishing-campaign?utm_campaign=email-Immediate&utm_medium=email&utm_source=denver-press-releases&utm_content=51037

b. Criminals sabotaging Cyber Monday, security experts warn.
http://www.computerworld.com/s/article/9222209/Criminals_sabotaging_Cyber_Monday_security_experts_warn

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Bendelier, Kenneth

From: E-Secure-IT <alert@e-secure-it.com>
Sent: November-30-11 5:56 AM
To: Bendelier, Kenneth
Subject: Critical: Heads-Up - Anonymous launches OpRobinHood against banks - 'We have come to take the 99%'s money back'

Importance: High

Generated by your Alert Subscription on Folder:
- Anonymous
- AnonOps
Source: The Register
Complete item: http://www.theregister.co.uk/2011/11/30/anon_oprobinhood/

Description:
Anonymous and other hacktivists have joined together to launch an attack on banks in response to recent crackdowns against the Occupy protest movement.

TeaMp0isoN and Anonymous are joining forces to run OpRobinHood, which will involve using stolen credit details to donate to charities and others, supposedly at the expense of banks.

In regards to the recent demonstrations and protests across the globe, we are going to turn the tables on the banks. Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks. Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people there [sic] money back.

Standard practice in cases where banks identify a fraudulent transaction is to reverse transactions and levy a chargeback a reversal of a prior outbound transfer of funds. So while customers with compromised credit cards might not lose out, charities who receive fraudulent donations might actually end up out of pocket.  TeaMp0isoN and Anonymous claim to have already taken Chase, Bank of America, and CitiBank credit cards with "big breaches across the map" and to have begun donating thousands to many protests around the world, as well as to homeless charities and other philanthropic organisations.

The hacktivists want bank account holders to withdraw their funds and deposit them in credit unions instead, something started with the legitimate Operation Cash Back scheme a few weeks ago. The hacktivists are not afraid to take on the banks, as their statement goes on to explain.

We are not afraid of the Police, Secret Service, or the FBI. We are going to show you banks are not safe and take our money back. We are going to hit the true evil while not harming their customers and helping others. We are not only starving the banks but are ready to start the attack. We have come to take the 99%'s money back. We are not asking permission.

TeaMp0isoN and Anonymous previously collaborated on the OpCensorThis rap song exercise, which the former was far more active in promoting than the latter. Anonymous needs little introduction. TeaMp0isoN is another (arguably more politically militant) hactivist group that's arguably most famous for defacing the BlackBerry blog around the time of the London riots.

E-Secure-IT

https://www.e-secure-it.com

Bendelier, Kenneth

From: <The SANS Institute <NewsBites@sans.org> on behalf of The SANS Institute <NewsBites@sans.org>
Sent: November-22-11 6:11 PM
To: Bendelier, Kenneth
Subject: SANS NewsBites Vol. 13 Num. 93 : Weatherford takes over cyber at DHS - heralding more balance with NSA; Details emerge about water utility hack; Anonymous gets forensics mail list archive

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Good News!
Yesterday, Mark Weatherford took over as Deputy Undersecretary for Cyber Security at the U.S. Department of Homeland Security. For the first time in many years, the U.S. cybersecurity program will be run by a technologist rather than by a lawyer. There are good reasons to believe that this change will herald an era of greater balance in national cybersecurity leadership between NSA and DHS. DHS has made five very important advancements in cybersecurity leadership, driven by technologists. The most important one shifts over $400 million per year away from paper-based checklist security and toward technology-based, automated, continuous monitoring of security, providing continuous situational awareness - a goal that DHS and NSA share. By combining the buying power of civilian agencies through DHS and of military agencies through NSA/DISA, total situational awareness and rapid risk reduction can be made very inexpensive across the federal government. That change, driven by DHS technologists, is in paragraph 28 of the directive posted at the White House site:
http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf

Paragraph 28 in this White House directive answers the question: "Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130?" Answer: "No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate re-authorization process is not necessary."

Alan

PS Because of the enormous security improvements to be gained through continuous monitoring, and the huge potential cost savings, and because of the powerful role played by Inspectors General (IGs) in determining what security initiatives are given priority, an independent oversight group has been established to evaluate IG and GAO reports on security over the next several years, measuring how well the IGs assess the continuous monitoring programs and how effectively they press agencies to move away from the discredited three-year static process. The independent group is led by Franklin Reeder who was the top IT official and Chief of Information Policy at OMB (where he led the development of the Privacy Act of 1974 and the Computer Security Act of 1987).

****

SANS NewsBites November 22, 2011 Vol. 13, Num. 93
****

TOP OF THE NEWS

More Details Emerge About Cyber Attack at Water Utility
Anonymous Gains Access to Computer Forensics Specialists Mailing List Archive
Wyden Says He Will Filibuster Protect IP Act if it Gets to the Floor
Legislators Investigating Possibility that Chinese Telecom Equipment

Enables Spying

THE REST OF THE WEEK'S NEWS
Bradley Manning Court Date Set
UK Police Shut Down 2,000+ Websites for Piracy and Theft
Deadline Extended for HIPAA Transaction Standard Compliance
Chrome Update Addresses JavaScript Flaw
AT&T Notifying Customers of Attempted Information Theft
Senate Will Vote on Cyber Security Legislation in 2012
Judge Says Warrant Required to Obtain Cell Phone Data
SOPA Support Dwindling

********** Sponsored By IBM **********

Register today for SANS Analyst webcast sponsored by IBM, "Integrating Security into Development, No Pain Required"
FREE SANS Analyst Paper also available at http://www.sans.org/info/91656

****

TRAINING UPDATE
- --EURO SCADA & Process Control System Security Summit, Rome, Dec 1-2, 2011 Pre-Summit Courses November 26-30, 2011 Post-Summit Courses December 3-4, 2011 Gain the most current information regarding SCADA and Control System threats and learn how to best prepare to defend against them.
http://www.sans.org/eu-scada-2011/
- --SANS San Antonio 2011, San Antonio, TX, November 28-December 5, 2011
7 courses. Bonus evening presentations include Effective Methods for Implementing the 20 Critical Security Controls; and Assessing
Deception: Are They Lying to You?
http://www.sans.org/san-antonio-2011/
- --SANS London 2011, London, UK, December 3-12, 2011
18 courses. Bonus evening presentations include IPv6 Challenges for Intrusion Detection and Understanding How Attackers Bypass Network and Content Restrictions.
http://www.sans.org/london-2011/
- --Incident Detection & Log Management Summit, Washington DC, December 7-8, 2011 Learn the latest techniques to detect breaches and intrusions!
http://www.sans.org/incident-detection-summit-2011/
- --SANS CDI 2011, Washington, DC, December 9-16, 2011
27 courses. Bonus evening presentations include Emerging Trends in Data Law and Investigations, and Critical Infrastructure Control Systems Cybersecurity.
http://www.sans.org/cyber-defense-initiative-2011/
- --SANS Security East 2012, New Orleans, LA January 17-26, 2012
11 courses. Bonus evening presentations include Advanced VoIP Pen
Testing: Current Threats and Methods; and Helping Small Businesses with Security.
http://www.sans.org/security-east-2012/
- --SANS Monterey 2012, Monterey, CA January 30-February 4, 2012
6 courses. Bonus evening presentations include Who Do You Trust? SSL and TLS Under Attack; and IOS Programming Demo.
http://www.sans.org/monterey-2012/
- --SANS Phoenix 2012, Phoenix, AZ February 13-18, 2012
7 courses. Bonus evening presentations include Desktop Betrayal:
Exploiting Clients Through the Features They Demand; and Windows Exploratory Surgery with Process Hacker.
http://www.sans.org/phoenix-2012/

- --Looking for training in your own community?
http:sans.org/community/ Save on On-Demand training (30 full courses) - See samples at
http://www.sans.org/ondemand/discounts.php#current
Plus Perth, Atlanta, and Bangalore all in the next 90 days.
For a list of all upcoming events, on-line and live: www.sans.org
****

TOP OF THE NEWS

--More Details Emerge About Cyber Attack at Water Utility (November 19 & 21, 2011) A hacker reportedly gained access to a Supervisory Control and Data Acquisition (SCADA) system at a water utility in Illinois and tampered with a water pump, causing it to burn out. The attack used IP addresses that originated in Russia. The exploit was conducted through the phpMyAdmin open source tool, which has a significant number of known vulnerabilities; questions are arising about why this particular piece of software was being used at the water utility. Federal authorities are investigating the incident. In a separate incident, a hacker using the online handle "pr0f" claims to have launched an attack against a SCADA system at a Houston, Texas, water treatment facility. That attack, according to the hacker, was made possible through "gross stupidity,"
as the software he exploited was protected with a three-character password.
http://www.zdnet.com/blog/security/scada-systems-at-the-water-utilities-in-illinois-houston-hacked/9821?tag=mantle_skin;content
http://www.informationweek.com/news/security/attacks/231903481
http://www.h-online.com/security/news/item/Hacker-destroys-pump-in-US-water-utility-1381968.html
http://www.bbc.co.uk/news/technology-15817335
http://krebsonsecurity.com/2011/11/cyber-strike-on-city-water-system/
http://www.computerworld.com/s/article/9222014/Apparent_cyberattack_destroys_pump_at_Ill._water_utility?taxonomyId=82
http://www.scmagazineus.com/water-utilities-in-illinois-houston-reportedly-hacked/article/217173/
http://news.cnet.com/8301-1009_3-57327968-83/hacker-says-he-broke-into-texas-water-plant-others/
http://www.v3.co.uk/v3-uk/news/2126382/scada-hack-blamed-breach-water-plant

--Anonymous Gains Access to Computer Forensics Specialists Mailing List Archive (November 19, 2011) Members of the hacking collective known as Anonymous have gained access to the Google account of a retired supervisor of a cyber crime investigation organization in southern California and released 38,000 emails taken from that account. Among the information exposed in the hack is the International Association of Computer Investigation Specialists mailing list archive, which includes discussions from specialists around the world.
http://www.wired.com/threatlevel/2011/11/anonymous-hacks-forensics/

--Wyden Says He Will Filibuster Protect IP Act if it Gets to the Floor (November 21, 2011) US Senator Ron Wyden (D-Oregon) says he will filibuster the Senate's Protect IP Act (PIPA), which is similar to the House's Stop Online Piracy Act (SOPA). Wyden put a hold on the bill earlier this year, but there are rumors that there are enough votes to override the hold after the Thanksgiving recess.
http://www.wired.com/threatlevel/2011/11/wyden-pipa-filibuster/
[Editor's Note (Murray): This bill is very unpopular with the public.
Demand Progress asserts that 20000 of their members have asked Senator Wyden to read their names as part of his threatened filibuster. On the other hand, the bill is popular among the legislators because it is backed by the very generous RIAA and MPAA. The rights of publishers, no matter how legitimate, do not trump all other interests. The legitimacy of the rights that one asserts is not measured by the contribution that accompanies the assertion.]

--Legislators Investigating Possibility that Chinese Telecom Equipment
Enables Spying
(November 17 & 21, 2011)

The US House Permanent Select Committee on Intelligence (HPSCI) will conduct an investigation into the possibility that Chinese telecommunications companies operating in the US are conducting cyber espionage. The committee will examine the possibility that Chinese telecommunications equipment - servers, routers and switches - could be used to help the Chinese government obtain sensitive information from the US.
http://www.computerworld.com/s/article/9221998/House_committee_to_investigate_China_s_Huawei_ZTE
http://www.theregister.co.uk/2011/11/21/us_probe_chinese_telco_firms/
http://www.wired.com/dangerroom/2011/11/china-trojan-horse-congress/

****

THE REST OF THE WEEK'S NEWS
--Bradley Manning Court Date Set
(November 21, 2011)
More than a year-and-a-half after he was arrested, Pfc Bradley Manning, who allegedly leaked classified documents to WikiLeaks, will have a public hearing at Ft. Meade in Maryland. The Article 32 hearing is set for December 16; it is similar to a civilian court grand jury hearing in that the judge will hear evidence to determine if there are sufficient grounds for a court-martial. If convicted on all charges, Manning could face life in prison. The hearing will be open to the media and the public except when classified information is discussed.
http://www.wired.com/threatlevel/2011/11/bradley-manning-hearing/

--UK Police Shut Down 2,000+ Websites for Piracy and Theft (November 18 & 21, 2011) Police in the UK have shut down more than 2,000 websites believed to be selling counterfeit or non-existent merchandise. The goods offered for sale include clothing, jewelry and sporting equipment. In some cases, payment was taken but the merchandise was never delivered. UK domain registrar Nominet helped pinpoint and shut down the offending sites. In a separate but related story, proposed changes to Nominet policy would allow the organization to deny requests for site takedowns unless provided with a court order or the site allegedly puts the public at risk, for instance, by selling questionable medications.
http://www.bbc.co.uk/news/technology-15820758
http://www.gizmodo.co.uk/2011/11/police-knock-2000-counterfeiting-co-uk-domains-offline/
http://www.macworld.co.uk/digitallifestyle/news/index.cfm?newsid=3319720
http://www.eweekeurope.co.uk/news/police-shutter-2000-fraudulent-shopping-sites-46617
http://www.theregister.co.uk/2011/11/18/dotuk_takedown_refresh/

--Deadline Extended for HIPAA Transaction Standard Compliance (November 17, 2011) Federal officials are giving healthcare providers an additional three months to comply with the new version of the Health Insurance Portability and Accountability Act (HIPAA) transaction and code set standards. Initially, the deadline was set for January 1, 2012, but now providers have until March 31, 2012 to comply. The standard applies to medical transaction processing, and is aimed at helping to track diagnoses and treatment.
http://www.computerworld.com/s/article/9221981/Feds_back_off_on_Jan.1_eHealth_standards_deadline?taxonomyId=84
http://www.cms.gov/ICD10/Downloads/CMSStatement5010EnforcementDiscretion111711.pdf

--Chrome Update Addresses JavaScript Flaw (November 17 & 18, 2011) Google's latest Chrome update addresses a vulnerability in the browser's JavaScript engine. The out-of-bounds write flaw could be exploited to allow remote code execution, but because Chrome uses native sandboxing, the vulnerability is considered less severe. Google Chrome 15.0.874.121 is available for Windows, Mac OS X, and Linux.
http://www.computerworld.com/s/article/9222000/Google_Chrome_update_addresses_high_severity_flaw?taxonomyId=145
http://www.msnbc.msn.com/id/45357749/ns/technology_and_science-security/
http://www.h-online.com/open/news/item/Chrome-15-update-fixes-high-risk-vulnerability-1380555.html

--AT&T Notifying Customers of Attempted Information Theft (November 21, 2011) AT&T is letting its customers know that attackers attempted to steal online account data; the company does not believe that any information was actually

obtained. The "organized and systematic" effort to gather the data was conducted with the help of auto-script technology to see which AT&T phone numbers are linked to which AT&T online accounts. AT&T spokesman Mark Siegel wrote in an email to customers that an investigation is underway.
http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/11/21/bloomberg_articlesLV14976S972L.DTL
http://www.washingtonpost.com/business/technology/atandt-customer-account-hack-attempted-no-accounts-compromised/2011/11/21/gIQA0tcoiN_story.html
http://technolog.msnbc.msn.com/_news/2011/11/21/8935345-att-tells-customers-of-hack-attempt
http://www.theregister.co.uk/2011/11/21/att_attack/
[Editor's Comment (Northcutt): I am an ATT customer and I have not received anything by email. The news stories say it was one percent of customers. We will see what next week brings.]

--Senate Will Vote on Cyber Security Legislation in 2012 (November 17, 2011) Senate Majority Leader Harry Reid (D-Nevada) has informed House Republicans that he will bring cyber security legislation to the floor early next year. In a letter to Senate Minority Leader Mitch McConnell (R-Kentucky), Reid wrote that "given the magnitude of the threat [of cyber attacks and cyber espionage] and the gaps in the government's ability to respond, we cannot afford to delay action on this critical legislation."
http://www.bloomberg.com/news/2011-11-17/reid-to-move-on-senate-cybersecurity-legislation-in-early-2012.html
http://cybersecurityreport.nextgov.com/2011/11/full_senate_to_vote_on_cyber_legislation_upon_return_next_year.php?oref=latest_posts

--Judge Says Warrant Required to Obtain Cell Phone Data (November 17, 2011) US District Judge Lynn Hughes has upheld a 2010 ruling that federal authorities need a search warrant to gain access to cell phone data that could be used to track the user's whereabouts. The earlier ruling from a magistrate judge denied three separate requests for cell phone companies to provide the information without a warrant. Hughes's ruling says that the information sought is constitutionally protected and requires a search warrant to be obtained. The authorities were requesting the information under the Stored Communications Act.
http://www.washingtonpost.com/national/houston-federal-judge-rules-that-feds-need-search-warrant-to-get-cellphone-tracking-data/2011/11/18/gIQABS8OZN_story.html

--SOPA Support Dwindling
(November 17 & 18, 2011)
Opposition to the House's Stop Online Piracy Act (SOPA) is on the rise.
Legislators on both sides of the aisle have voiced opinions that the legislation would not work as currently drafted. According to Representative Darrell Issa (R-California), original sponsors of the bill are showing less support for it as they learn about the impact its provisions could have on the Internet. Issa has called the measure extreme and said that he "didn't like the way [it] was being assembled,"
acknowledging the need for flexibility because "any rule you write has to assume innovation will make it obsolete quickly." The Department of Energy's Sandia National Laboratory has said that SOPA would thwart the deployment of DNSSEC. Sandia's mission includes research on infrastructure security and cyber security. A hearing on the issue earlier this week drew criticism for heavily favoring supporters of the measure in representation. Organizations that felt unrepresented at the hearing raised public outcry, asking people to contact their legislators and let their opinions be known.
http://thehill.com/blogs/hillicon-valley/technology/194635-gops-issa-effort-to-grease-the-skids-for-online-piracy-bill-has-failed
http://arstechnica.com/tech-policy/news/2011/11/strange-bedfellows-nancy-pelosi-ron-paul-join-sopa-opposition.ars
http://www.theregister.co.uk/2011/11/20/sopa_breaks_dnssec/
http://news.cnet.com/8301-31921_3-57326956-281/sandia-labs-sopa-will-negatively-impact-u.s-cybersecurity/
http://www.wired.com/threatlevel/2011/11/blacklist-bill-analysis/
SOPA FAQ:
http://www.computerworld.com/s/article/9221979/FAQ_What_the_SOPA_soap_opera_is_all_about?taxonomyId=144

****

The Editorial Board of SANS NewsBites

John Pescatore is Vice President at Gartner Inc.; he has worked in computer and network security since 1978.

Stephen Northcutt founded the GIAC certification and is President of STI, The Premier Skills-Based Cyber Security Graduate School, www.sans.edu.

Dr. Johannes Ullrich is Chief Technology Officer of the Internet Storm Center and Dean of the Faculty of the graduate school at the SANS Technology Institute.

Ed Skoudis is co-founder of InGuardians, a security research and consulting firm, and author and lead instructor of the SANS Hacker Exploits and Incident Handling course.

William Hugh Murray is an executive consultant and trainer in Information Assurance and Associate Professor at the Naval Postgraduate School.

Rob Lee is the curriculum lead instructor for the SANS Institute's computer forensic courses (computer-forensics.sans.org) and a Director at the incident response company Mandiant.

Rohit Dhamankar is a security professional currently involved in independent security research.

Tom Liston is a Senior Security Consultant and Malware Analyst for InGuardians, a handler for the SANS Institute's Internet Storm Center, and co-author of the book Counter Hack Reloaded.

Dr. Eric Cole is an instructor, author and fellow with The SANS Institute. He has written five books, including Insider Threat and he is a founder with Secure Anchor Consulting.

Ron Dick directed the National Infrastructure Protection Center (NIPC) at the FBI and served as President of the InfraGard National Members Alliance - with more than 22,000 members.

Mason Brown is one of a very small number of people in the information security field who have held a top management position in a Fortune 50 company (Alcoa). He is leading SANS' global initiative to improve application security.

David Hoelzer is the director of research & principal examiner for Enclave Forensics and a senior fellow with the SANS Technology Institute.

Alan Paller is director of research at the SANS Institute.

Marcus J. Ranum built the first firewall for the White House and is widely recognized as a security products designer and industry innovator.

Clint Kreitner is the founding President and CEO of The Center for Internet Security.

Brian Honan is an independent security consultant based in Dublin, Ireland.

David Turley is SANS infrastructure manager and serves as production manager and final editor on SANS NewsBites.

Please feel free to share this with interested parties via email, but no posting is allowed on web sites. For a free subscription, (and for free posters) or to update a current subscription, visit http://portal.sans.org/

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (Darwin)
Comment: GPGTools - http://gpgtools.org

iEYEARECAAYFAk7L87EACgkQ+LUG5KFpTkaYgQCdFurNYZRgmChPztpG6oto4FQd
W6oAoJl25IQnQU2cjJ+6EfglMRPYtsKt
=o5Yn
-----END PGP SIGNATURE-----

s.19(1)

Dvorkin, Corey

From: Scrivens, Mark <MScriven@justice.gc.ca>
Sent: November-25-11 9:35 AM
To: Dvorkin, Corey; Slatkoff, Ari; Pilon, Claude
Cc: Bradley, Kees
Subject: RE: weird

[redacted]

From: Dvorkin, Corey [mailto:Corey.Dvorkin@ps-sp.gc.ca]
Sent: 2011-Nov-25 8:55 AM
To: Slatkoff, Ari (PSEPC-SPPCC); Scrivens, Mark; Pilon, Claude (PSEPC-SPPCC)
Cc: Bradley, Kees
Subject: FW: weird

weird indeed!

The safeguards could also afford protection to some grey hat hackers similar to the Anonymous collective and LulzSec, and at minimum would ensure they were not simply arrested, she said.

Maurushat was pitching the ethical hacking standards dumped by Australia to the Canadian Government and said she hoped the effort to pay off within three years.

If it did, Canada would be the first country to have safeguards for ethical hacking.

Corey Michael Dvorkin
Acting Director / Directeur par intérim
Cyber Policy / Politiques cyber
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 OP8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

From: Bradley, Kees
Sent: November 25, 2011 8:40 AM
To: Dvorkin, Corey
Subject: weird

http://www.scmagazine.com.au/News/281205,government-shuns-ethical-hacker-safeguards.aspx

check the reference to ethical hacking in Canada...

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-25-11 8:21 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; [redacted] Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 25, 2011 / le 25 novembre 2011

Print media

Explosion de cybercrimes
Dans une année où la criminalité a continué de fléchir, les infractions commises au moyen d'un ordinateur ont cependant connu une hausse vertigineuse de 70 % au Québec, en 2010. C'est ce que révèlent les plus récentes données du ministère de la Sécurité publique, compilées à partir des statistiques annuelles des enquêtes menées par les différents corps de police de la province. Le Ministère dénombre pas moins de 1270 crimes comportant l'utilisation d'un ordinateur ou d'Internet, en 2010, soit 520 de plus que l'année précédente. Le Journal de Montréal, 8

Online media

UK Government Releases Cyber Security Strategy
The UK government has ruled out introducing new anti-cyber crime laws, but could employ hackers as part of its new cyber security strategy released today. A boost to Ministry Defence spending and a one-stop shop for reporting cyber crime are stars of the new policy, but courts will be encouraged "to use existing powers to impose appropriate online sanctions for online offences," according to the report. Cyber crime will be handled by a single specialist group handled - the new National Crime Agency (NCA) - which will include "those with specialist skills" to back up police. Otherwise known as good-guy hackers. Huffington Post (UK); The Guardian; The Telegraph; BBC News; ZDNet; SC Magazine UK; British Forces News; eGovmonitor

Government shuns ethical hacker safeguards
The Australian Government has rejected efforts to create legal safeguards for ethical hacking, according to a UNSW researcher. Researcher Alana Maurushat was among several security professionals to raise the idea during the recent reviews of Australia's cybercrime laws. The safeguards could also afford protection to some grey hat hackers similar to the Anonymous collective and LulzSec, and at minimum would ensure they were not simply arrested, she said. Maurushat was pitching the ethical hacking standards dumped by Australia to the Canadian Government and said she hoped the effort to pay off within three years. If it did, Canada would be the first country to have safeguards for ethical hacking. SC Magazine

Phishing E-mail Alert to Members of Concordia University
Canada based Concordia University's IITS (Instructional and Information Technology Services) has advised everyone holding e-mail accounts with the Institution for remaining vigilant of phishing electronic mails, which are presently aiming at their mailboxes. Concordia.ca published this dated November 16, 2011. Posing as a message from IITS, the fake e-mails addressing faculty and other staff say that the e-mail has been sent to all teachers as well as staff members from the IITS HelpDesk of The Concordia University in connection with accounts on Alcor Webmail that they hold. It then says

that IITS noticed campus members' accounts on Alcor Webmail that spammers compromised. The miscreants acquired admission into Webmail accounts followed with utilizing them to carry out illegitimate online operations. Presently, IITS HelpDesk is upgrading and maintaining its database, while it aims to upgrade its E-mail Security Server to have improved online facilities. SPAM Fighter

Beware the Black Friday iTunes malware scam

It's not just bargain hunters taking advantage of Black Friday, the scammers are too. Be on the lookout for malware-loaded emails disguised as a $50 iTunes gift certificates. The malware opens up a backdoor on the user's system to allow more malware to be installed. ZDNet; Times of India; The Telegraph; CNet

All-round Scam on Facebook Pushes Backdoor Trojan

Security researchers from Microsoft lately detected one significantly all-round social engineering scam that dupes Facebook visitors into loading one especially malicious backdoor Trojan, which's equipped with keylogging abilities. And though the e-mails utilized for wooing the users are different they actually take onto spoofed YouTube web-pages, published Help Net Security dated November 18, 2011. Thus, when a user lands on one such fake YouTube web-page, he's told for making his Web-browser up-to-date with one given ActiveX component, which however, is an advanced backdoor that bypasses firewall and has been identified as Backdoor:Win32/Caphaw.A. The malware contains virtually all malicious functions associated with loading File Transfer Protocol (FTP) server, keylogger, as well as proxy server onto the target PC. Additionally, there's one integral remote desktop feature that's associated with Virtual Network Computing (VNC), the familiar open-source project. SPAM Fighter

McAfee Suspects Sophisticated Indulge at Cybercriminals' Demeanor

According to McAfee's third quarter security threats report (Q3-2011), revealed by Intel-owned security technology firm, cybercriminals seems to change their tactics of circulating malware for avoiding law enforcement, reports v3.co.uk on November 21, 2011. Commenting on the findings, Toralv Dirro, Security Strategist at McAfee Labs EMEA (Europe Middle East and Africa) said that as a result of a sudden augment of virus indulgence, large botnets are being shut down and operators are being driven to concentrate more on smaller and localized networks, highlights v3.co.uk on November 21, 2011. While explaining the matter, Dirro claimed that law enforcement becomes more interesting when the botnet is bigger. It is completely different in case of smaller botnets and the matter becomes rather uninteresting. SPAM Fighter

Cyber attack that wasn't to live forever on the web

Though it apparently wasn't true, the purported cyber attack by the Russians on the Curran-Gardner water system will be accepted as fact by current and future generations. There are people who always will believe that the original theory about the Russian hackers is true and the subsequent denial by the Department of Homeland Security is a conspiracy to hide the truth. Joe Weiss, the San Francisco-based cybersecurity expert who first reported on his blog the suspicion that Russians had launched a cyber attack on a U.S. water system, one that allegedly turned out to be the Curran-Gardner Township Public Water District, is not ready to concede that the attack never happened. State Journal-Register

Hayward, Jane

From: Glazer, David on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-17-11 8:22 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
November 17, 2011 / le 17 novembre 2011

MINISTER / MINISTRE

'My message is we can't lose hope'
Canada's new top cop is starting his job with some solemn pledges: to get to the bottom of sexual harassment allegations within the RCMP; restore the tarnished national reputation of the police force; and lead a team of senior managers without bullying them into submission. "Appropriately, some of the stumbles and the challenges that we face are brought to Canadians' attention," incoming RCMP Commissioner Bob Paulson said Wednesday. "I get this. I recognize that I have a lot of work to do, a lot of work ahead of me as we continue to transform the RCMP. Accountability and leadership will be areas of focus for me and my team as we go forward." Within minutes, Paulson appeared in the foyer of the House of Commons with **Public Safety Minister Vic Toews**, who revealed that the government is concerned about recent complaints by female Mounties of sexual harassment and has referred the matter to the Commission for Public Complaints Against the RCMP. Ottawa Citizen, A3 (The StarPhoenix, Leader-Post, Windsor Star); Times & Transcript; Telegraph-Journal (Edmonton Journal, Calgary Herald, The Province); Le Devoir; L'Acadie Nouvelle (Le Droit); Whig-Standard (London Free Press); Chronicle-Herald (The Record); Toronto Star; La Presse

Province nearing policing deal
Manitoba is days away from securing a new 20-year deal to keep the Mounties in the province, Attorney General Andrew Swan said Wednesday. **Mike Patton, a spokesman for Public Safety Minister Vic Toews, said Wednesday the same terms and conditions of a new RCMP policing contract will apply to all provinces, including Saskatchewan and Alberta, with the main goal of striking "an appropriate balance between giving our police forces the tools necessary to do their job and ensuring fairness for Canadian taxpayers."** Winnipeg Free Press, A4

The Mounties get their man
An editorial states, "Bob Paulson is a tough Mountie with a military background and 25 years experience dealing with gangsters, murderers, terrorists and all manner of miscreants. So what messages was the newly-named Royal Canadian Mounted Police commissioner anxious to deliver when his appointment was announced on Wednesday?... While the RCMP commissioner would continue to report to Parliament through the **Public Safety Minister** on policing and law enforcement, he or she would answer to the board for administration and organization…The combination of a new majority Conservative government and a new commissioner who has worn the red serge tunic offers a chance to bring in genuine reform. That should be the priority. The Mounties' image needs restoring. So does the public trust." Toronto Star, A22

Restoring the RCMP
An editorial states, "The RCMP's new commissioner better be a quick study, because Bob Paulson appears to have a tough case to crack. On the same day the veteran Mountie was appointed head of Canada's national police force, the federal government announced it will ensure there's an independent investigation of allegations of widespread sexual harassment in the RCMP. "It is imperative that all members of the RCMP be free to face the daily and expected challenges of a day's work without harassment and without fear of mistreatment by co-workers and superiors," said Public Safety Minister Vic Toews on Wednesday…" Calgary Herald, A14

CYBER SECURITY / CYBERSÉCURITÉ

*** Canadian servers host Syrian government sites**

More than a dozen Syrian government websites are being hosted on Canada-based servers, according to a new research report that raises questions about the effectiveness of international sanctions against a regime accused of ongoing crimes against humanity. Globe and Mail, A4

*** Website snafu strictly 'routine'**
"Routine maintenance" -- not Anonymous -- knocked Mayor Rob Ford briefly off the Internet Wednesday. But the Sun has learned Toronto Police are investigating a threat that Anonymous, a group of hacker activists, allegedly made against Ford and the city. Toronto Sun, 5; Toronto Star

*** Facebook security breach raises vulnerability concerns**
A widespread spam attack on Facebook has caused violent and pornographic images to be posted on some users' profile pages, representing one of the worst security breaches in the website's history and raising concerns about its vulnerability to hackers. Daily Gleaner, D6

*** Malicious virus armies target Android devices**
The arsenal of malicious code aimed at Android- powered gadgets has grown exponentially, with criminals hiding viruses in applications people download to devices, according to Juniper Networks. The Province, A23

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

'Blue-collar worker with white-collar mentality'
As Prime Minister Stephen Harper officially announced Bob Paulson as the new RCMP commissioner Wednesday, observers said he will need to find a way to restore the reputation of a force that has been mired in scandal and instil a new sense of pride among the rank and file. Michel Juneau-Katsuya, a former RCMP officer and agent with the Canadian Security Intelligence Service, said one thing he'll be watching for is how Paulson responds when something bad happens. Ottawa Citizen, A3 (The Gazette); Globe and Mail; National Post; National Post; Red Deer Advocate (The Guardian); Chronicle-Herald; Times Colonist

*** Mounties not in disarray, says outgoing top cop**
Departing RCMP Commissioner William Elliott insisted Wednesday that the RCMP is not a force in disarray and that the vast majority of Canadians still approve of the job that the Mounties are doing. While he admitted that being commissioner at times was a "daunting challenge," he said he believes the force is in a better position than when he took over more than four years ago. Daily Gleaner, A9 (Edmonton Journal)

*** Stalking, coercion alleged**
An RCMP sex-conduct hearing was rocked by new evidence Wednesday as an unexpected witness came for-ward claiming that her boss, a well-connected B.C. Mountie, coerced her into sex, criminally stalked her and made veiled threats. Edmonton Journal, A19 (Calgary Herald, The Province, Times Colonist)

*** 'Superheroes' get mixed reviews**
A group of young B.C. men who dressed as superheroes to confront would-be sex offenders are gaining wide praise from the public, but are drawing criticism from police who say crime fighting should be left to the proper authorities. Ottawa Citizen, A8 (Edmonton Journal, Times Colonist); Globe and Mail; Globe and Mail; National Post; Ottawa Sun (Whig-Standard); Telegraph-Journal (Calgary Herald); Chronicle-Herald (Red Deer Advocate); L'Acadie Nouvelle; Toronto Star; Vancouver Sun

*** No job for the Mounties**
An opinion piece states, "Robert Fowler, in a most credible and readable account of his 130-day kidnapping, A Season in Hell, writes that his survival was "a near run thing." That judgment brings home to all of us the near-death experiences these kidnappings are. In writing he provides an enormous public service to those of us who observe such events from a distance and grope for solutions that we hope do less harm than good... Fowler also paints a dismaying picture of the role played by the RCMP during the kidnapping. Starting in the late 1990s the RCMP began to promote a role for its officers in these international kidnappings. The arguments were that these were crimes and their mandate required involvement. Their arguments ignored the reality that the force had no mandate to enforce Canadian law outside the borders of Canada..." Ottawa Citizen, A15

*** A lousy job, but**
An editorial states, "To say Bob Paulson, newly appointed head of the ailing RC-MP, has his work cut out is to state the blindingly obvious. Even before he took on his new role Wednesday, the force was dealing with a widening sexual

harassment scandal involving complaints from female officers. The issue has been referred to the Commission for Public Complaints Against the RCMP and Paulson has called for an internal review..." Ottawa Citizen, A14

*** Province targets registry issue**
The clock is ticking and Quebec knows it. One day after resuming the charge to amend Ottawa's omnibus anti-crime bill, the province has signalled it's ready to go to bat against Ottawa again on another front: plans to scrap the long-gun registry. The Gazette, A12; Edmonton Journal; La Tribune (Le Devoir)

*** RCMP cameras loaded with sensitive images found in trees**
RCMP have been left red-faced after police investigation pictures, including some depicting dead bodies, were found on surveillance cameras installed in a Grand Forks, B.C., tree, forcing police to contact victims' families after the cameras were taken. Staff Sergeant Dan Seibel said Mounties want the cameras back so they can review what's on their memory cards and call relatives. Globe and Mail, S3 (The Guardian, Chronicle-Herald); Telegraph-Journal

*** Uprooting dysfunctions**
An editorial states, "It is the rare individual who indicts his organization on the same day he is called to lead it. But incoming RCMP Commissioner Bob Paulson is right to make rooting out harassment within the RCMP his top priority, to order a comprehensive review of existing allegations, and to say, "This is not the RCMP that I joined. And this one cannot continue." The force's dysfunctions are legion and include bungled terror investigations and instances of brutality against innocent people - but reducing workplace harassment, so critical to morale and to the public's trust, is an excellent place to start. It's good that he's serious, because the RCMP has been less than serious about sexual harassment in the past..." Globe and Mail, A18

*** Mountie charged with drunk driving**
RCMP in Manitoba have charged one of their own with drunk driving. Const. Tracey Santo is charged with impaired driving and driving over the legal limit. Her first court date is Nov. 21. Winnipeg Sun, 14; Winnipeg Free Press

*** RCMP officer charged with drunk driving**
A B.C. RCMP officer has been charged with drunk driving offences and will appear in Surrey, B.C. provincial court. Cpl. Tony Bernard has been charged with drinking and driving, refusal to provide a breath sample, dangerous operation of a motor vehicle and failing to stop after an accident, RCMP said. Times & Transcript, A2; Edmonton Journal; The Province

*** Nos hells INQUIÈTENT LE FBI**
Même en prison, les Hells Angels québécois continuent de sévir, au point de contribuer à "un problème grandissant" à la frontière canado-américaine. C'est le constat tiré par le Federal Bureau of Investigation, la plus grande organisation policière des États-Unis. Le FBI pointe la réserve mohawke d'Akwesasne comme étant l'un des principaux maillons faibles de la lutte à la contrebande. Le Journal de Montréal, 5

*** Tobacco shop opens again despite raid - Provincial seizure**
One day after provincial authorities seized thousands of Mohawk cigarettes from the Dakota Chundee Smoke Shop, store clerks had restocked their tobacco supply and reopened the doors at noon. "It's business as usual," store employee Charles Blacksmith said Wednesday, three hours after it reopened. Winnipeg Free Press, A9

*** Lacroix arrêté dans une affaire de fraude**
Des policiers de la Sûreté du Québec (SQ) et de la Gendarmerie royale du Canada (GRC) ont procédé à l'arrestation de quatre individus, dont l'homme d'affaires de Lac-Beauport Jean-Noël Lacroix, au cours de la journée d'hier, afin qu'ils répondent de leur implication dans une affaire présumée de fraude à caractère fiscal d'une valeur d'un million de dollars. Le Soleil, 21

*** Bill would ban wearing masks during riots**
A private member's bill to ban the use of masks in a riot is set to see its first round of debate in the House of Commons today. Calgary Herald, A9 (Times Colonist)

*** Il se fait confisquer ses sept armes**
Un homme du Saguenay-Lac-Saint-Jean s'est fait saisir ses sept armes à feu après avoir publié sur YouTube des dizaines de vidéos le montrant en train de tirer. Au total, il a envoyé plus de 200 vidéos sur lesquels on le voit en train de tirer en forêt. Journal Montreal, 16

*** La SQ frappe les trafiquants**
Une trentaine de personnes reliées au trafic de stupéfiants et à des fraudes à caractère fiscal ont fait l'objet d'une vaste opération policière, tôt hier matin dans la grande région de Québec. Journal Montreal, 4

*** Man charged with feeding 'pot bears' once again**
Allen Piche has apparently resumed his "pot bear" picnic. The Christina Lake man, charged last year with feeding up to two dozen black bears on his rural property, has allegedly done it again. Piche, who also faces charges of running a marijuana grow-op, was reportedly caught feeding bears again following a months-long investigation by conservation officers. The Province, A12 (Times Colonist)

*** Scrapping gun registry won't harm criminal investigations**
An opinion piece states, "Reports that scrapping the long-gun registry would "significantly compromise" law enforcement's ability to trace firearms in Canada are without factual basis..." The Province, A15

*** A waste of time over the gun registry**
An opinion piece states, "As if the long list of disagreements in the provincial realm wasn't enough to keep them occupied, Liberals and New Democrats found another argument this week completely outside their jurisdiction. "Resolved: That this house support law-abiding gun owners and support the federal government's decision to repeal the federal long-gun registry."..." Times Colonist, A10

*** One region, one police force**
An opinion piece states, "It's about time. Greater Victoria appears to be edging, ever so slowly, closer to a full integration of its police forces, a step that is long overdue. That does not mean that the fight is over. There is still plenty of resistance to the idea, but every step toward integration should help to ease some of the fears of what a single force might bring..." Times Colonist, A10

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

*** Mounted attack**
Handling allegations of systemic sexual harassment within the RCMP is top of mind for the new top Mountie. The national police force is also dealing with upcoming budget cuts and a reputation tarnished by high-profile scandals such as Robert Dziekanski's 2007 death after cops repeatedly used a Taser on him, and accusations it dropped the ball on investigating B.C. serial killer Robert Pickton. Ottawa Sun (Winnipeg Sun, Toronto Sun, Calgary Sun, Edmonton Sun)

*** Aid to sex-trade workers can't keep PACE with funding cuts**
As the Missing Women Commission of Inquiry spends millions to find out about murdered and missing women, the only Vancouver group that helps women leave the survival sex trade is about to run out of money. The Providing Alternatives Counselling and Education Society (PACE) - a Vancouver group that for 17 years has provided advocacy and support to sex workers dealing with family, financial, tenancy and addiction issues - can only cover its payroll until three days before Christmas. The Province, A19

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

*** 14 arrested for fraud**
Police in the Toronto area have arrested 14 people and laid 145 charges in connection to a massive, $10-million fraud ring. Investigators from the York Regional Police, the Canada Border Services Agency and the Ontario Ministry of Transportation say the fraud ring was involved in money laundering, forging documents along with banking and passport fraud. Ottawa Citizen, A8 (Edmonton Journal, The Province, Windsor Star)

*** Hot on the trail of suspected drug dealer**
A column by Barb Pacholik states, "...They stare out from vehicles on a route to an abandoned farmyard in southwest Saskatchewan, near the U.S. border... South of the border, a courier and his 30-kilogram cargo of white bricks tightly wrapped in paper and plastic are also waiting for that van. A team of officers blending into a night lit by a sliver of moon also anxiously await that meeting. The desolate fields along the Saskatchewan-Montana border have been chosen deliberately by those who prefer to conduct their business away from prying eyes..." The StarPhoenix, A6 (Leader-Post)

*** Crown drops porn charges**
A 26-year-old Kingston area man, currently fighting extradition to the U.S. on child pornography charges, has had his Canadian charges dropped on similar allegations. Crown attorney Ross Drummond disclosed in Kingston's Ontario Court of Justice Tuesday that he was withdrawing all charges against Brandon W. Lane. Lane still faces charges in the U.S., however, where he's accused of engaging in a child exploitation enterprise, conspiracy to advertise the distribution of

child pornography, and conspiracy to distribute child pornography. Lane and another Canadian, Paul Graham Fry, were both indicted south of the border, in absentia, in March. Kingston Whig Standard, 1

*** Cellphones pack real punch**
A sharp-eyed Canadian border guard in Vancouver helped keep hundreds of bizarre -- and potentially lethal--weapons from reaching the streets of Toronto. Toronto Police Wednesday unveiled more than 200 illegal weapons seized from a Danforth Ave.-Dawes Rd. area apartment last Thursday. Toronto Sun, 9; Toronto Star; The Record

*** Airport security has work cut out for them**
Federal screening officers seized 958 knives from outbound passengers at the Hamilton airport between January 2010 and the end of August, according to statistics obtained by The Spectator under a Freedom of Information request. Hamilton Spectator, A3

*** Deported man paid $4,000 to sneak back in**
It took a few hours riding in a car and a short muddy walk that ended with $4,000 in cash passed to a pair of alien smugglers, but those were the only obstacles Shaid Uddin faced in getting into Canada despite a previous deportation. Mr. Uddin's cross-border jaunt, revealed during his immigration fight in the Federal Court of Canada, highlights the porous nature of Canada's long, unsecured border with the United States and the easy success of a thriving illegal alien smuggling business. National Post, A6

*** Une sikhe renvoyée en Inde craint d'être violée**
Manjit Kaur vit au Canada depuis cinq ans. Elle a demandé l'asile politique, mais ne l'a pas obtenu. Son mari, sikh lui aussi, expulsé au mois de mai, a été victime de torture depuis son retour dans son pays natal. Malgré les craintes de la femme, son expulsion vers l'Inde a été maintenue hier soir. La Presse, A18

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

*** Le sénateur Boisvenu rabroue Fournier - «Il a eu un discours pour défendre les jeunes criminels. C'est ça, son discours.[...] Je pense que le Québec est soft on crime.»**
Le ministre québécois de la Justice, Jean-Marc Fournier, ne se fait pas d'amis à Ottawa en critiquant le projet de loi conservateur en matière de justice criminelle. Le sénateur Pierre-Hugues Boisvenu l'accuse d'être mal informé à propos de C-10. Pire, il estime que le Québec n'est pas le paradis de la réhabilitation que présente le ministre, mais plutôt une province «soft on crime». Le Devoir, A1, Le Soleil, Chronicle Herald, La Tribune, Le Droit, La Presse

*** Convictions, but no law**
Lawyers and women's rights supporters say they're upset that hookers arrested in a recent sweep are being convicted even though Canada's prostitution laws sit in limbo before the courts."The laws are unconstitutional," insisted Terry Soukup, assistant director of the Barrie Elizabeth Fry Society. "We should not be dictating how women choose to work and feed themselves or their children." Soukup said all cases should be put on hold until the validity of prostitution laws are argued in the Ontario Court of Appeal. Toronto Sun, 3

*** 'Dead' laws clog Criminal Code**
A column states, "...Parliament's duty is to create new criminal law where needed. But Parliament has a corresponding duty to subtract law ---- to repeal outdated and unenforceable criminal laws. It's failing, miserably, in that duty. The Criminal Code has no introduction or preface. It contains no statement of guiding principles or policy. It nowhere says what our criminal law stands for, or is supposed to achieve for society. It's pretty much just a catalogue of forbidden acts the state has determined to be wrong and deserving of punishment. It's also a catalogue full of stuff that shouldn't be there. There are offences in the code no one's been charged with, or successfully prosecuted for, in decades, because they're anachronistic, inappropriate or illegal. Witchcraft, blasphemy and defamation are among the big ones..." Winnipeg Free Press, A14

*** P.E.I. double murderer denied full parole**
A two-time convicted killer with a fetish for victims' panties has been denied release from a Kingston prison after the parole board noted Ernest DesRoches, 65, has refused sex offender treatment behind bars for 37 years. DesRoches, serving two life sentences for the 1974 killings of two neighbours, and paralyzing a third in rural Prince Edward Island, waived his parole hearing last month. The parole board later reviewed his prison file in his absence and denied him full parole. Guardian, A5

*** Nonobstant**

Une lettre déclare «"Si mon frère avait été jugé en vertu du projet de loi C-10, il serait en prison, aujourd'hui. Au lieu de ça, il est marié, père de trois enfants, a un bon emploi et mène une vie tout à fait exemplaire." Il n'y aurait eu que ce cas, cité par ma voisine, que la démarche entreprise par le ministre de la Justice du Québec pour faire amender le projet de loi C-10 en vaudrait la peine. Pourtant, des cas semblables, on pourrait en citer des centaines, tous des jeunes qui sont retombés sur leurs pieds à la suite d'une bêtise de jeunesse, grâce à notre système de réhabilitation et qui seraient devenus des criminels en fréquentant les bancs de la prison plutôt que ceux de l'école... » Le Devoir, A8

*** Un fils manifeste contre son père**
Éric Chenel poursuit son offensive afin d'empêcher que son père, Jean-Claude Chenel, un ex-résidant de La Rédemption et de Mont-Joli, au Bas-Saint-Laurent, puisse sortir légalement de prison le 22 novembre. Une manifestation aura lieu dimanche de 11h à 16h30, devant l'Institut Louis-Philippe-Pinel, à Montréal. Jean-Claude Chenel avait été condamné en 2008 à la prison pour tentative de meurtre, pour agression sexuelle et pour séquestration. Le Soleil, 30

*** We need to be smart, not tough, on crime**
A letter states, "Mandatory sentences do not work, and result in overcrowded prisons and take money and resources away from crime prevention and rehabilitation. Texas is moving away from this failed fill-the-prisons approach; the Canadian Bar Association, representing 37,000 Canadian legal professionals, has said the bill 'would move Canada along a road that has failed in other countries, at great expense.' We do not need a 'tough on crime bill' what we need is a 'smart on crime bill'." Hamilton Spectator, A14

*** Harper is less popular than pot**
A letter states "Reason #11 to oppose Bill C-10: There are more Canadians who want cannabis legalized than who voted for Stephen Harper. Mandatory penalties for growing cannabis are regressive, cruel and completely unsupported by evidence. These provisions will only further complicate matters for Canadians who use this plant as a medicine." Toronto Star, A22

*** View a violent offender through the eyes of a judge**
An opinion piece states, "Twenty-six-year-old Ray Sharkey is a fairly typical, chronic violent offender. To the federal Conservatives, I have no doubt he is a prime example of why we need mandatory and longer prison terms. Probation and conditional sentencing was a waste of time with this young thug, and perhaps a lengthy stint in the Big House after his first vicious assault would have set him up on the right path. I'm not convinced... I agree the idea that he's going to turn his life around seems a fantasy compared with the very real risk he poses in the community. And whenever Sharkey gets out, he'll simply be older, just as unemployable and probably even more resentful about the life he can't have. He is unquestionably a dangerous man capable of running amok, but at what point do you write him off and toss away the key?..." Vancouver Sun

PUBLIC SERVICE / FONCTION PUBLIQUE

*** Want to save $4 billion? Just call me**
An opinion piece states, "Dear Deloitte, I know how valuable your time is, so I'll get right to the point. As you know, the government has hired your firm to help find $4 billion in annual savings from spending of $258 billion this year. Some people crack wise about how much you're getting paid for this, and $90,000 a day is a lot of money, but if your sharpeyed auditors can find the billions, the $20 million we'll pay you is well worth it, because the politicians are not counting our pennies carefully enough..." Ottawa Citizen, A3 (The StarPhoenix, The Gazette, Leader-Post, Edmonton Journal, Calgary Herald)

*** PS unions fear battle over severance**
The federal unions that vowed never to surrender severance pay without a fight are in contract talks with a government that's made the issue a dealbreaker. Ottawa Citizen, A1

INTERNATIONAL / INTERNATIONAL

*** U.K. says spies foiled Libyan death plots**
British intelligence foiled a plot by Col. Moammar Gadhafi's henchmen to assassinate Western diplomats and Libya's revolutionary leadership, the Foreign Secretary has disclosed. Edmonton Journal, A25; Windsor Star

*** Major drug tunnel uncovered at border**

An estimated 14 tonnes of marijuana were seized after the discovery of a cross-border tunnel that authorities said Wednesday was one of the most significant secret drug smuggling passages ever found on the U.S.-Mexico border. The Record, A11; Le Soleil

*** All is not well for Tamils in Sri Lanka**
An editorial states, "Sri Lanka's High Commissioner Chitranganee Wagiswara tries to justify the war crimes by the government against Tamil civilians by asserting that Tamil Tigers were terrorists. She is by implication accepting that war crimes were committed by both Sri Lanka's army and the Tamil Tigers. But terrorism by a rebel group cannot justify war crimes by Sri Lanka on her civilians..." Toronto Star, A22

OTHER / AUTRE

Death of renowned psychiatrist Menzies leaves 'big hole'
A Saskatoon forensic psychiatrist involved in the cases of Robert Latimer, Karla Homolka and dozens of others across Canada has died. Dr. Robin Menzies, who also conducted landmark studies in post-traumatic stress disorder and other areas, died Wednesday. StarPhoenix, A3

For the Occupiers, an end and a beginning
At Occupy Burlington in Vermont, it happened after a 35-year-old army veteran shot himself in the head. At Occupy Oakland in California, it was after rival gangs clashed, leaving one man dead. Evictions of Occupy Wall Street protests are sweeping away encampments from New York's Zuccotti Park to St. Paul's Cathedral in London, leading some activists to accuse authorities of co-ordinating efforts to throw them out. Officials cite public safety as the motivation, saying the camps have become dangerous and in some cases deadly. The Globe and Mail, A16; * Chronicle Herald, * Times Colonist

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

Williston, Sandra

From: Beaudoin, Luc S
Sent: November-17-11 10:27 AM
To: 'Alain.Labossiere@ic.gc.ca'
Subject: RE: Vtc

Yes. Their potential global support to the Occupy WS, Toronto, etc and threat to cities like Toronto and stock exchange (who were mentioned in seperate Anon ops claims 1 month ago)

L

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: Alain.Labossiere@ic.gc.ca [mailto:Alain.Labossiere@ic.gc.ca]
Sent: November 17, 2011 10:25 AM
To: Beaudoin, Luc S
Subject: Re: Vtc

Anonymous, what exactly you looking for? Toronto?

----- Original Message -----
From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca]
Sent: Thursday, November 17, 2011 10:23 AM
To: Labossière, Alain: DGEPS-DGGPN
Subject: RE: Vtc

Send them my regards. Point to raise:
- CCIRC now (as of Monday) under NCSD (policy shop in charge of National Cyber Strategy)
- BIND DNS: we are looking for more info about the attacks (sources, packets, exploits, impacts, targets etc). We have ISC advisory.
- Anonymous: we are looking for more info...anyone ?

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-17-11 8:16 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary - 2011-11-17

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 17, 2011 / le 17 novembre 2011

Print media

Canadian servers host Syrian government sites
More than a dozen Syrian government websites are being hosted on Canada-based servers, according to a new research report that raises questions about the effectiveness of international sanctions against a regime accused of ongoing crimes against humanity. Globe and Mail, A4

Website snafu strictly 'routine'
"Routine maintenance" -- not Anonymous -- knocked Mayor Rob Ford briefly off the Internet Wednesday. But the Sun has learned Toronto Police are investigating a threat that Anonymous, a group of hacker activists, allegedly made against Ford and the city. Toronto Sun, 5; Toronto Star

Facebook security breach raises vulnerability concerns
A widespread spam attack on Facebook has caused violent and pornographic images to be posted on some users' profile pages, representing one of the worst security breaches in the website's history and raising concerns about its vulnerability to hackers. Daily Gleaner, D6

Malicious virus armies target Android devices
The arsenal of malicious code aimed at Android- powered gadgets has grown exponentially, with criminals hiding viruses in applications people download to devices, according to Juniper Networks. The Province, A23

Online media

As spy business booms, Canada in the crosshairs
Hackers are becoming so sophisticated with their attacks that they are mining Facebook profiles for personal information that could help them steal sensitive data. Security expert Michel Juneau-Katsuya says a Department of National Defence employee told investigators he received an email from someone pretending to be a co-worker who said he had seen the employee at his daughter's soccer game over the weekend. The hacker claimed to have been added to the employee's work team, which was assembling sensitive information, and asked for a copy of the work done so far. Montreal Gazette

Province not disaster ready, auditor says
Critical provincial government information is not sufficiently protected in the event of a disaster like a fire or a major cyber attack, according to auditor general Jacques Lapointe. Metro Halifax

U.S. military better prepared for cyber warfare – General

The U.S. military now has a legal framework to cover offensive operations in cyberspace, the commander of the U.S. Strategic Command said Wednesday, less than a month after terming this a work in progress. Reuters

Cyber warfare not theoretical, can actually kill
Cyber warfare is already a reality and here to stay despite suggestions that such attacks will not lead to fatality, note security insiders, who warn that cyberattacks can actually lead to loss of lives as technology is increasingly integral to daily life. ZDNet Asia

William Hague rings the cyber attack alarm, again
THE UK Foreign Secretary William Hague has for the third time in recent months warned about the threat of cyber attacks from overseas and the UK's readiness to respond effectively. The Inquirer

How can we address the growing botnet issue?
The high-profile takedown of the "DNS Changer" botnet, which had control of more than four million machines and generated $14 million of "income," shows what many in the security industry have known for some time: The botnet problem continues to grow and more coordinated efforts are needed to solve the problem. Government Security News

Research Lab Offers Duqu Detection and Removal Tool
Microsoft is usually pretty good at responding to threats, but it's been a little slow on the draw with the Duqu malware, a.k.a. Son of Stuxnet. Yes, it has offered a work-around to protect against it, but the company has yet to offer adequate protection, detection and removal of the malicious software. Fortunately, a third party has come to the rescue. The Laboratory of Cryptography and System Security (CrySyS), which initially found the Duqu virus, has released a toolkit to detect and remove the virus from affected systems. The Duqu Detector Toolkit v1.01 is open source, with the code fully available for download. Network World

Klassen, Nathan

From: Dincoy, Rana
Sent: November-16-11 11:29 AM
To: Klassen, Nathan
Cc: Cameron, Bud; Pitcher Robert; Bendelier, Kenneth
Subject: RE: News items for the weekly report

Great! Thanks for your help...

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

From: Klassen, Nathan
Sent: November 16, 2011 11:28 AM
To: Dincoy, Rana
Cc: Cameron, Bud; Pitcher Robert; Bendelier, Kenneth
Subject: RE: News items for the weekly report

As requested…

- **Suggested write-up for the highlights section**

Noteworthy Open Source Reports: (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

- **News**

1. **Hackers threaten Toronto over Occupy policy –** The hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict individuals from the Occupy Toronto camp. Calgary Herald;

   - **Analysis:** Anonymous is a group of loosely affiliated – socially conscious – hackers that have in the past successfully carried out threats. They last targeted Canada in an operation called 'tarrmageddon' (i.e. targeting oilsand companies in Alberta). If the city of Toronto's internet service is severely affected this could have finical, social, and security impacts for the city. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat – they are taking precautionary measures.

2. **Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world –** A new survey by the Anti-Phishing Working Group (APWG) reveals that cyber attacks against Chinese e-commerce and banking sites soared by 44% in the first half of 2011. The survey also reveals that close to 70% of all maliciously

registered domain names in the world were established by Chinese cyber criminals – for use against Chinese enterprises."Reference: http://net-security.org/secworld.php?id=11921; and

- **Analysis:** The APWG is a very credible group, and as such, this survey revealed some interesting information. The biggest surprise is the number of maliciously registered domain names Chinese cyber criminals have established for use against Chinese brands and enterprises.

3. **The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker** – DARPA funded researchers are building a program for "generating and distributing believable misinformation." Their ultimate goal is to plant, auto-generated, false documents in classified networks and program them to track down intruders' movements. The program aims to both: (1) scare off individuals browsing WikiLeaks; and (2) minimize insider threats (one of the greatest vulnerabilities in military networks). Reference: http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/

- **Analysis:** Basically the US government is creating products capable of tracking individuals, and as such, there may be legal / privacy implications.

Klassen, Nathan

From: Dincoy, Rana
Sent: November-16-11 11:12 AM
To: Klassen, Nathan
Cc: Cameron, Bud; Pitcher Robert; Bendelier, Kenneth
Subject: RE: News items for the weekly report

Hi Nate,

thanks for this. Communications has advised us that for copyright infringement reasons, we should paraphrase news items in any external facing written product. Would you mind doing that for these news items, and make item 3 more succinct and "executive friendly" language?

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

From: Klassen, Nathan
Sent: November 16, 2011 11:09 AM
To: Dincoy, Rana
Cc: Cameron, Bud; Pitcher Robert; Bendelier, Kenneth
Subject: News items for the weekly report

Hi Rana,

As requested, here are the news items the editorial board decided on for the weekly report. I have written: (1) the highlight section; and (2) analysis for each news item. Let me know if you have any questions, comments, or concerns.
Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

- **Suggested write-up for the highlights section**

Noteworthy Open Source Reports: (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

- **News**

1. **Hackers threaten Toronto over Occupy policy –** The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group. Calgary Herald;

   - **Analysis:** Anonymous is a group of loosely affiliated – socially conscious – hackers that have in the past successfully carried out threats. They last targeted Canada in an operation called 'tarrmageddon' (i.e. targeting oilsand companies in Alberta). If the city of Toronto's internet is severely affected this could have finical, social, and security impacts for the city. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat – they are taking precautionary measures.

2. **Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world –** "A new survey by the Anti-Phishing Working Group (APWG) reveals that phishing attacks perpetrated against Chinese e-commerce and banking sites soared by 44 percent in the first half of 2011. Some 70 percent of all maliciously registered domain names in the world were established by Chinese cybercriminals for use against Chinese brands and enterprises."Reference: http://net-security.org/secworld.php?id=11921;

   - **Analysis:** The APWG is a very credible group, and as such, this survey revealed some interesting information. The biggest surprise is the amount of maliciously registered domain names Chinese cyber criminals have established for use against Chinese brands and enterprises.

3. **The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker:** "WikiLeakers may have to think twice before clicking on that "classified" document. It could be the digital smoking gun that points back at them. Darpa-funded researchers are building a program for "generating and distributing believable misinformation." The ultimate goal is to plant auto-generated, bogus documents in classified networks and program them to track down intruders' movements, a military research abstract reveals."We want to flood adversaries with information that's bogus, but looks real," says Salvatore Stolfo, the Columbia University computer science professor leading the project. "This will confound and misdirect them." (You can make your own fake doc on the research lab's website, too.)The program aims to scare off uninvited riff-raff as well as minimize insider threats, one of the greatest vulnerabilities in military networks. Fake "classified" documents, when touched, will take a snapshot of the IP address of the intruder and the time it was opened, alerting a systems administrator of the breach."Reference: http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/;

   - **Analysis:** Basically the US government is creating products capable of tracking individuals, and as such, there may be legal / privacy implications.

Klassen, Nathan

From: Cameron, Bud
Sent: November-16-11 11:11 AM
To: Klassen, Nathan; Dincoy, Rana
Cc: Pitcher Robert; Bendelier, Kenneth
Subject: RE: News items for the weekly report

Looks great Nate. Under 2, replace the word "amount" by "number".

From: Klassen, Nathan
Sent: November 16, 2011 11:09 AM
To: Dincoy, Rana
Cc: Cameron, Bud; Pitcher Robert; Bendelier, Kenneth
Subject: News items for the weekly report

Hi Rana,

As requested, here are the news items the editorial board decided on for the weekly report. I have written: (1) the highlight section; and (2) analysis for each news item. Let me know if you have any questions, comments, or concerns. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

- **Suggested write-up for the highlights section**

Noteworthy Open Source Reports: (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

- **News**

1. **Hackers threaten Toronto over Occupy policy –** The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group. Calgary Herald;

   - **Analysis:** Anonymous is a group of loosely affiliated – socially conscious – hackers that have in the past successfully carried out threats. They last targeted Canada in an operation called 'tarrmageddon' (i.e. targeting oilsand companies in Alberta). If the city of Toronto's internet is severely affected this could have finical, social, and security impacts for the city. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat – they are taking precautionary measures.

2. **Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world** – "A new survey by the Anti-Phishing Working Group (APWG) reveals that phishing attacks perpetrated against Chinese e-commerce and banking sites soared by 44 percent in the first half of 2011. Some 70 percent of all maliciously registered domain names in the world were established by Chinese cybercriminals for use against Chinese brands and enterprises."Reference: http://net-security.org/secworld.php?id=11921;

- **Analysis:** The APWG is a very credible group, and as such, this survey revealed some interesting information. The biggest surprise is the amount of maliciously registered domain names Chinese cyber criminals have established for use against Chinese brands and enterprises.

3. **The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker:** "WikiLeakers may have to think twice before clicking on that "classified" document. It could be the digital smoking gun that points back at them. Darpa-funded researchers are building a program for "generating and distributing believable misinformation." The ultimate goal is to plant auto-generated, bogus documents in classified networks and program them to track down intruders' movements, a military research abstract reveals."We want to flood adversaries with information that's bogus, but looks real," says Salvatore Stolfo, the Columbia University computer science professor leading the project. "This will confound and misdirect them." (You can make your own fake doc on the research lab's website, too.)The program aims to scare off uninvited riff-raff as well as minimize insider threats, one of the greatest vulnerabilities in military networks. Fake "classified" documents, when touched, will take a snapshot of the IP address of the intruder and the time it was opened, alerting a systems administrator of the breach."Reference: http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/;

- **Analysis:** Basically the US government is creating products capable of tracking individuals, and as such, there may be legal / privacy implications.

Klassen, Nathan

From: Klassen, Nathan
Sent: November-16-11 11:09 AM
To: Dincoy, Rana
Cc: Cameron, Bud; Pitcher Robert; Bendelier, Kenneth
Subject: News items for the weekly report

Hi Rana,

As requested, here are the news items the editorial board decided on for the weekly report. I have written: (1) the highlight section; and (2) analysis for each news item. Let me know if you have any questions, comments, or concerns.
Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

➢ Suggested write-up for the highlights section

Noteworthy Open Source Reports: (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

➢ News

1. **Hackers threaten Toronto over Occupy policy –** The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group. Calgary Herald;

   - **Analysis:** Anonymous is a group of loosely affiliated – socially conscious – hackers that have in the past successfully carried out threats. They last targeted Canada in an operation called 'tarrmageddon' (i.e. targeting oilsand companies in Alberta). If the city of Toronto's internet is severely affected this could have finical, social, and security impacts for the city. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat – they are taking precautionary measures.

2. **Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world –** "A new survey by the Anti-Phishing Working Group (APWG) reveals that phishing attacks perpetrated against Chinese e-commerce and banking sites soared by 44 percent in the first half of 2011. Some 70 percent of all maliciously registered domain names in the world were established by Chinese cybercriminals for use against Chinese brands and enterprises."Reference: http://net-security.org/secworld.php?id=11921;

   - **Analysis:** The APWG is a very credible group, and as such, this survey revealed some interesting information. The biggest surprise is the amount of maliciously registered domain names Chinese cyber criminals have established for use against Chinese brands and enterprises.

3. **The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker:** "WikiLeakers may have to think twice before clicking on that "classified" document. It could be the digital smoking gun that points back at them. Darpa-funded researchers are building a program for "generating and distributing believable misinformation." The ultimate goal is to plant auto-generated, bogus documents in classified

networks and program them to track down intruders' movements, a military research abstract reveals."We want to flood adversaries with information that's bogus, but looks real," says Salvatore Stolfo, the Columbia University computer science professor leading the project. "This will confound and misdirect them." (You can make your own fake doc on the research lab's website, too.)The program aims to scare off uninvited riff-raff as well as minimize insider threats, one of the greatest vulnerabilities in military networks. Fake "classified" documents, when touched, will take a snapshot of the IP address of the intruder and the time it was opened, alerting a systems administrator of the breach."Reference: http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/;

- **Analysis:** Basically the US government is creating products capable of tracking individuals, and as such, there may be legal / privacy implications.

Klassen, Nathan

From: Klassen, Nathan
Sent: November-16-11 11:28 AM
To: Dincoy, Rana
Cc: Cameron, Bud; Pitcher Robert; Bendelier, Kenneth
Subject: RE: News items for the weekly report

As requested…

- **Suggested write-up for the highlights section**

Noteworthy Open Source Reports: (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

- **News**

1. **Hackers threaten Toronto over Occupy policy –** The hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict individuals from the Occupy Toronto camp. Calgary Herald;

   - **Analysis:** Anonymous is a group of loosely affiliated – socially conscious – hackers that have in the past successfully carried out threats. They last targeted Canada in an operation called 'tarrmageddon' (i.e. targeting oilsand companies in Alberta). If the city of Toronto's internet service is severely affected this could have finical, social, and security impacts for the city. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat – they are taking precautionary measures.

2. **Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world** – A new survey by the Anti-Phishing Working Group (APWG) reveals that cyber attacks against Chinese e-commerce and banking sites soared by 44% in the first half of 2011. The survey also reveals that close to 70% of all maliciously registered domain names in the world were established by Chinese cyber criminals – for use against Chinese enterprises."Reference: http://net-security.org/secworld.php?id=11921; and

   - **Analysis:** The APWG is a very credible group, and as such, this survey revealed some interesting information. The biggest surprise is the number of maliciously registered domain names Chinese cyber criminals have established for use against Chinese brands and enterprises.

3. **The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker** – DARPA funded researchers are building a program for "generating and distributing believable misinformation." Their ultimate goal is to plant, auto-generated, false documents in classified networks and program them to track down intruders' movements. The program aims to both: (1) scare off individuals browsing WikiLeaks; and (2) minimize insider threats (one of the greatest vulnerabilities in military networks). Reference: http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/

   - **Analysis:** Basically the US government is creating products capable of tracking individuals, and as such, there may be legal / privacy implications.

Klassen, Nathan

From: Klassen, Nathan
Sent: November-16-11 10:35 AM
To: Beaudoin, Luc S
Subject: for the weekly report -- can you read my analysis on BB -- are you okay with it

Hey Luc,

Can you read this on BB and let me know if my analysis is correct? Cheers,

Nate

1. **Hackers threaten Toronto over Occupy policy –** The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group. Calgary Herald;

   - Analysis: Anonymous is a group of loosely affiliated – socially conscious – hackers that have in the past successfully carried out threats. They last targeted Canada in an operation called 'tarrmageddon' (i.e. targeting oilsand companies in Alberta). If Anonymous carries through with their threat Toronto's city services could be severely impacted. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat and they are taking precautionary measures.

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Beaudoin, Luc S
Sent: November 16, 2011 9:19 AM
To: Klassen, Nathan
Cc: Turbide, Frank
Subject: FW: Request of delegated authority for release

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: Beaudoin, Luc S
Sent: November 15, 2011 1:54 PM
To: Anderson, Windy

Cc: Cameron, Bud
Subject: Request of delegated authority for release

CCIRC is requesting delegation of Release Authority to the Director of CCIRC or delegate (Operations Manager / Strategic manager / Technical Manager) for the following products :

- Daily Report: Internal to PS + CTU partners
- Weekly Technical Report: Fed, Prov, Muni, Fin, Telecom, Energy
- Cyber Flash: All contacts, non-public
- Information Note: All CI contacts, often public (www)
- Advisory: all CI contacts, generally public (www)
- Alert: all CI contacts, generally public (www)
- Technical Report: all CI contacts, sometimes public (www)
- Take Down request: 1-on-1, in Canada only, RCMP cc'd
- Notification of victim: 1-on-1, mostly in Canada, through other CERTs for international

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-16-11 8:55 AM
To: * Media Monitoring / Suivi des médias; * NCSD / DGCN; * [redacted]; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique - 2011-11-16

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 16, 2011 / le 16 novembre 2011

Print media

That Facebook 'friend' could be a spy
Hackers are becoming so targeted with their attacks that they are mining Facebook profiles for personal information that could help them steal sensitive data. Security expert Michel Juneau-Katsuya says a Department of National Defence employee told investigators he received an email from someone pretending to be a co-worker who said he had seen the employee at his daughter's soccer game over the weekend. The hacker claimed to have been added to the employee's work team, which was assembling sensitive information, and asked for a copy of the work done so far. The personal information came from pictures the DND staffer had posted to Face-book. The staffer alerted department officials. Juneau-Katsuya says international espionage is reaching record levels as governments move away from costly military confrontations in favour of electronic attacks and computer data theft - and they are picking on average people to get what they want. Speaking at the release of the 2011 Telus-Rotman IT Security Study, Juneau-Katsuya said more than 10 times more spy activity goes on today than at the peak of the Cold War. Ottawa Citizen, A1 (Edmonton Journal, Calgary Herald, Windsor Star)

Canadian businesses unprepared for hackers
Canadian businesses are increasingly being victimized by hackers but are also less prepared for such Internet threats, new reports have found. Breaches of Canadian publicly traded companies jumped an "alarming" 50% in 2011, says a joint study released Tuesday by Telus Corp. and the University of Toronto's Rotman School of Management. The annual study said public companies in Canada were hacked an average of 18 times this year, compared with an average of 12 attacks suffered in 2010. Overall, the study says, attacks on businesses and government offices were down nearly 50% from last year, to an average of 7.6 breaches in 2011 from 14.6 in 2010. Insider breaches, in which hackers turned out to be employees, were extremely prevalent in government - the "most startling" result of the survey, researchers said - accounting for 42% of every government computer hacked in 2011. National Post, FP4 (Times Colonist, The Province, Calgary Herald, Montreal Gazette)

Report warns of security chaos in power grid
The cyber-security of the North American power grid is "in a state of near chaos," according to report by a respected U.S. energy consultancy monitoring the industry's transition to wireless digital technologies. The white paper by Pike Research reveals that a $60 smart phone application can bypass security measures and allow direct communications between the phone and some control systems (ICS) that regulate breakers, relays, feeders and the flow of electricity. The news comes on the heels of a warning from the cyber-security arm of the U.S. Department of Homeland Security that the hacker collective known as Anonymous appears intent on exploiting the ICS vulnerabilities within the energy industry. Ottawa Citizen, A4 (Edmonton Journal, Windsor Star)

U.S. not afraid of using force against cyber attacks
The United States reserves the right to retaliate with military force against a cyberattack and is working to sharpen its ability to track down the source of any attack, the Pentagon said in a report made public on Tuesday. The 12-page report to Congress, which was mandated by the 2011 Defense Authorization Act, was one of the clearest statements to date of U.S. cybersecurity policy and the role of the military in the event of an attack on U.S. assets through cyberspace. The report said the Defence Department was attempting to deter aggression in cyberspace by developing effective defences that prevent adversaries from achieving their objectives and by finding ways to make attackers pay a price for their actions. Windsor Star, C11

Social media bans may help hackers
If your company's computer network is being hacked more than usual, your policy on social networks may be to blame. A report in IT security issued jointly by Telus and the Rotman School of Management surveyed 649 firms and found companies that ban employees from using social media suffer 30 per cent more computer security breaches than ones that allow free use of sites like Facebook and Twitter. Toronto Star, B3

Android security threats surging
Google's Android operating system for mobile devices has had an almost sixfold increase in threats such as spyware and viruses since July, according to Juniper Networks. That may increase the perception that Apple devices are safer than smartphones and tablets that run on Android, said Juniper. Making malware is easier with Android software because the applications aren't checked, the source code is open and the apps can be sold on external sites, Hoffman said. Android is free and available for download by anyone, while Apple screens each application added to its store. Toronto Star, B3

Facebook blames flood of porn on 'co-ordinated' attack
Facebook said Tuesday that a "co-ordinated spam attack" was responsible for graphic images appearing in the news feeds of some members of the world's largest social network. Facebook, which has more than 800 million members, said some users of the social network were tricked into unknowingly sharing the offensive content. It's likely that the affected users have unwittingly downloaded a piece of malware onto their personal computers, Graham Cluley, senior technology consultant at security firm Sophos Ltd said. Ottawa Citizen, A11; StarPhoenix; Calgary Herald

Online media

Australian websites caught up in DNS Changer case
Thousands of computers in Australia may have been affected by the largest botnet, dubbed domain name system (DNS) Changer, according to evidence from Trend Micro. A group in Estonia was investigated by the Federal Bureau of Investigation (FBI) and found to be responsible for the malware which hijacked users' clicks. It then redirected to hacker-created sites that resembled the real domains. Trend Micro Australia software architecture director, Jon Oliver, said the company had been tracking DNS Changer since 2006 when it started identifying strange behaviour in command and control servers doing "DNS tricks." CIO

Duqu Gang Working on Trojan for Years: Kaspersky
Security researchers find that some Duqu Trojan components date back to 2007 and Iran may have seen an early variant months ago, but didn't share the information with the global security research community. The team behind the Duqu Trojan may have been working on the Trojan for at least four years, according to the latest analysis of the sophisticated malware. Kaspersky Lab researchers have identified the overall methods used by the authors of the Duqu Trojan and an approximate timeline of the attack, Alexander Gostev, chief security expert at Kaspersky Lab, wrote on the Securelist blog. The analysis was based on samples provided by the Computer Emergency Response Team - Sudan that were used in at least three attacks against unidentified targets in the country. eWeek

Bitdefender finds Anonymous threat to attack Facebook
Bitdefender, an award-winning provider of innovative Internet security solutions, has found a recent video post by the hacktivist group, Anonymous Central, saying it intends to attack Facebook accounts with a 'highly sophisticated' piece of malware, codenamed Fawkes Virus. Allegedly, the malware – which was 'fully written' by Anonymous' programmers – has already been tested. According to the message, the Fawkes Virus consists of "a highly sophisticated worm, with advanced network self-replication and remote abilities. It sends out malicious links and gains access of your account." PR Wire

Stolen Malaysian key used to sign malicious software
A malicious program that uses a signing key has been detected. According to F-Secure, a malicious program has been using a digital certificate that was stolen from the Malaysian government. This certificate has been used to legitimise software when users download it from the web, helping it to remain undetected. Mikko Hypponen, chief research officer at F-Secure, claimed it is not that common to find a signed copy of malware, but it is even rarer that it is signed with an

official government key. F-Secure detected that the 'mardi.gov.uk' signing key was found to belong to the Malaysian Agricultural Research and Development Institute, and its investigations suggest that it was stolen quite some time ago. SC Magazine U.K.

FBI Accusing Group of Criminals Involved in Click-Fraud

According to FBI (Federal Bureau of Investigation), it along with its global associates has accused 6 persons of carrying out one advanced campaign of click-fraud, which yielded them USD counting a few millions, published Eweek.com dated November 9, 2011. Approximately 4m PCs from 100 countries contracted infection due to the six-member cyber-ring's activity involving malware, which enabled it to pocket around $14m via manipulation of Internet ads, the agency stated. On November 8, 2011, cops detained 6 nationals from Estonia. One more from Russia is still operating, believes FBI. SPAM Fighter

Internet Companies and Lawmakers Speak Out Against the Stop Online Piracy Act

If freedom of expression, privacy and innovation online matter to you, it's time to pay attention to what's happening in Congress right now. There's a gathering storm over bills proposed in the United States House of Representatives and Senate that have the potential to significantly hinder innovation, free speech and cybersecurity on the Internet in the name of fighting online piracy. SOPA is "really a Trojan horse that might be better named the Social Media Surveillance Act," said Leslie Harris, CEO of CDT, in a press conference today. "Expect it to have a devastating effect on social media content and expression." That the proposed bill has advanced with significant bipartisan support, along with PROTECT IP Act in the Senate, shows that online innovation and freedom of expression still need strong defenders against 20th century institutions whose quest for copyright protection would leave collateral damage in the form of human right defenders and entrepreneurs. Huffington Post

Ambulance System Disabled by Malware

A malware infection recently disabled the communications network for New Zealand's St. John Ambulance service, forcing dispatchers to use manual backup systems. eSecurity Planet

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-15-11 8:28 AM
To: * DGOPS-CCIRC; * Media Monitoring / Suivi des médias; * NCSD / DGCN; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; [redacted] De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; [redacted] Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; [redacted] Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique - 2011-11-15

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 15, 2011 / le 15 novembre 2011

Print media

Toronto taking hacker collective's threat of cyber-attack seriously
The city of Toronto says it is taking seriously a threat by the hacker collective Anonymous to interfere with the city's website if officials move on Occupy Toronto. Toronto's branch of the worldwide occupation movement is based in St. James Park, where a small tent city sprung up last month. Occupiers are attempting to raise awareness about the gulf between the rich and the poor, but their campsite has drawn criticism from area residents and Mayor Rob Ford, who has suggested it is time for the group to "move on." On the weekend, Anonymous, an amorphous collective of hackers, threatened to have the city "removed from the Internet" if it follows through on plans to evict campers. Montreal Gazette, A8; Edmonton Sun

Unmasking Anonymous
In this occasional feature, the National Post tells you everything you need to know about a complicated issue. Today, Megan O'Toole examines a threat, purportedly from the hacker collective known as Anonymous, to derail the city's website if officials move in on Occupy Toronto protesters… National Post, A9

New 'supervirus' hits Iran's computers
Iran says its defence computer systems have been infected with a "supervirus" similar to one believed to have been created by Israel which severely damaged Tehran's nuclear program last year. Anti-virus experts have identified a virus called Duqu that they said shared properties with the Stuxnet worm apparently created by Mossad, the Israeli security service. It was thought to have targeted the nuclear program's centrifuges, the devices that enrich uranium to create nuclear fuel. It was not clear from the Iranian statement whether Duqu had also struck nuclear facilities, but it was the regime's first admission of damage. Windsor Star, D2

Online media

Toronto 'won't negotiate with cyber-terrorists'
Toronto councillor Paul Ainslie says he doesn't "negotiate with cyber-terrorists." The chairman of the city's government management committee said Monday he's not worried by threats against the city and Mayor Rob Ford from the hacking group Anonymous. A group claiming to be Anonymous posted a video on YouTube Saturday, stating it would "remove" Ford and the city from the Internet if the city moved to evict the 500-or-so Occupy Toronto demonstrators who have camped out in St. James Park for the last month. Ainslie's committee oversees the city's IT systems but he says he's not losing sleep over the threat. Sun News Network

FAQ: What's the big deal about Duqu?
The recently discovered Duqu Trojan has received considerable attention from the security research community. Here's why. What is Duqu? It's a Remote Access Trojan (RAT) that is designed to steal data from computers it infects. It was discovered by the Laboratory of Cryptography and Systems Security (CrySys) at Budapest University. RATs are pretty common these days. Why is so much attention to Duqu? Duqu is believed to have been created by the same people who wrote Stuxnet, the worm that was used to disrupt operations at Iran's Natanz nuclear facility last year. A lot of security analysts believe that it is a precursor to the next Stuxnet and poses a grave threat to the industrial control systems that manage equipment at critical infrastructure facilities such as power plants and water treatment facilities. Computer World

Duqu Detector Toolkit Released by CrySys
Security research lab The Laboratory of Cryptography and System Security (CrySyS), which was responsible for discovering the Duqu virus, has dished out a toolkit that would help detecting and eradicating the virus from affected systems. The Duqu Detector Toolkit v1.01, which is available for download from the CrySys website, is an open source tool that helps detect the virus, which is based on the Stuxnet virus source code. While Stuxnet was designed to take on industrial control systems in nuclear power plants, Duqu has been designed to gather information that would help in conducting cyber attacks in the future. IT Pro Portal

Iran Claims To Have Contained 'Duqu' Computer Virus
Iran claimed Monday that it has contained the so-called espionage malware Duqu that had infected some computer systems linked to the Islamic Republic's controversial nuclear program. RTT News

Employees' Droids among biggest government cyber menaces
In 2012, agencies should worry about hackers attacking the growing number of federal employees toting their own iPhones and Droids to work, according to a forecast of next year's greatest cyber dangers compiled by M86 Security Labs. On Tuesday, the network security firm is expected to release its annual predictions of the top computer threats to business and government organizations. At federal agencies, the biggest targets are likely to be employee-owned devices, a department's own public website and cloud services. Nextgov

Mobile malware and targeted attacks to proliferate in 2012
Mobile malware and targeted attacks are among the biggest problems facing end users and administrators in the coming year, according to the latest Threat Predictions report from M86 Security. The company said that attacks on social networking services will combine with targeted operations and mobile threats to represent the top security risks in the next 12 months. V3

F-Secure spots malware signed with real code certificate
Researchers from security vendor F-Secure have spotted a rare malicious software sample that carried a valid secure code signing certificate from a Malaysian governmental institution. A code signing certificate is a kind of digital signature that ensures the authenticity and integrity of an application to be run on a computer. Malicious software programs often present fake digital signatures, but ones that are legitimate and attached to malware are rare, said Mikko Hypponen, chief research officer for F-Secure. The certificate was signed by "anjungnet.mardi.gov.my," which is part of Malaysia's Agricultural Research and Development Institute. Hypponen said F-Secure contacted the organisation, which then found that a Windows server responsible for generating the certificates had been hacked. Techworld; SC Magazine

Whistler Bootkit Improves, Bypasses Anti-Virus Detection
According to Mircea Pavel, researcher at security company BitDefender, new malicious software, Rootkit.MBR.Whistler.B was recently contaminating plentiful of the Whistler bootkit records an MBR (master bootkit record), published Softpedia on November 9, 2011. Following a computer disk's final segmentation, the entire data of Whistler stays with the malware. And suppose the un-segmented space isn't sufficient the bootkit will make the final segmentation smaller, ensuring that a minimum of 400 free sectors is created. SPAM Fighter

40,000+ email addresses and passwords discovered on phishing site
You know those spam emails that ask you to provide your username/password credentials for your bank, email, Facebook, or otherwise? Well, one user on Reddit decided to take a closer look at the Web site of a link included within one of those emails, and what they ultimately found was a text file filled with ~47,000 email addresses and passwords belonging to Hotmail and MSN users. Though it's unclear as to if these were successfully-phished email addresses or email addresses being used solely to send out phishing emails, the individual on Reddit wrote a script in Python to test the validity of the addresses and found that ~85% out of ~2000 were accessible via the passwords accompanying them. ZDNet

Trojan Surrounding Controversy in Germany Top Malware

Kaspersky the security company has just published its October 2011 malware statistics within its new malware report for the month, which suggests that a prominent incident of the October month related to a controversy, which surfaced in Germany after a backdoor Trojan was discovered that cops in the country utilized for intercepting messages as well as voice traffic, suspicious computers generated. The outcry occurred not just due to 5 federal states, which substantiated that the PC-Trojan was used, however, as well due to the federal laws of the country that solely permitted agencies of law enforcement for tapping suspects' voice traffic generated through Skype whereas the malicious program spied on several more applications. Cops loaded the PC-Trojan around which the controversy occurred, onto the computer of a suspect while conducting a scrutiny at Munich airport, it is disclosed in Kaspersky's latest report. SPAM Fighter

Cyberwar: the offensive on citizens' rights

Cyberwar cynic Marcus Ranum, chief security officer of Tenable Security, reckons the notion of cyberwar is really a war on citizens' rights. While Stuxnet, aimed at Iran's nuclear equipment, has been taken to signal the entry of cyberwar into military doctrine, that particular example would be better described as "state sponsored terrorism", according to Ranum. The notion of cyberwar flared up in May after a classified version of a Pentagon cyber strategy paper that reportedly concluded that the Laws of Armed Conflict also applied in cyberspace. Australia's Chief of the Defence Force David Hurley recently expressed reservations about cyber "war" because of problems attributing the attack to a source. CSO

Disaster recovery plans 'should be in place to handle power outages'

Businesses have been advised to prepare their data recovery strategies so that problems can be kept to a minimum as a result of a power failure. Writing for Continuity Central, Dr Jim Kennedy, who has 30 years of experience dealing with information and cyber security, believes that every organisation needs to be prepared for a major power cut. This is because issues such as disruption to business and lost revenue can both occur as a result, Dr Kennedy acknowledged. Ontrack Data Recovery

Klassen, Nathan

From: Klassen, Nathan
Sent: November-14-11 4:52 PM
To: Cameron, Bud; Dincoy, Rana; Bendelier, Kenneth; Pitcher Robert
Subject: FW: News items for the weekly report

Hi all,

As per the meeting invite – here are a few ranked news items for discussion tomorrow. Cheers,

Nate

From: Klassen, Nathan
Sent: November 14, 2011 2:44 PM
To: Dincoy, Rana
Cc: Cameron, Bud
Subject: News items for the weekly report

Hi Rana,

As discussed, here are a few news items for the weekly report (I have ranked in order of importance – Nate's opinion☺). I would also recommend only reporting on the top 3-5 as this would save both: (1) analyst time; and (2) document space. Let me know if you have any questions, comments, or concerns. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

- **Suggested write-up for the highlights section**

Noteworthy Open Source Reports: (1) Canada to spend $477M to thwart foreign cyber attacks; (2) Hackers threaten City of Toronto; (3); FBI arrests made in massive internet fraud scheme – Canada affected; (4) US accuses Russia and China of widespread cyber espionage; and (5) 600, 000 facebook users' accounts are compromised every day.

- **News**

1. **Canada to spend $477 M in bid to thwart foreign cyber attacks –** Canada is poised to spend nearly half a billion dollars to gain access to a constellation of U.S. air force satellites designed to foil foreign cyber attacks. Global Mercury, as Canada's $477 million share of the Wideband Global Satcom (WGS) network, is to be known, will be immediately activated when a memorandum of understanding between the Department of National Defence and the U.S. air force is signed within the next few weeks. Edmonton Journal;

2. **Hackers threaten Toronto over Occupy policy –** The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group. Calgary Herald;

3. **FBI arrests six in massive internet fraud scheme**– Charges against Six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that infected more than four million computers located in over 100 countries with malware." Reference: http://www.net-security.org/secworld.php?id=11928;

4. **US accuses China and Russia of widespread cyber espionage** – China and Russia are singled out for their cyber espionage efforts in a report sent to US Congress. The US has accused China and Russia of wide-scale cyber espionage, saying they would continue to steal sensitive American data. There has been a spate of attacks this year in which nation states have been blamed. When Mitsubishi Heavy Industries, one of Japan's military contractors, was hit earlier this year, fingers pointed to Beijing. Last year, Google claimed China was responsible for a hack on the web giant, in attacks that became known as Operation Aurora. PC & Tech Authority;

5. **600,000 Facebook Logins Are Compromised Each Day –** Whether you're on it all the time or not quite as often, your Facebook account runs the constant risk of being compromised. A recent study found that 600,000 Facebook logins are compromised each day. CW33 News;

6. **Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world** – "A new survey by the Anti-Phishing Working Group (APWG) reveals that phishing attacks perpetrated against Chinese e-commerce and banking sites soared by 44 percent in the first half of 2011. Some 70 percent of all maliciously registered domain names in the world were established by Chinese cybercriminals for use against Chinese brands and enterprises."Reference: http://net-security.org/secworld.php?id=11921;

7. **The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker:** "WikiLeakers may have to think twice before clicking on that "classified" document. It could be the digital smoking gun that points back at them. Darpa-funded researchers are building a program for "generating and distributing believable misinformation." The ultimate goal is to plant auto-generated, bogus documents in classified networks and program them to track down intruders' movements, a military research abstract reveals."We want to flood adversaries with information that's bogus, but looks real," says Salvatore Stolfo, the Columbia University computer science professor leading the project. "This will confound and misdirect them." (You can make your own fake doc on the research lab's website, too.)The program aims to scare off uninvited riff-raff as well as minimize insider threats, one of the greatest vulnerabilities in military networks. Fake "classified" documents, when touched, will take a snapshot of the IP address of the intruder and the time it was opened, alerting a systems administrator of the breach."Reference: http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/; and

8. **Duqu is precursor to next Stuxnet - Malware as invasive as Stuxnet created specifically to collate information on industrial targets –** A trojan discovered last month uses the same code as last year's Stuxnet worm, and is thought to have been written by the same authors, according to a report by Symantec. Duqu, however, is different in that it uses a zero-day exploit, thought to be carried out through vulnerability in Word, to collect information on specific targets, rather than control them. Symantec call the malware "the precursor to the next Stuxnet" as it is thought that it is collecting the information in order to carry out a more informed attack on industrial targets. Duqu pretends to be a driver and uses a digital certificate to aid installation (which was revoked on October 14th 2011). It is thought that the keys required to make the certificate work were stolen from a company in Taiwan. Once the malware has been installed, it downloads additional executables to the target machine, mostly infostealers which include keyloggers and software to report on system information. In order to extract the information, the control and command function masks the outgoing information as a jpg in order to appear legitimate. The malicious software runs on an infected machine for thirty days, after which it deactivates itself. However, Symantec have noted that some of the files downloaded to an infected machine instruct the malware to extend its lifetime. TechWatch

Klassen, Nathan

From: Klassen, Nathan
Sent: November-14-11 2:44 PM
To: Dincoy, Rana
Cc: Cameron, Bud
Subject: News items for the weekly report

Hi Rana,

As discussed, here are a few news items for the weekly report (I have ranked in order of importance – Nate's opinion☺). I would also recommend only reporting on the top 3-5 as this would save both: (1) analyst time; and (2) document space. Let me know if you have any questions, comments, or concerns. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

- **Suggested write-up for the highlights section**

Noteworthy Open Source Reports: (1) Canada to spend $477M to thwart foreign cyber attacks; (2) Hackers threaten City of Toronto; (3); FBI arrests made in massive internet fraud scheme – Canada affected; (4) US accuses Russia and China of widespread cyber espionage; and (5) 600, 000 facebook users accounts are compromised every day.

- **News**

1. **Canada to spend $477 M in bid to thwart foreign cyber attacks –** Canada is poised to spend nearly half a billion dollars to gain access to a constellation of U.S. air force satellites designed to foil foreign cyber attacks. Global Mercury, as Canada's $477 million share of the Wideband Global Satcom (WGS) network, is to be known, will be immediately activated when a memorandum of understanding between the Department of National Defence and the U.S. air force is signed within the next few weeks. Edmonton Journal;

2. **Hackers threaten Toronto over Occupy policy –** The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group. Calgary Herald;

3. **FBI arrests six in massive internet fraud scheme**– Charges against Six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that infected more than four million computers located in over 100 countries with malware." Reference: http://www.net-security.org/secworld.php?id=11928;

4. **US accuses China and Russia of widespread cyber espionage –** China and Russia are singled out for their cyber espionage efforts in a report sent to US Congress. The US has accused China and Russia of wide-scale cyber espionage, saying they would continue to steal sensitive American data. There has been a spate of attacks this year in which nation states have been blamed. When Mitsubishi Heavy Industries, one of Japan's military contractors, was hit earlier this year, fingers pointed to Beijing. Last year, Google claimed China was responsible for a hack on the web giant, in attacks that became known as Operation Aurora. PC & Tech Authority;

5. **600,000 Facebook Logins Are Compromised Each Day –** Whether you're on it all the time or not quite as often, your Facebook account runs the constant risk of being compromised. A recent study found that 600,000 Facebook logins are compromised each day. CW33 News;

6. **Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world –** "A new survey by the Anti-Phishing Working Group (APWG) reveals that phishing attacks perpetrated against Chinese e-commerce and banking sites soared by 44 percent in the first half of 2011. Some 70 percent of all maliciously registered domain names in the world were established by Chinese cybercriminals for use against Chinese brands and enterprises."Reference: http://net-security.org/secworld.php?id=11921;

7. **The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker:** "WikiLeakers may have to think twice before clicking on that "classified" document. It could be the digital smoking gun that points back at them. Darpa-funded researchers are building a program for "generating and distributing believable misinformation." The ultimate goal is to plant auto-generated, bogus documents in classified networks and program them to track down intruders' movements, a military research abstract reveals."We want to flood adversaries with information that's bogus, but looks real," says Salvatore Stolfo, the Columbia University computer science professor leading the project. "This will confound and misdirect them." (You can make your own fake doc on the research lab's website, too.)The program aims to scare off uninvited riff-raff as well as minimize insider threats, one of the greatest vulnerabilities in military networks. Fake "classified" documents, when touched, will take a snapshot of the IP address of the intruder and the time it was opened, alerting a systems administrator of the breach."Reference: http://www.wired.com/dangerroom/2011/11/darpa-trap-wikileaks/; and

8. **Duqu is precursor to next Stuxnet - Malware as invasive as Stuxnet created specifically to collate information on industrial targets –** A trojan discovered last month uses the same code as last year's Stuxnet worm, and is thought to have been written by the same authors, according to a report by Symantec. Duqu, however, is different in that it uses a zero-day exploit, thought to be carried out through vulnerability in Word, to collect information on specific targets, rather than control them. Symantec call the malware "the precursor to the next Stuxnet" as it is thought that it is collecting the information in order to carry out a more informed attack on industrial targets. Duqu pretends to be a driver and uses a digital certificate to aid installation (which was revoked on October 14th 2011). It is thought that the keys required to make the certificate work were stolen from a company in Taiwan. Once the malware has been installed, it downloads additional executables to the target machine, mostly infostealers which include keyloggers and software to report on system information. In order to extract the information, the control and command function masks the outgoing information as a jpg in order to appear legitimate. The malicious software runs on an infected machine for thirty days, after which it deactivates itself. However, Symantec have noted that some of the files downloaded to an infected machine instruct the malware to extend its lifetime. TechWatch

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-14-11 8:25 AM
To: * DGOPS-CCIRC; * Media Monitoring / Suivi des médias; * Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Slade, Nancy; Spendlove, Jim; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique - 2011-11-14

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 14, 2011 / le 14 novembre 2011

Print media

Canada to spend $477 M in bid to thwart foreign cyber attacks
Canada is poised to spend nearly half a billion dollars to gain access to a constellation of U.S. air force satellites designed to foil foreign cyber attacks. Global Mercury, as Canada's $477 million share of the Wideband Global Satcom (WGS) network, is to be known, will be immediately activated when a memorandum of understanding between the Department of National Defence and the U.S. air force is signed within the next few weeks. Edmonton Journal

Hackers threaten Toronto over Occupy policy
The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group. Anonymous has previously stated it would ignore the Occupy Canada movement unless it saw an "interruption" to the protests. Calgary Herald

Cyber threat doesn't faze Ford
Mayor Rob Ford still wants the Occupy Toronto protesters out of St. James Park despite an ultimatum issued via Youtube video by a group claiming to be the Anonymous hacker-activists. "You have said that by next week the occupiers shall be removed. And we say by next week if you do not change your mind, you shall be removed from the Internet," proclaims the video's computer-generated voice, typical of messages from the loosely organized collective of hackers. Toronto Star; Winnipeg Sun

Twitter ruling reveals extent of surveillance
Last Thursday in Alexandria, Va., United States District Court Judge Liam O'Grady ruled that private information on the Twitter accounts of three users related to WikiLeaks must be turned over to the U.S. federal government because the data is hosted on U.S. servers. At the same time, the judge blocked the users' attempt to discover whether other Internet companies have been ordered to turn their data over as well, noting that the trio had no reasonable expectation of privacy when they used Twitter services, even if the information in question was known only to Twitter and not publicly disclosed. Calgary Herald

Online media

Rise of outsourcing poses new cybersecurity problems
Big banks, hospitals and insurance companies worry about computer security because they handle so much personal information. Now, in the age of outsourcing, they also have to worry about whether their partner firms are secure. And

that's created a new kind of business consultant: The information security auditor who determines how much security is enough. Chicago Tribune

U.S. Works to Counter Electronic Spy Risks
The Obama administration is quietly working to counter potential risks posed by foreign telecommunications companies' expansion in the U.S. market, which federal officials say they fear could make the nation vulnerable to spying. The initiative, previously unreported, doesn't target a particular company or country, but China remains a focus of U.S. government concerns about electronic spying. Wall Street Journal

UK Cyber Security Strategy themes revealed
The UK government will urge businesses to form 'uncomfortable partnerships' with competitors as part of the upcoming UK Cyber Security Strategy, ZDNet UK has learned. Businesses must look to forming close working relationships with competitors to share sensitive cybersecurity information, they will be told when the document is published. The UK Cyber Security Strategy is due on 25 November, a Cabinet Office spokesman confirmed on Thursday. ZDNet

Duqu trojan was years in development, say Kaspersky
The hacker group behind Duqu may have been working on its attack code for more than four years, sccording to new analysis of the Trojan. Moscow-based Kaspersky Lab published some findings today from a recent rooting through Duqu samples provided by researchers in the Sudan, saying that one driver included with the attack payload was compiled in August 2007, extending the timeline of the gang's work. Computerworld UK

Duqu authors sprinkle humour in dangerous code
For all of the concern around Duqu, the most discussed piece of malicious software since Stuxnet, the latest analysis of its code shows its writers have a sense of humour. Wrapped in the code used to infect computers is an "Easter egg," or a hidden message. Easter eggs have long been inserted in computer code, often seen only by those who enjoy browsing computer code. Computerworld UK

Duqu Trojan revealed to be shape-shifting serial killer
Security analysts have found more mysterious but fascinating details in the Duqu Trojan, the so-called "son of Stuxnet" discovered just two months ago. Moscow's Kaspersky Lab got hold of a different variant of Duqu than the original, and found that the Trojan's creators not only may have been working on Duqu since 2007, but seem to have a sense of humor as well. MSNBC

Spam Researchers Help Bust Global Cybercrime Ring
When law enforcement authorities took down this week an international ring of Internet grifters who allegedly scammed more than $14 million from their victims, a key element of their crackdown was a spam database maintained by the University of Alabama-Birmingham. PC World

FBI Botnet Bust Hinged On Public-Private Partnership
Policymakers and government officials have used the term "public-private partnerships" as a way to fight online threats so frequently that it has become code for doing nothing. Yet the recently announced Operation Ghost Click shows that such teamwork is necessary to take on cybercriminals and more advanced threats online. Information Week

5 Fast-Spreading Computer Viruses
Does it ever seem like everyone's out to get you? On the Internet, that is. Your every keystroke being followed, prying eyes over your shoulder when you enter in a password, fake Nigerian princes luring you with the promise of riches? You're not paranoid, you're pragmatic. Operation Ghost Click, the largest cybercrime ring to date, was just brought down by international law enforcement efforts. PC Magazine

Free Android antivirus software is 'useless,' says testing firm
Consumers and workers who install free Android antivirus scanners from relatively unknown developers are mostly wasting their time, an independent testing firm has found. "During our tests, we found out that the majority of free products are -- to make it short -- useless," says Andreas Marx, CEO of AV-Test. Of all the major mobile platforms, Android is at most risk for malware. InfoWorld

CI pinpoints 200 millionth piece of cloud-based malware
The good news is that Collective Intelligence (CI), the engine for Internet security created in 2006 by Panda Security's malware research laboratory, recently processed its 200 millionth malware file via the cloud. That's also the bad news. CI uses the Internet "community" -- users of Panda's free CloudAntivirus, along with other companies and collaborators -- to locate malware. Computerworld

As cyber crimes go international, so must enforcement agencies

A massive investigation by the FBI, international law enforcement agencies, private industry, and nongovernment organizations has led to the charging of seven Estonian and Russian citizens for a widespread click fraud scheme that had infected more than 4 million computers and netted the group more than $14 million, the FBI said on Wednesday.
Infoworld

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-08-11 8:16 AM
To: * DGOPS-CCIRC; * Media Monitoring / Suivi des médias; * NCSD / DGCN; Allison, Catherine; Baker, William V.; 'Black, Dave'; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; 'Clarfield-Henry, Alexis'; Crépeault, David; 'CSIS Media Monitoring'; De Curtis, Laura; 'Dunn, John'; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; 'Gilbert, Monica'; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; ' Panthaky, Jasmine; 'Patry, Line'; Patton, Michael; 'RCMP Emerging Trends'; Roberts, Shane; Robinson, N.; 'Slade, Nancy'; Spendlove, Jim; Sreblowski, Myles; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary - 2011-11-07

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 8, 2011 / le 8 novembre 2011

Online media

US increases cyberwarfare spending
The Defense Advanced Research Projects Agency (DARPA) has announced that it's to boost its investment in cyber research by 50 percent over the next five years, in response to the increasing threat of cyber warfare. DARPA's role in the creation of the internet means we were party to the intense opportunities it created and share in the intense responsibility of protecting it. Our responsibility is to acknowledge and prepare to protect the nation in this new environment," says DARPA director Regina Dugan. DARPA's now recruited a cyber team composed of experts, including 'white hat' hackers. "I should emphasize that national policymakers, not DARPA, will determine how cyber capabilities will be employed to protect and defend the national security interests of the United States," says Dugan. "But the agency has a special responsibility to explore the outer bounds of such capabilities so that our nation is well prepared for future challenges." TG Daily

Smartphone malware surges by 800% in four months
Malware aimed at smartphones has surged by 800 percent in the past four months, says Get Safe Online. According to research that was conducted by the national online security initiative, and has been released as part of Get Safe Online week, which takes place this week (November 7 to 11) and aims to promote safe surfing to Brits, 17 percent of smartphone users now use their phone for money matters and over a fifth (22 percent) download new apps at least once a month. However, with fraudsters populating app stores with malicious software that Get Safe Online says often masquerad as 'free levels' to popular and legitimate online games, or even as security tools, there's an increasing risk for smartphone owners. Once downloaded, the malware enables fraudsters to take control of the victim's phone, allowing them to make calls, send and intercept SMS and voicemail messages, and browse and download online content. They can also gain access to all personal and payment data available on the phone - which can then be sold onto and used by identity fraudsters - and to 'spam' other mobile web users to commit further fraud. PC Advisor

iOS : faille dans la certification des applications
L'expert en sécurité Charlie Miller a encore frappé et trouvé une faille dans iOS qui permet de publier des applications vérolées sur l'App Store malgré le processus de validation d'Apple. En contrôlant étroitement ce qui est diffusé sur son portail App Store, Apple a su lutter efficacement contre les applications malveillantes cachant sous des apparences anodines des malwares cherchant à récupérer des données personnelles ou à gonfler la facture mobile des utilisateurs. Cependant, ce système de validation peut être mis en défaut par un bug présent à partir de iOS 4.3 et au-delà, permettant de publier dans l' App Store des applications cachant des outils permettant de prendre à distance un contrôle partiel de l'appareil mobile et d'accéder à certaines données. La faille a été découverte par Charlie Miller, expert en sécurité chez Accuvant, qui a publié sur l' App Store une application utilisant ce défaut de sécurité qui est d'autant plus gênant qu'il est exploitable non pas sur des terminaux jailbreakés mais sur des appareils standard, avec des applications non pas disponibles sur un portail alternatif mais bien sur l' App Store officiel. GNT

Recent Study Finds 600,000 Facebook Logins Are Compromised Each Day
Whether you're on it all the time or not quite as often, your Facebook account runs the constant risk of being compromised. A recent study found that 600,000 Facebook logins are compromised each day. Mart Nelson is an expert on cyber security and says phishers are the main log-in info stealers. CW33 News

Israeli Government Denies Official Websites Hacked by Anonymous
The government of Israel has denied that its websites have suffered an attack from the hacker group Anonymous. Rumours of an Anonymous attack started after several official websites including those of the Mosaad and secret service agency Shin Bet went offline. The sites went offline soon after a threat was made by Anonymous to launch a cyber attack against the government. In the threating video, Anonymous demanded that the Israeli government should refrain from blocking shipping vessels to Gaza or face its wrath. Israeli officials claim the blacking out of government websites soon after the threats were made was just a coincidence. The outage was caused by a hardware glitch in the servers rather than a hacking induced software glitch. IT Pro Portal

NSS Labs claims its new tool can detect all Duqu drivers - But other security vendors expect Duqu to continue to evade detection
NSS Labs has released an open source scanning tool that is capable of detecting all malicious drivers used by the new Duqu threat, according to the security research firm's engineers. However, other security vendors believe that the malware's creators are capable of evading detection at any time. According to NSS Labs, its scanner uses advanced pattern recognition techniques and was created to further research Duqu, the piece of malware that has captured the attention of the entire security industry in recent weeks. Computerworld UK

Duqu is precursor to next Stuxnet - Malware as invasive as Stuxnet created specifically to collate information on industrial targets
A trojan discovered last month uses the same code as last year's Stuxnet worm, and is thought to have been written by the same authors, according to a report by Symantec. Duqu, however, is different in that it uses a zero-day exploit, thought to be carried out through a vulnerability in Word, to collect information on specific targets, rather than control them. Symantec call the malware "the precursor to the next Stuxnet" as it is thought that it is collecting the information in order to carry out a more informed attack on industrial targets. Duqu pretends to be a driver and uses a digital certificate to aid installation (which was revoked on October 14th 2011). It is thought that the keys required to make the certificate work were stolen from a company in Taiwan. Once the malware has been installed, it downloads additional executables to the target machine, mostly infostealers which include keyloggers and software to report on system information. In order to extract the information, the control and command function masks the outgoing information as a jpg in order to appear legitimate. The malicious software runs on an infected machine for thirty days, after which it deactivates itself. However, Symantec have noted that some of the files downloaded to an infected machine instruct the malware to extend its lifetime. TechWatch

DNS cache poisonings foist malware attacks on Brazilians - 'Desperate cries' from those visiting innocent sites
An attack on several Brazilian ISPs has exposed large numbers of their subscribers to malware attacks when they attempt to visit Hotmail, Gmail, and other trusted websites, security researchers have warned. The attacks work by poisoning the domain name system cache that the service providers use to translate domain names such as google.com into internet protocol numbers such as 74.125.224.144. By replacing legitimate IP addresses with ones leading to servers controlled by attackers, the hack is causing end users to be surreptitiously directed to sites that exploit software vulnerabilities on their computers or trick them into installing malware. UK Register

Klassen, Nathan

From: Bendelier, Kenneth
Sent: November-08-11 8:03 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description: **Busy Busy "Anonymous".** "The Internet Collective known as Anonymous had a busy "Guy Fawkes Weekend". Here are a few highlights on their recent activities."
Reference: http://www.f-secure.com/weblog/archives/00002266.html

2. Item Description: **Anonymous takes down El Salvadoran sites**. "The hacktivist group's "Operation Justice El Salvador" branch has "tried to attack our website to publicize the private information of internal and external users," the economy ministry said. According to the AFP report, presidential spokesman David Rivas told reporters that the attack took the form of a distributed denial of service. The attack comes as no surprise, given that it was preceded by threats: "Anonymous threatened several government websites two weeks ago, including that of the presidency, which on Saturday received at least 30 million hits, saturating the system," Rivas told reporters. The government temporarily took the site offline to stop the attack, Rivas said, while also fending off attacks on the legislative assembly, the National Civil Police and the ministries of justice and labor."
Reference: http://nakedsecurity.sophos.com/2011/11/08/anonymous-attacks-el-salvadoran-sites/

3. Item Description: **Brazilian ISPs hit with massive DNS cache poisoning attacks**. "A massive DNS cache poisoning attack attempting to infect users trying to access popular websites is currently under way in Brazil, warns Kaspersky Lab expert Fabio Assolini. "Brazil has some big ISPs. Official statistics suggest the country has 73 million computers connected to the Internet, and the major ISPs average 3 or 4 million customers each. If a cybercriminal can change the DNS cache in just one server, the number of potential victims is huge," he points out. And that is exactly what has been happening during last week. Users trying to reach Google, YouTube, Facebook and other popular global and local sites were being faced with pop-up windows telling them to install "Google Defence" and similar thematic software or Java applet in order to be able to access the wanted site."
Reference: http://www.net-security.org/secworld.php?id=11903

4. Item Description: **Cyber-Bullying and online Grooming: helping to protect against the risks:** "Children are the most valuable part of every society, regardless of culture, religion and national origin. Given the rapidly increasing digitalisation of their lives, it seemed important to assess risks related to internet usage and, in particular, the risk of become a victim of online grooming and cyber bullying activities. A recent survey on the technology skills of children (2), (3) reveals that digital devices and the internet play a significant role in their lives. Today's kids are living in an environment that is radically different from that of their parents; virtual environments are increasingly prevalent in private and education environments. This development is detrimental to their physical activities, social skills and the behavioural model that prevailed in previous generations. ENISA has formed a Working Group consisting of international experts in various disciplines related to the area of children's online protection. Interdisciplinary knowledge and relevant experience in the area were the criteria of their engagement. During the selection phase of the scenario to be assessed, the expert group has identified cyber bullying and online grooming as an area that requires further elaboration. With this assessment we aim to demonstrate how attacks based on misuse of data (i.e. data mining and profiling) can affect minors."
Reference: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/at_download/fullReport

5. Item Description: **Router glitch causes widespread net outages:** "Internet services throughout North America and Europe saw widespread outages and slowdowns on Monday after backbone provider Level 3 Communications suffered a global failure, network providers said. Time Warner Cable in the US, Research in Motion services for BlackBerry subscribers, and UK ISPs Eclipse Internet, Easynet, and MerulaSupport were all reportedly experiencing problems on Monday. According to multiple accounts, including a variety of Twitter dispatches, at least some of the outages were the result of a bug in Juniper routers that corrupted BGP, or border gateway protocol, tables."
Reference: http://www.theregister.co.uk/2011/11/07/global_net_outage/

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Williston, Sandra

From: Beaudoin, Luc S
Sent: November-07-11 9:08 AM
To: Scouten, Julia
Cc: Melanson, Daryl
Subject: Daily

- Please remove Event 2454
- Consider adding the following:

Daryl, if you have the ref for the News-bits this AM that be nice to add.

Reported Compromise / Data Breach:

1. Item Description: **Israel's security websites down after 'anonymous' hacker threat**

The websites of Israel's military and its intelligence services were down Sunday, two days after a hacker group appeared to threaten the Jewish state over its interception of a Gaza-bound flotilla. The websites of the Israel Defense Forces, the Shin Bet domestic intelligence agency and the Mossad foreign intelligence service were all unavailable through the day and into the evening. Prime Minister Benjamin Netanyahu's office, whose website was functioning, said that the outage was caused by a technical glitch rather than by hackers. "Israeli government websites crashed today because of a server malfunction, not as a result of a cyber attack," Ofir Gendelman, a Netanyahu spokesman, wrote in a posting on Twitter. The website problems came two days after a video apparently from "hacktivist" group Anonymous was posted on YouTube, threatening the Israeli government with retaliation over its interception of two Gaza-bound ships. The boats carrying 27 activists, crew and journalists were intercepted in international waters before they could breach Israel's blockade on the Palestinian territory. A14

- Reference: Calgary Herald,

2. Item Description: **Nearly 2,700 personal tax files downloaded on missing laptop - PRIVACY RULES BROKEN**

The confidential tax files of almost 2,700 Canadians are missing after a Canada Revenue Agency worker took them home and let a friend download them onto a laptop. The laptop has disappeared, the agency is scrambling to rewrite its security protocols and the privacy commissioner is asking why no one alerted her to the breach in confidentiality.

- Reference: Red Deer Advocate, A5

3. Item Description:Adidas sites suffer cyber-attack

Adidas, the German sportswear and equipment maker, said on Sunday that all its websites remained closed down on Sunday after what it called a 'sophisticated and criminal' attack.

- Reference: http://www.straitstimes.com/BreakingNews/TechandScience/Story/STIStory_731336.html

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

Dvorkin, Corey

From: Julianne Prokopich
Sent: November-07-11 11:16 AM
To: Dick, Robert; Gordon, Robert; Dvorkin, Corey; Hatfield, Adam
Cc: Motzney, Barbara; Maillé, Marie Anick; Tolan, Katie
Subject: WSHDC Look ahead: Cybersecurity (NOV 7 - 11)
Attachments: 11411 BNA Report - NIST Seeks Feedback on Proposed Guidelines for Federal Cloud Adoption.docx; 110411 CQ -Survey Finds Infrastructure Unprepared for Cyberattack.docx

FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: The Office of the National Counterintelligence Executive released a Report to Congress in October titled *Foreign Economic Collection and Industrial Espionage, 2009-2011.* The Report concluded that foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. Cyberspace—where most business activity and development of new ideas now takes place—amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect. Other highlights of the report follow.

US Technologies and Trade Secrets at Risk in Cyberspace: Foreign collectors of sensitive economic information are able to operate in cyberspace with relatively little risk of detection by their private sector targets. The proliferation of malicious software, prevalence of cyber tool sharing, use of hackers as proxies, and routing of operations through third countries make it difficult to attribute responsibility for computer network intrusions. Cyber tools have enhanced the economic espionage threat, and the IC judges the use of such tools is already a larger threat than more traditional espionage methods.

Economic espionage inflicts costs on companies that range from loss of unique intellectual property to outlays for remediation, but no reliable estimates of the monetary value of these costs exist. Many companies are unaware when their sensitive data is pilfered, and those that find out are often reluctant to report the loss, fearing potential damage to their reputation with investors, customers, and employees. Moreover, victims of trade secret theft use different methods to estimate their losses; some base estimates on the actual costs of developing the stolen information, while others project the loss of future revenues and profits.

Pervasive Threat From Adversaries and Partners: Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, and citizens of dozens of countries.

1. **Chinese actors are the world's most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC cannot confirm who was responsible.**
2. **Russia's intelligence services are conducting a range of activities to collect economic information and technology from US targets.**
3. **Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities.**

Outlook: Because the United States is a leader in the development of new technologies and a central player in global financial and trade networks, foreign attempts to collect US technological and economic information will continue at a high level and will represent a growing and persistent threat to US economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment. report

WSHDC:

NOV 3 –American intelligence agencies, in an unusually blunt public criticism of China and Russia, reported to Congress on NOV 3 that those two foreign governments steal sensitive American technology over the Internet as a matter of national policy. Both China and Russia hide behind the anonymity of proxy computers and dispersed routers in third countries to pilfer proprietary corporate information to accelerate their own economic development, according to the new intelligence assessment. They have also targeted the computer networks of government agencies and universities, the report said. Article

NOV 3 – EU and US cybersecurity officials have tested how they would co-ordinate their response to a hacking attack. The exercise in Brussels marked the first time the two bodies have role-played the scenario together. The stress tests follow a similar event involving the European nations last year. Organisers said afterwards that states "must increase their efforts". Article

NOV 3 –The U.S. Department of Justice now says its use of a cellphone-tracking device in a controversial Arizona case could be considered a "search" under the Fourth Amendment, a tactical move legal experts say is designed to protect the secrecy of the gadgets known as "stingrays." Article

NOV 2 – Plans by the hacker collective Anonymous to expose collaborators with Mexico's bloody Zetas drug cartel – a project it dubbed "#OpCartel" – have fallen into disarray, with some retreating from the idea of confronting the killers while others say that the kidnap of an Anonymous hacker, the incident meant to have spawned the scheme, never happened. The apparent climbdown by the group came as one security company, Stratfor, claimed that the cartel was hiring its own security experts to track the hackers down – which could have resulted in "abduction, injury and death" for anyone it traced. Article

NOV 2 –The National Institute of Standards and Technology Nov. 1 asked for public comments on a draft "roadmap" calling for the federal government to take security precautions and other steps before adopting cloud computing technology. The roadmap identifies key requirements for cloud adoption, including the development of voluntary, "consensus-based" interoperability, portability, and security standards. [See attached for BNA Report]

NOV 2 –The Stuxnet computer worm continues to rattle security experts around the world, one year after its existence was made public. A growing awareness of the cyberthreat too critical infrastructure assets, however, may well deepen concerns about the "blowback" risk to the U.S. homeland from the development of a potent cyber weapons designed to be used elsewhere. The appropriate level of information-sharing between the offensive and defensive teams within the U.S. cyber community is likely to be the focus of intense interagency discussion. Article

NOV 1 – At a global conference on Internet security, the U.S. and U.K. set out principles they hope will form the basis of international cooperation in Web governance, in which states would work together on issues such as security and copyright protection without imposing new restrictions on users. The conference, attended by business and government leaders from around the world, shows how cybersecurity has vaulted on the foreign-policy agenda. But it is as likely to highlight disagreements as much as consensus, with China and others as interested in clamping down on Internet users than shutting the door on criminals and spies. Article

OCT 27 –Secretary Napolitano said the No. 1 type of cyberattack that worries her is one that would damage the nation's critical infrastructure and cause loss of life or disrupt everyday living. She was vague, though, when asked if the U.S. had already come close to experiencing that type of attack. Napolitano merely said that the DHS is learning from every incident. Napolitano offered sobering figures, such as that Web-based intrusions have increased 90 percent since 2009. The secretary said she'd like to have "cyber geeks" with expertise in hacking come work for her department. Napolitano's comments came during a cybersecurity symposium at The Washington Post building. Article

WHITE HOUSE:

NOV 1 – Vice President Biden delivered remarks at the London Cyberspace Conference via video teleconference.

UPCOMING HEARINGS:

NOV 9 @ 2:30pm – The Senate Committee on the Judiciary will hold a hearing on, "Your Health and Your Privacy: Protecting Health Information in a Digital World." 226 Dirksen Bldg

THINK TANKS:

NOV 1 – Symantec Corp. surveyed 3,475 organizations in 37 countries this summer and compiled results that indicate the awareness about threats and engagement with government infrastructure protection programs has dropped off substantially. In 2010, 55 percent of those surveyed indicated they were aware of the government programs, a figure that dropped to 36 percent this year. The percentage of respondents who said they were engaged in those programs also fell from 56 to 37. And the number willing to cooperate with those programs went from 66 percent down to 57. [See attached for CQ article]

OCT 31 –At least 48 chemical and defense companies were victims of a coordinated cyber attack that has been traced to a man in China, according to a new report from security firm Symantec Corp. Computers belonging to these companies were infected with malicious software known as "PoisonIvy," which was used to steal information such as design documents, formulas and details on manufacturing processes, Symantec said. It did not identify the companies, but said they include multiple Fortune 100 corporations that develop compounds and advanced materials, along with businesses that help manufacture infrastructure for these industries. Article

UPCOMING EVENTS:

None to report.

Julianne Prokopich
Research Analyst, Public Safety and Border Security | Analyste en Recherche, Sécurité publique et de la sécurité des frontières
Embassy of Canada | Ambassade du Canada
501 Pennsylvania Avenue NW, Washington, DC 20001
Phone: (202) 682- 7743 Ext 7743 | Fax (202) 682-7792
Julianne.Prokopich@international.gc.ca

Dvorkin, Corey

From: Barr, Corri <Corri.Barr@tbs-sct.gc.ca>
Sent: November-07-11 8:27 AM
To: Dvorkin, Corey
Subject: FW: Just FYI

Corri Barr
Director, Parliamentary and Cabinet Affairs | Directrice des affaires parlementaires et du cabinet.
Strategic Communications, Media and Parliamentary Relations | Communications stratégiques, médias et relations parlementaires
Strategic Communications and Ministerial Affairs | Communications stratégiques et affaires ministérielles
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Corri.Barr@tbs-sct.gc.ca
Telephone | Téléphone 613-952-1693 / Facsimile | Télécopieur 613-941-4000 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Canada

Better government: with partners, for Canadians | Un meilleur gouvernement : avec nos partenaires, pour les Canadiens

---

From: Le Gras, Gilbert
Sent: November 7, 2011 8:24 AM
To: Barr, Corri
Subject: FW: Just FYI

As discussed

From: Le Gras, Gilbert
Sent: Monday, November 07, 2011 08:03 AM
To: Proulx, Michel; Bashir, Imraan
Cc: Gosselin, Michael; Gilbert, Tanis
Subject: Just FYI

CYBER SECURITY / CYBERSÉCURITÉ

*** Israel's security websites down after 'anonymous' hacker threat**

The websites of Israel's military and its intelligence services were down Sunday, two days after a hacker group appeared to threaten the Jewish state over its interception of a Gaza-bound flotilla. The websites of the Israel Defense Forces, the Shin Bet domestic intelligence agency and the Mossad foreign intelligence service were all unavailable through the day and into the evening. Prime Minister Benjamin Netanyahu's office, whose website was functioning, said that the outage was caused by a technical glitch rather than by hackers. "Israeli government websites crashed today because of a server malfunction, not as a result of a cyber attack," Ofir Gendelman, a Netanyahu spokesman, wrote in a posting on Twitter. The website problems came two days after a video apparently from "hacktivist" group Anonymous was posted on YouTube, threatening the Israeli government with retaliation over its interception of two Gaza-bound ships. The boats

carrying 27 activists, crew and journalists were intercepted in international waters before they could breach Israel's blockade on the Palestinian territory. Calgary Herald, A14

Gilbert LeGras
Senior Communications Strategist | Stratège principal en communications
Strategic Communications, Media and Parliamentary Relations | Communications stratégiques, médias et relations parlementaires
Strategic Communications and Ministerial Affairs | Communications stratégiques et affaires ministérielles
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Gilbert.LeGras@tbs-sct.gc.ca

Telephone | Téléphone 613-948-7744 / Facsimile | Télécopieur 613-941-4000 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-07-11 8:24 AM
To: * DGOPS-CCIRC; * Media Monitoring / Suivi des médias; * NCSD / DGCN; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Slade, Nancy; Spendlove, Jim; Sreblowski, Myles; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary - 2011-11-07

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 7, 2011 / le 7 novembre 2011

Print media

Israel's security websites down after 'anonymous' hacker threat
The websites of Israel's military and its intelligence services were down Sunday, two days after a hacker group appeared to threaten the Jewish state over its interception of a Gaza-bound flotilla. The websites of the Israel Defense Forces, the Shin Bet domestic intelligence agency and the Mossad foreign intelligence service were all unavailable through the day and into the evening. Prime Minister Benjamin Netanyahu's office, whose website was functioning, said that the outage was caused by a technical glitch rather than by hackers. "Israeli government websites crashed today because of a server malfunction, not as a result of a cyber attack," Ofir Gendelman, a Netanyahu spokesman, wrote in a posting on Twitter. The website problems came two days after a video apparently from "hacktivist" group Anonymous was posted on YouTube, threatening the Israeli government with retaliation over its interception of two Gaza-bound ships. The boats carrying 27 activists, crew and journalists were intercepted in international waters before they could breach Israel's blockade on the Palestinian territory. Calgary Herald

Nearly 2,700 personal tax files downloaded on missing laptop - PRIVACY RULES BROKEN
The confidential tax files of almost 2,700 Canadians are missing after a Canada Revenue Agency worker took them home and let a friend download them onto a laptop. The laptop has disappeared, the agency is scrambling to rewrite its security protocols and the privacy commissioner is asking why no one alerted her to the breach in confidentiality. Red Deer Advocate

Online media

Scam warning for UK smartphone users
Britain is increasingly at risk from scams that could see smartphone owners' mobile bills rocketing. A national computer security campaign has urged people in the UK to be wary of downloading harmful applications to their handset. Get Safe Online says there has been a massive increase in smartphone malware as more people opt for the sophisticated mobile devices. Mobile Choices

États-Unis et Europe s'entraînent aux contre-cyberattaques
Le 3 novembre à Bruxelles, les Etats-Unis et les membres européens étaient réunis pour participer à des exercices de défense informatiques. L'exercice, « Cyber Atlantic 2011 », s'est déroulé sous la houlette de l'agence européenne Enisa et du département de la défense américain. Preuve, s'il en fallait encore une, que la cyber-sécurité est devenue un élément de préoccupation majeure dans divers Etats, cette séance collective de prévention et de tests a réuni les Etats-Unis et 20 membres de l'UE, dont 16 ont participé à cet évènement baptisé « Cyber Atlantic 2011 ». L'Informaticien

Cyber-Attack Alert - Chemical companies have been under siege by a hacker in China, security software firm says.
A cyber-attack campaign emanating from China targeted private companies involved in the research, development, and manufacture of chemicals and advanced materials between July and September of this year, according to a report from the computer security company Symantec. The firm claims the campaign, which it has dubbed the "Nitro" attacks, targeted intellectual property and followed similar attacks on nongovernmental organizations and the auto industry. Twenty-nine companies in the chemical sector were confirmed targets in the attack, according to the report, along with 19 firms in other industries including defense. Symantec says the hackers operated by sending e-mails purporting to be meeting invitations from established business partners. Opening the e-mails could have triggered a program called Poison Ivy that passed through networks and computers—primarily to obtain administrator credentials and access codes. Chemical & Engineering News

Cyber criminals may target London 2012 Olympics computer systems: Expert
Crime gangs may target London 2012 Olympics computer systems as a cover for a far bigger cyber attack on financial institutions in the City, an expert has warned. One of the UK's leading experts on cyber security have warned all traders, banks and financial institutions to act now to shore up systems against an attack next July. According to experts, the London Olympics is billed as the first "truly digital games," Express.co.uk reports. Stuart Okin, former chief security adviser at Microsoft UK, said it was a "given" that hackers would try and breach Olympic security. TruthDive

Le virus informatique Duqu est en France
Repéré il y a quelques semaines, Duqu, un cheval de Troie qui se glisse dans un fichier Word, est comparé à Stuxnet et pourrait préfigurer une attaque très ciblée contre des sites industriels. Microsoft estime le risque faible et vient seulement de publier un patch. Le 9 octobre dernier, l'éditeur Symantec publiait sa découverte d'un virus nommé Duqu (car il génère deux fichiers dont le nom commence par DQ), « qui semble le précurseur d'une attaque de type Stuxnet ». Il partage en effet une partie de son code avec ce virus qui, en 2010, avait ciblé des équipements industriels, du type de ceux utilisés en Iran dans des installations industrielles. Futura-Techno

Microsoft propose un correctif provisoire pour contrer Duqu
Alors que l'éditeur travaille sur un patch définitif qui sera disponible avec la mise à jour du 13 décembre, il met à disposition un "Fix It" pour contrer le cheval de Troie. Microsoft a publié du code qui permet de bloquer temporairement les attaques prenant à parti la vulnérabilité de Windows que Duqu exploite. Ce correctif peut dès à présent être téléchargé. En revanche, il faut l'utiliser avec parcimonie car il bloque l'emploi des polices True Type. Le logiciel malveillant se propage en effet via une faille présente dans Word, et plus précisément dans le moteur Win32k True Type, qui fait partie par défaut des systèmes Windows. L'Informaticien

US accuses China and Russia of widespread cyber espionage
China and Russia are singled out for their cyber espionage efforts in a report sent to US Congress. The US has accused China and Russia of wide-scale cyber espionage, saying they would continue to steal sensitive American data. There has been a spate of attacks this year in which nation states have been blamed. When Mitsubishi Heavy Industries, one of Japan's military contractors, was hit earlier this year, fingers pointed to Beijing. Last year, Google claimed China was responsible for a hack on the web giant, in attacks that became known as Operation Aurora. PC & Tech Authority

Nearly two dozen PCs in Japanese government offices found to have Trojan horse viruses
Personal computers at the head office and local branch offices of the Japanese Internal Affairs and Communications Ministry have been infected with computer viruses and have repeatedly been accessed by servers abroad, according to the ministry. The ministry announced Friday that 22 PCs have been infected. The incident is similar to recently revealed cyberattacks targeting the country's House of Representatives, the House of Councillors and Foreign Ministry computers. The viruses found in the internal affairs ministry's PCs are similar to ones found in the other recent cases. PhysOrg.com

DroidKungFu un malware très dangereux sous Android
Fortinet vient de publier sont rapport du mois d'Octobre. Dans ce rapport, il apparapit que ce mois-ci, FortiGuard Labs a observé le développement continu du nouveau logiciel malveillant DroidKungFu, qui a de multiples variantes et se comporte de façon similaire aux logiciels malveillants que l'on trouve aujourd'hui sur les PC. "DroidKungFu représente clairement la prochaine évolution des logiciels malveillants sur mobiles," déclare Derek Manky, sénior stratégiste en sécurité chez Fortinet. "Tandis que les premières tentatives de logiciels malveillants sur Android, comme Zitmo (Zeus in the Mobile), sont capables d'intercepter le type d'authentification à deux-facteurs que les banques utilisent pour valider l'identité du titulaire du compte lorsqu'il se connecte, DroidKungFu fait beaucoup plus. En prenant la forme d'une application client VPN légitime, le logiciel malveillant s'implante rapidement dans les appareils en utilisant l'ingénierie sociale. Une fois exécuté, DroidKungFu télécharge d'autres logiciels malveillants, ouvre des URL dans un navigateur, lance des programmes et supprime des fichiers du système." Programmez!

'Skype becoming a popular platform for malware'

Skype video calling service is also becoming a popular platform for malware distribution, according to software security firm Kaspersky Lab. In its recently released Malware Statistics Report, the company said cybercriminals make fake phone calls to Skype users that do not have call restrictions and warn them of infection on their computers unless they visit a specific website. The said website, when visited, will download malware onto the users' computers and ask them to pay a certain amount to activate "security" functions. Kaspersky Lab security expert Alexander Gostev noted that there has been a rise in attacks using Skype in September. He then advised users to only receive phone calls from those who are in their contacts list. ABS-CBN News

Hayward, Jane

From: Glazer, David on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-07-11 8:01 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
November 7, 2011 / le 7 novembre 2011

MINISTER / MINISTRE

'Welcome mat' wearing thin
While the Americans have no intentions -- yet -- of building a Mexican-style barrier to keep illegals from heading south from Canada, that tune may change if Canada doesn't yank out the welcome mat for every bogus refugee applicant crying of persecution. When up to 50 Hungarian Roma can arrive at Pearson International on a daily basis and be accepted over dubious claims of being persecuted back home by "skinheads or neo-Nazis," our welcome mat is obviously way too welcoming. According to federal **Public Safety Minister Vic Toews**, 9,200 failed refugees yearly go underground in the Toronto area alone. This is huge concern -- for us, and for the Americans. Edmonton Sun, 14 (Calgary Sun, Toronto Sun, Ottawa Sun, Winnipeg Sun)

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Time for Canada to up its spy game
As the Harper government prepares to reintroduce the anti-terrorism measures that were allowed to lapse because of opposition concerns about privacy and Charter rights, there are whispers Conservative plans to expand the role of Canada's spy service to operate overseas are being dusted off. Currently, the Canadian Security Intelligence Service is largely concerned with domestic intelligence and is able to conduct covert operations overseas only if there is a direct threat to Canada. When Stockwell Day was Public Safety Minister, from 2006 to 2008, progress was made on expanding CSIS' role and the plan was to reform the 1985 CSIS Act by removing the words "within Canada" from its mandate, allowing the agency to replicate its domestic operations overseas. Negotiations were held with U.S. and U.K. spy agencies on how to go about foreign operations. National Post, A1

*** Stuck with one Khadr**
The RCMP respected individual rights in the Abdullah Khadr case, and now Canada is stuck with the suspected al-Qaeda terrorist. But our institutions worked as they should. Abdullah Khadr appears to be home free. It is not a terribly comforting ending to his saga. A United States extradition request was rejected by a judge. On Friday, the Supreme Court of Canada refused to hear an appeal of that rejection. But there is something heartening, too. Canada's security agencies played by the rules. Canada's hands have not always been so clean in the war on terror. The case of Abdullah Khadr is noteworthy because Canada respected the letter and spirit of the Charter of Rights and Freedoms. The civilian spy agency, CSIS, told Pakistan's notorious Inter-Services Intelligence Directorate that it would have to treat Mr. Khadr in accordance with international law. When U.S. officials sought Canada's permission to move Mr. Khadr to the U.S. for trial, this country's foreign affairs department said no. And the RCMP would not let a future prosecution be contaminated by conducting an interrogation in Pakistan with the Pakistanis present. Globe and Mail, A14

CYBER SECURITY / CYBERSÉCURITÉ

*** Israel's security websites down after 'anonymous' hacker threat**
The websites of Israel's military and its intelligence services were down Sunday, two days after a hacker group appeared to threaten the Jewish state over its interception of a Gaza-bound flotilla. The websites of the Israel Defense Forces, the Shin Bet domestic intelligence agency and the Mossad foreign intelligence service were all unavailable through the day and into the evening. Prime Minister Benjamin Netanyahu's office, whose website was functioning, said that the outage was caused by a technical glitch rather than by hackers. "Israeli government websites crashed today because of a server

malfunction, not as a result of a cyber attack," Ofir Gendelman, a Netanyahu spokesman, wrote in a posting on Twitter. The website problems came two days after a video apparently from "hacktivist" group Anonymous was posted on YouTube, threatening the Israeli government with retaliation over its interception of two Gaza-bound ships. The boats carrying 27 activists, crew and journalists were intercepted in international waters before they could breach Israel's blockade on the Palestinian territory. Calgary Herald, A14

*** Nearly 2,700 personal tax files downloaded on missing laptop - PRIVACY RULES BROKEN**
The confidential tax files of almost 2,700 Canadians are missing after a Canada Revenue Agency worker took them home and let a friend download them onto a laptop. The laptop has disappeared, the agency is scrambling to rewrite its security protocols and the privacy commissioner is asking why no one alerted her to the breach in confidentiality. Red Deer Advocate, A5

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Man charged after Mountie beaten
A man is facing 15 charges after being accused of beating up an RCMP officer, stealing his police car, then crashing the vehicle a short time later in Slave Lake this weekend. Ottawa Citizen, A3 (Leader-Post, National Post, Edmonton Journal, Calgary Herald, Telegraph-Journal, Le Nouvelliste); * Edmonton Sun

*** Les coûts de la sécurité explosent**
Les coûts des services de sécurité de la GRC sur la colline du Parlement à Ottawa ont presque doublé depuis deux ans, soit depuis la manifestation de Greenpeace sur le toit de l'édifice de l'Ouest. De 3,6 millions de dollars en 2009-2010, ces coûts sont passés à 6,3 millions en 2010-2011, selon des documents que La Presse a obtenus en vertu de la Loi sur l'accès à l'information. Les périodes couvertes vont du 1er avril au 31 mars. Les frais sont associés aux salaires du personnel, à l'entretien des véhicules et au carburant, entre autres. Le Quotidien, 12 (La Tribune, La Voix de l'Est, La Presse)

*** Your gun matters less than the intent in your heart**
A letter states, "...The "gun" issue in this country is about more than firearms. Gun laws, such as the long-gun registry, do not save lives..." National Post, A13

*** Quebec's legal community vigilant after assault on lawyer**
The bloody assault on a high-profile Quebec criminal lawyer outside his home in a quiet, leafy Montreal neighbourhood has shocked members of the province's legal community as they ponder the possibility it's not an isolated incident. Gilles Dore, a veteran lawyer who has defended alleged members of organized crime, was attacked Friday night and taken to hospital after suffering serious injuries from blows to the head and torso. Globe and Mail, A6

*** Not sorry to see gun registry go**
Charles Lamb misses the point MP Kevin Sorenson was making about the anger and frustration most of us feel after being forced, under threat of serious jail time and a criminal record, to license ourselves and register our private property with the federal government. Recent statistics obtained by Breitkreuz from the Library of Parliament and Statistics Canada, and cited by National Post columnist Lorne Gunter, showed that licensed owners and their registered firearms are rarely involved in the most violent crimes. Calgary Herald, A13

*** Goodbye and good riddance to long gun registry**
An opinion piece states, "One sunny afternoon in early fall, a bunch of my neighbours were standing around watching a sick raccoon die on somebody's front lawn. In the old pre-gun registry days, someone would have gone home, got a shotgun or .22 and put the poor creature out of its misery..." Whig-Standard, 5

*** Drug bust snares local biker**
Police have arrested nine people and seized drugs valued at more than $5 million in a two-province investigation that involved a man with alleged ties to the Hells Angels. The arrests - seven in Cambridge and two in Newfoundland - were made Friday, the culmination of a four-month joint investigation involving Waterloo Regional Police, Ontario Provincial Police and Royal Canadian Mounted Police. The Record, A1

*** Gun registry helps**
An opinion piece states, "I'm very concerned about how our current government ignored the public, experts and the evidence in their unrelenting mission to dismantle the long-gun registry. The long-gun registry made sense. It was costly to set up - $1 billion over 10 years. But the annual cost of maintaining it was a measly $2 million to $4 million. Eliminating the registry now will mean all those billions of dollars go to waste, with nothing to show for..." The Record, A8

*** Lettres - Aux armes, citoyens!**
Un lettre déclare, « ...l'État autorise les citoyens qui le demandent à porter de manière dissimulée des armes à feu légères, des pistolets électriques Taser, des armes blanches et des matraques. Beau cocktail. A mon avis, ils auraient pu se forcer un peu et allonger la liste afin d'y inclure des bâtons de baseball! Et dire que le gouvernement Harperien s'inspire des pratiques politiques des États-Unis... Les conservateurs et leurs sbires, qui prêchent pour la loi et l'ordre, nous projettent dans un avenir sombre qui risque de déstabiliser les bases mêmes de notre pays en imitant les loufoqueries de nos insouciants voisins du sud... » Le Devoir, A6

*** Construction - Le courage d'agir**
Un article d'opinion déclare, « ...Mais la FTQ-Construction et le Conseil provincial du Québec des métiers de la construction, visés par l'annonce de Mme Lemieux, ne portent pas à eux seuls tous les maux du secteur. Aux employeurs qui tolèrent si facilement le travail au noir, lui-même porte d'entrée pour le crime organisé, la CCQ s'en vient aussi avec un message: elle sé-vi-ra. Assumer ainsi ses responsabilités est un langage rare dans le Québec de ces dernières années. Cela fait du bien à entendre. Et du bien aussi de voir que c'est une lionne qui arrive enfin à mater une telle jungle. » Le Devoir, A6

*** Les leçons de l'histoire - Lutter contre la corruption et... l'oubli**
Un article d'opinion déclare, « L'intérêt pour la corruption semble sans précédent au Québec. Cet engouement médiatique reflète-t-il une hausse réelle de la corruption dans notre province? Y aurait-il des raisons de s'inquiéter de la moralité dans nos administrations?... » Le Devoir, A7

*** Family balks as cops clear cops in fatal shooting**
The Wright family was advised to keep quiet while officers from the Vancouver Police Department probed the Langley RCMP shooting. On Wednesday, Vancouver major-crime detectives announced their conclusion that there were no reasonable grounds to believe the officer involved, an 18-year veteran, broke the law. Al Wright says he's tired of "suppressing" his family. The Province, A6

*** Les criminalistes de la région peu inquiets**
Les avocats criminalistes du Saguenay-Lac-Saint-Jean ne craignent pas les représailles de leurs clients ou de membres d'organisation criminalisée et ne croient même pas que ça pourrait se produire dans la région. Le Quotidien, 6

*** Newfoundlanders arrested in RCMP drug bust**
Two people from Newfoundland and Labrador have been arrested in an interprovincial drug bust against the Hells Angels motorcycle club. The Telegram, A8

*** Duchesneau de retour au ministère des Transports ?**
Mis à la porte il y a quelques jours, l'ex-patron de l'Unité anticollusion, Jacques Duchesneau, pourrait reprendre du service au ministère des Transports. Un mois plus tôt, son rapport ayant eu l'effet d'une bombe, Jacques Duchesneau avait livré un témoignage percutant et très médiatisé en commission parlementaire; il disait avoir constaté un "empire clandestin " dans le milieu de la construction. Il affirmait que le crime organisé y était bien implanté. Journal Montreal, 6

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

*** Inquiry shifts to investigation that failed to stop Pickton**
The two police agencies that failed to stop Robert Pickton as he hunted sex workers in Vancouver's Downtown Eastside are about to appear at the public inquiry into the case to explain why they were unable to catch a serial killer. That work is set to begin Monday, as Vancouver's Deputy Chief Doug LePard, who authored an internal report about the Pickton investigation, becomes the first police witness. After him, the author of a similar RCMP report will testify, as will a senior officer from the Peel Regional Police in Ontario who was asked to provide an outside opinion. Red Deer Advocate, A6 (Chronicle-Herald)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Border guard helped smuggle cocaine
A Canada Border Services Agency border guard who helped cocaine traffickers smuggle drugs into B.C. has been sentenced to five years in a U.S. jail, followed by four years of supervised release. Jasbir Singh Grewal, 40, was handed the term in a Seattle courtroom Friday by U.S. district court Judge Robert Lasnik. National Post, A6 (The StarPhoenix, Vancouver Sun)

Woman at border had bomb instructions: files
A member of an extreme-right Alaskan militia is in police custody after trying to enter Canada with a concealed pistol and a "hoard of documents" on bomb-making and biotoxins, according to Alaskan court documents. On Oct. 27, Mary Ann Morgan, 53, pulled up to the border crossing station in Beaver Creek, one of only two border crossings between Alaska and the Yukon Territory. When officers asked if she had any firearms in the truck, she told them she had a Beretta .32 - a semi-automatic concealed carry pistol - in the back. National Post, A4

*** No fence for Canada**
U.S. officials say they have no intention of migrating a southern border fence to the quieter line with Canada. A recent American environmental impact analysis of constructing a few sections of a fence along key areas of the Canadian border caused a minor seismic shock on this side of the boundary. But Mark Borkowski, assistant commissioner for the office of technology innovation and acquisition with U.S. Customs and Border Protection, says officials don't see any cause currently to place the same type of brooding barriers on the Canadian border as they now have on their southern frontier. Winnipeg Sun, 13

*** Dealing with a not-so-friendly neighbour to the south**
An opinion piece states “Pierre Trudeau once compared Canada's relationship with the United States to sleeping with an elephant. But a more apt description today of the American governmental system is that of an octopus, whose many arms are ready to suck the life out of Canadian interests at any time with little regard for the overall relationship between our two nations. (One arm is) the Department of Homeland Security, always ready to add more security checks, more fees, and more border programs. Now Homeland Security is musing about building fences along part of our border. Few Canadians have likely heard of the U.S. Government Accountability Office, but this arm of the octopus recently had a few folks walk across a stretch of our 8,500-kilometre border with video cameras in hand, looking for certain proof that more security is needed. Meanwhile, Canadian and American governments are in the final stages of negotiating an agreement to reduce border wait times and paperwork, as well as sharing security duties on a shared perimeter. Unfortunately, Canadian negotiators cannot walk away. Our trade and security partnership with the United States is based on our own benefit and self-interest, not on how sophisticated or friendly the U.S. government acts towards us. Still, it takes steady nerves and a strong stomach these days to handle Canadian-American relations.” Charlottetown Guardian, A9

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Harper defends contentious anti-crime bill
Prime Minister Stephen Harper says his contentious anti-crime measures aren't "terribly expensive" and provinces such as Ontario and Quebec that complain about having to foot the bill for the added costs to their prison systems should accept their "constitutional responsibilities" to help keep streets safe. Leader-Post, A5 (Ottawa Citizen, The Star Phoenix, National Post, The Gazette, Vancouver Sun, Calgary Herald, The Province, Telegraph-Journal, Winnipeg Free Press,); * Calgary Sun (Edmonton Sun, Toronto Sun, Ottawa Sun, Winnipeg Sun); * Le journal de Montréal

*** Ignoring crime's true victims**
An opinion piece states, “Prime Minister Stephen Harper promised to pass his Omnibus Crime Bill in 100 days and his government is on track. The Commons Justice Committee is hearing a little from a lot of witnesses and most are being cut off mid-sentence. The Committee is moving at lightning speed. Government officials say Bill C-10 will "provide support and protection for victims of crime."... With Stephen Harper's government, "victims come first." Having advocated for victims of crime for almost 20 years, I reviewed the proposed legislation. In the hundreds of pages of would-be law, I found only a few that deal with victims. Among those are several provisions that enhance the rights of victims in the corrections and parole system. These are important provisions, but were first introduced in 2005 by the Liberal government of Paul Martin... There is no evidence that the billions the governments are going to spend on this crime agenda will enhance justice for victims of crime. The Conservatives need to consider the implications of their proposed bill, and ask themselves if they're truly willing to put the needs of victims first.” National Post, A12

*** The provinces and the cost of the crime bill**
An editorial states, “It is one thing for the federal government to unilaterally pass new tough-on-crime laws. It is quite another, however, to burden cash-strapped provinces with costs stemming from the measures without adequate consultation... Debatable as the proposed measures may be, however, it is the federal government's exclusive prerogative to legislate in matters of criminal law. And it's not as though the Conservatives suddenly sprang this legislation on an unsuspecting Canadian public once they nailed down a parliamentary majority. The measures had previously been put forward, though in separate bills, and the Conservatives campaigned on them leading up to the May 2 election that delivered them their majority. What the government has neglected to do up to now, and what it should

decently do, is, first: determine what the cost of the measures is likely to be, including the anticipated multibillion-dollar bill for the spate of new prisons that will have to be built. It is disturbing that the government has not so far come up with a figure - or, if it does have one in hand, that it has not confided it to the public..." The Gazette, A23

***Gas station killer violates parole again**
The young man who dragged Grant de Patie to his death during a gas-and-dash robbery in Maple Ridge in 2005 has violated his parole for the second time by ignoring his curfew and failing to return to his Victoria halfway house, according to de Patie's father. Doug de Patie said he was informed by National Parole Board officials at around 11 p.m. Saturday night that Darnell Pratt, 22, was on the loose again. Pratt, who was give a nine-year prison sentence after pleading guilty to manslaughter in 2005, was freed last week in keeping with federal statutory release. He was also let out in 2010, but was sent back to prison after violating parole in Kamloops. Vancouver Sun, A6, The Province

*** Decriminalize**
Not only should medical marijuana be made available to patients in need, but adult recreational use should be regulated. Drug policies modelled after alcohol prohibition have given rise to a youthoriented black market. Throwing more money at the problem is no solution. Attempts to limit the supply of illegal drugs while demand remains constant only increase the profitability of drug trafficking. For addictive drugs like heroin, a spike in street prices leads desperate addicts to increase criminal activity to feed desperate habits. The drug war doesn't fight crime, it fuels crime. Taxing and regulating marijuana is a cost-effective alternative to a neverending drug war. As long as marijuana distribution is controlled by organized crime, consumers will come into contact with hard drugs like methamphetamine, cocaine and heroin. This "gateway" is a direct result of marijuana prohibition. Calgary Herald, A13

*** Third time on probation for 'at risk' double murderer**
A convicted double murderer known for breaching release conditions has been granted full parole for the third time. Patrick James Tremblay may be relocating to the Calgary area in January. Tremblay, 43, is serving a life sentence for two counts of seconddegree murder in the execution-style slaying of an elderly Alberta couple Feb. 6, 1985. He has a history of violating conditions and having parole revoked. Calgary Herald, B2

*** Expand horizons**
A letter states, "The local academic community is late in joining the ranks of security and police practitioners who have been aware of environmental criminology since the 1970s. This is a multimillion-dollar industry with courses taught by police, security, universities, many books written, global conferences held and associations focused on environmental crime control...Environmental crime control has been used in the U.K. as a plank in the Home Office's platform since the early 1980s. To say that this theory is gaining in acceptance is a statement 30 years too late..." Calgary Herald, A13

*** Couple dead in murder-suicide**
The murder of a Hamilton mother of three over the weekend is drawing attention to a fact buried in recent reports about Canada's dropping crime rate. While figures released last month by Statistics Canada show the national homicide rate has tumbled to its lowest level in more than four decades, the number of spousal murders has not gone down, Interval House executive director Clare Freeman pointed out Sunday. Hamilton Spectator, A1

*** When tough is not smart**
An opinion piece states, "The Harper government's omnibus crime bill suggests that judges should be encouraged to give harsher sentences "to deter the young person from committing offences." The intention is to "reduce barriers to custody for violent and repeat young offenders" and to encourage the use of adult sentences for youths.... There are three problems with the suggestion that offending by youths (or adults) can be reduced by imposing harsher sentences. First, decades of research has demonstrated that harsher sentences for youths (or adults) do not reduce reoffending. Nor would harsher sentences deter others. These are not ideological statements; they are based on evidence from numerous studies. The results are quite consistent: one cannot punish away crime..." Toronto Star, A17

PUBLIC SERVICE / FONCTION PUBLIQUE

Public service muscles up for 'fight of our lives'
If you were headed for a brawl - maybe you would call it the "fight of your life" - you might want to look for a tough friend to back you up as you head for that showdown in the schoolyard. Muscle up, if you will. That's precisely what professionals in Canada's public service did this weekend, deciding to join the Canadian Labour Congress as they gird for battle with a Conservative government intent on cutting jobs. The move by the Professional Institute of the Public Service of Canada has, in effect, fired the first shot in the coming war. Toronto Star, A6

INTERNATIONAL / INTERNATIONAL

Dozens killed, missing in mudslides
Mudslides in western Colombia after days of heavy rain have killed at least 22 people and dozens are still missing, according to an updated official toll Sunday. Six bodies were found earlier in the day, bringing the death toll to 22, Sandra Calvo of the government's risk management division said, noting that 17 others were injured. About 70 people are still missing, according to local media, though officials could not confirm the figure. Vancouver Province, A12

*** Deadly attacks mar Muslim Eid celebrations in Damaturu - Hotels frequented by diplomats, politicians may be next, U.S. warns**
Nigeria marked the Muslim feast of Eid el-Adha amid fears and tears as the U.S. warned of possible new attacks after deadly blasts claimed by Islamists killed 150 people in the northeast of the country. The attacks on Friday in Damaturu were among the deadliest ever carried out by Boko Haram, an Islamist sect based in the north of Africa's most populous country. The U.S. embassy in Nigeria warned that the sect could next attack hotels and other targets in the capital Abuja during the Muslim holiday. Vancouver Sun, B5

OTHER / AUTRE

Occupiers vow to stay despite woman's death
Occupy Vancouver protesters say a young woman's death at the Vancouver Art Gallery site shouldn't be cause to force the closure of the three-week-long encampment. The woman, identified online as 23-year-old Ashlie Gough of Victoria, was found unresponsive in her tent Saturday afternoon from a rumoured drug overdose. Police said the death is not considered suspicious. After news of the woman's death broke, Mayor Gregor Robertson said he had asked city manager Penny Ballem to find a way to force the protesters from the makeshift tent city, calling it unsafe. National Post, A5; * L'Acadie Nouvelle; * La Voix de L'Est,

*** Canada-U.S. summit eyes common issues**
Given the wide range of issues and interests common to both the Canadian and U.S. securities industries, a joint conference between the two national organizations that represent them was long overdue. In early October, it took place at a conference convened in New York by the Investment Industry Association of Canada (IIAC) and its U.S. sister organization, the Securities Industry and Financial Markets Association (SIFMA). National Post, JV1

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-06-11 9:06 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
November 6, 2011 / le 6 novembre 2011

MINISTER / MINISTRE

Group targets Rwanda hero
Members of the Rwandan community in Toronto are calling on Ottawa to stop a well-known activist who inspired the hit movie Hotel Rwanda -- and is now accused of being a "genocide denier" -- from visiting Canada later this month. Officials of the Rwandese Canadian Association of Greater Toronto have asked **Public Safety Minister Vic Toews** and Immigration Minister Jason Kenney to refuse a visa or ban the entry of Paul Rusesabagina, the inspiration behind the award-winning movie depicting the 1994 genocide in Rwanda in which more than 800,000 Tutsis were slaughtered by the Hutu majority. Toronto Sun, 18

That's no way to treat a visitor
Don Shellenberger came to Ottawa from Atlanta late last month to take in the sights, the fall weather - "It got really cold, which was nice" - and, if you can believe it, the Transitway. He figures he spent much of his four-day visit riding OC Transpo buses around the city. "I sort of have this weird thing about public transit, and the (Transitway) seemed interesting," he says. And in case Andy Haydon is wondering, Schellenberger, an environmental protection manager for the Georgia state government, loves the busway, a Haydon legacy. He even took a ride on the O-Train, but it sounds as if he'll take a pass if he visits again. If he ever does return, the Canadian Border Services Agency should think of having two Ottawa airport customs officers on hand to apologize for the treatment they gave him on Oct. 22. We know CBSA employees are not paid to be tourism ambassadors, but is the buffoonery really necessary when they decide to play heavy with visitors? . . . The Public Citizen contacted the CBSA and the office **of Public Safety Minister Vic Toews** on Thursday for comment. They said they would look into the matter. Shellenberger also filed a complaint with the CBSA. Ottawa Citizen, B1

Obliged to out themselves?
When Glen Murray told his mother he was gay, she collapsed on the living room floor of their Montreal home in a flood of tears and begged him not to tell his father. It was the 1970s, and homophobia was commonplace. Murray knew his father - who once told him that he used to beat up gay people - wouldn't react well to the news, but the then 17-year-old said he never expected to be disowned . . . Recently, as friends and family of Hubley were laying the 15-year-old to rest in Ottawa, a group of Conservative MPs, including **Public Safety Minister Vic Toews**, Foreign Affairs Minister John Baird and Public Works Minister Rona Ambrose, created a YouTube video offering bullied teenagers a message of support. Edmonton Journal, B1

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

BUG-OUT BAGS: What to grab when disaster strikes
A hurricane is coming, terrorists are blowing up the block or bad guys are parachuting into the backyard. You have to get the hell out of Dodge, right now. What do you grab to go? "Bug-out bags" are backpacks full of gear that will keep you secure for at least 72 hours when it all hits the fan and they are a central commandment of survivalists. Toronto Sun, 26

CYBER SECURITY / CYBERSÉCURITÉ

Anonymous busts pervs: Hacktivist group releases IPs of online patrons

A notorious hacktivist group's war against those who access child porn online continues. Late last month, Anonymous claimed that it crashed several child porn sites and shamed those who allegedly patronized them. Late last week, Anonymous released the IP addresses of nearly 200 visitors to child porn sites, using information collected from the sites it had shut down. Toronto Sun, 25

Virus threats on the rise
Virus and malware attacks against organizations have increased because of employees using Facebook, Twitter, LinkedIn and other social media in the workplace, according to a global study. Of the 4,640 organizations surveyed by the Ponemon Institute, a research firm, more than half said these attacks grew as a result of workers using social networks. The Province, A41

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

Nova Scotia remains could be those of missing teen
Police in Nova Scotia have found human remains at a property in Healthbell, a community in Pictou County. Officers found the remains early Saturday afternoon during a search in the ongoing investigation into the disappearance of missing teen Amber Kirwan, 19. Winnipeg Sun, 10; Chronicle-Herald

Hi-tech crime busting
It's a parent's worst nightmare. Last February, notorious sex offender John Francis Dionne swiped a 10-year-old girl shopping with her dad from a Calgary mall and headed in a hurry toward Airdrie in his van. An RCMP officer spotted the vehicle and pulled it over for speeding. But since nothing appeared out of the ordinary, Dionne was issued a ticket and drove away. Fortunately , Dionne dropped the girl off unharmed at a McDonald's restaurant, but the incident raised concerns about the information the Mountie -- a 25-year veteran -- had at the time of the traffic stop. Edmonton Sun, 4

Critics fear arrival of big brother
In order to come up with the Talon framework, the province has looked at police database models used in other regions of Canada, including B.C. PRIME-BC (Police Records Information Management Environment for British Columbia) was introduced in February 2003 as a better way to track serial killers, sex offenders and other criminals. It connects every municipal police department and RCMP detachment throughout the province, along with access to information about criminals and crimes to all police agencies. Edmonton Sun, 5

Oakland violence serves as warning to both sides
Over a week ago, an injured Occupy protester was carried by his colleagues through a haze of teargas in downtown Oakland after having his skull fractured during a dustup with police. It took seconds for the image of 26-year-old Scott Olsen-- blood running down his face, his unmoving eyes staring straight ahead like two small, wet stones--to go viral . . . Councillor Giorgio Mammoliti agreed, saying a balance must be struck between upholding the law and maintaining order -- despite, he said, occupiers now "breaking four or five bylaws" with what they're doing in the park. "If we start rattling their cage, they're going to start breaking the windows of all those merchants (nearby)," said Mammoliti, alluding to the damage done to downtown Toronto during the G20 Summit riots in June 2010. Toronto Sun, 7

Police chief beset by murders: Rod Knecht must deal with worst homicide rate in Canada
New police Chief Rod Knecht came to Edmonton with a plan. "I was told early in my career by a very wise supervisor, 'When you move to a new location, keep your ears and eyes open and your mouth shut for six months,' " Knecht says."That was very good advice. It served me very well in the past. I came here and I was going to employ that same strategy, but as you know, about six weeks into being here the honeymoon was over." Edmonton Journal, A1

Goodbye and good riddance to long gun registry
An editorial piece states, "One sunny afternoon in early fall, a bunch of my neighbours were standing around watching a sick raccoon die on somebody's front lawn. In the old pre-gun registry days, someone would have gone home, got a shotgun or .22 and put the poor creature out of its misery. But, as one said to me, his gun wasn't registered and he didn't want to be seen with it. Someone might call the cops or a cruiser might happen by. That, in a nutshell, is what's wrong with the gun registry: It makes criminals out of perfectly ordinary people doing nothing wrong, while it makes near-criminals out of those who have registered..." Toronto Sun, 31

City aims to identify at-risk neighbourhoods
Imagine if a simple walk around the block could help you predict whether your neighbourhood was at risk of becoming a crime magnet. It sounds like something out of Minority Report, the Hollywood movie where police could peer into the future to stop crimes before they happened. But the idea of being able to prevent crime by identifying certain warning signs in a community is a strategy Calgary is working on now. Calgary Herald, B3

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Bigotry keeps Roma on the run: Refugees describe the discrimination, intimidation and violence that forced them to flee their native Hungary
An opinion piece states, "...Jozsef and Timea's IRB hearing was on Feb. 16, 2011. They were not successful. Jozsef tried to tell the judge he had seen terrible things while travelling to Roma areas with Viktoria Mohacsi, that he could not have endured another beating. He wanted the judge to see the Gyongyospata documentary but he felt the judge had already made up his mind. Their application was rejected on March 19. The chief reason: Hungary is a democracy. Their appeal was turned down in August. Jozsef still holds onto the hope that his "preremoval risk assessment application" to Canada's Border Services will keep him safe. I am not so optimistic..." Toronto Star, A15

INTERNATIONAL / INTERNATIONAL

Canadian jailed in Indonesia
A Canadian engineer with ties to Vancouver has been imprisoned in Indonesia, accused of corporate espionage. Canada's foreign affairs department and a UN organization that deals with corporate human rights violations are looking into the case of Rick van Lee, who was imprisoned following a dispute with his employer. Times Colonist, A7

N.S. woman jailed in border seizure
A federal judge in Maine has sentenced a 23-year-old Canadian woman to 18 months in prison on weapons and drug charges. The U.S. Attorney's Office says Janaya Crawley of Nova Scotia was sentenced Friday in U.S. District Court in Bangor on charges of being a drug addict in possession of a firearm and possessing a controlled substance. Chronicle-Herald, A3

Canadian Forces returning home from Libya
Members of the Royal Canadian Air Force have begun their return from Libya, where they flew missions aiding civilians who were in revolt against former dictator Moammar Gadhafi. Canada took a major role in the UN-mandated operation to protect the people of Libya from the Gadhafi regime while also imposing an arms embargo and a no-fly zone. Edmonton Journal, A8; Toronto Star; Chronicle-Herald

Militants canadiens battus en Israël
Des organisateurs canadiens d'une expédition qui tentait de forcer le blocus naval sur la bande de Gaza affirment que certains militants ont été tabassés lorsque les troupes israéliennes ont arraisonné leur navire, vendredi. «Selon les dernières nouvelles, les militants sont toujours détenus et au moins certains d'entre eux ont été battus en refusant de quitter volontairement le navire», a affirmé l'un des porte-parole du groupe de militants, Dylan Penner. Le Soleil, 23; Edmonton Sun; Calgary Herald; Toronto Star

Terror attacks from Islamist sect in Nigeria kill 150
At least 150 people died in a "heinous" wave of gun and bomb attacks Friday in northern Nigeria that were claimed by the Islamist Boko Haram sect. President Goodluck Jonathan condemned the assaults, which officials said included at least five suicide bomb blasts, and "directed security agencies to ensure the arrest of perpetrators of these heinous acts," said a statement from his spokesman, Reuben Abati. The Province, D27

OTHER / AUTRE

INSIDE THE OCCUPIED PARK
Waking up in a down-town park on a cold November morning, my breath visible and a thin crust of frost on my tent, I admittedly wished momentarily I was covering the Occupy movement in L.A. rather than T-T-T-Toronto. But I quickly remind myself that I'm there to peel back the curtain and take a closer look at what's happening beneath the surface in St. JamesPark-- the good, the bad and the ugly. Toronto Sun, 4

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

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-05-11 8:59 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne - First Part / Première partie

Daily Media Summary / Revue de presse quotidienne
First Part / Première partie
November 5, 2011 / le 5 novembre 2011

MINISTER / MINISTRE

Senate wants two-tier pardon fees for ex-cons
The Senate is calling on the government to consider a two-tiered structure for pardon user fees despite approving a massive hike aimed at covering new costs associated with processing. **Public Safety Minister Vic Toews** has proposed a $631 application fee, up from $150. It's meant to cover a spike in processing costs after Bill C-23 took effect in June 2010 and increased the number of factors the National Parole Board must consider before issuing a pardon. Winnipeg Free Press, A24

Gun registry useless? That's not what police say
An opinion piece states, "…Statistics Canada released a study recently saying the number of homicides in Canada in 2010 hit its lowest level since the 1960s. And whether it's related or not, since the registry opened its doors, homicides involving long guns have tumbled by more than half. But don't tell the minister that. He's not listening. ***"The registry has done nothing to keep guns out of the hands of criminals,"*** **Public Safety Minister Vic Toews** said. Victims disagree…" The Guardian, A15

Croupir en prison
Un article d'opinion déclare, «…**Le ministre de la Sécurité publique, Vic Toews**, a affirmé que les coûts engendrés par le projet de loi C-10 sont de deux milliards de dollars sur cinq ans. Selon le Globe and Mail, le directeur parlementaire du budget, Kevin Page, estime plutôt que le gouvernement fédéral devra débourser un milliard de dollars supplémentaires par année pour faire fonctionner le système carcéral fédéral…» L'Acadie Nouvelle, 12

Public figures urged to come 'out'
When Glen Murray told his mother he was gay, she collapsed on the living room floor of their Montreal home in a flood of tears and begged him not to tell his father. It was the 1970s, and homophobia was commonplace. Murray knew his father, who once told him that he used to beat up gay people, wouldn't react well to the news, but the then-17-year-old said he never expected to be disowned . . . Recently, as friends and family of Hubley were laying the 15-year-old to rest in Ottawa, a group of Conservative MPs, including **Public Safety Minister Vic Toews**, Foreign Affairs Minister John Baird and Public Works Minister Rona Ambrose, created a YouTube video offering bullied teenagers a message of support. Vancouver Sun, B3

EMERGENCY MANAGEMENT / GESTION DES MESURES D'URGENCE

BUG-OUT BAGS: What to grab when disaster strikes
A hurricane is coming, terrorists are blowing up the block or bad guys are parachuting into the backyard. You have to get the hell out of Dodge, right now. What do you grab to go? "Bug-out bags" are backpacks full of gear that will keep you secure for at least 72 hours when it all hits the fan and they are a central commandment of survivalists. Winnipeg Sun, 7

What to do with flood victims
An opinion piece states, "Careful planning needs to go into deciding where Manitoba First Nations affected by flooding will go once their time in Winnipeg ends. Aboriginal Affairs and Northern Development Canada says the cost for hotels and expenses for flood evacuees is now at $23 million. Tragically, about 2,100 individuals from eight First Nation haven't been able to return to their homes…" Winnipeg Sun, 11

Lament from a distant shore
An opinion piece states, “Those of us Manitobans who lived near the shores of Lake Manitoba are Canada's newest victims of their government's deliberate action to deprive them of the use of their property and their livelihoods. To add insult to injury, this same government tells the rest of its citizenry they are taking good care of flood victims and they are being compensated for their losses…” Winnipeg Free Press, J1

Swine flu cases in U.S. are mild, but have mutation
Two new cases of human infection with a flu virus that has been sporadically jumping to people from pigs have been spotted in the United States, the Centers for Disease Control reported Friday. The new cases, in Maine and Indiana, bring to seven the number seen in the United States since July. To date, Canada has seen no infections with this virus, the National Microbiology Laboratory said. Hamilton Spectator, A11

L'OMS prône la vigilance
L'Organisation mondiale de la santé (OMS) affirme que le nombre de cas de grippe résistante aux médicaments est encore faible et qu'il n'y a pas, actuellement, de risque majeur pour la santé publique. L'organisation indique toutefois que des groupes de cas récents sont un rappel que les pays devraient être à l'affût des cas de grippe qui ne réagissent pas aux médicaments antigrippaux oseltamivir, zanamivir et peramivir. Le Nouvelliste, 46

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Eritrea's 'EXTORTION'
The government of Eritrea, which the United Nations accuses of supplying a long list of armed groups, including the al-Qaeda affiliate AlShabab, has been raising money in Canada by taxing Eritrean-Canadians, interviews and documents show. The 2% "diaspora tax" is collected by the Consulate-General of Eritrea in Toronto and helps explain how one of the world's least developed countries raises revenues as it trains, arms and finances rebels from Sudan to Somalia. National Post, A1

CYBER SECURITY / CYBERSÉCURITÉ

Malware myopia
In September, researchers discovered a cunning strain of malware, dubbed the Lurid Downloader, that has been systematically and silently stealing data from carefully targeted government computers in 61 countries. The discovery was made by Trend Micro, a Tokyo-based computer security company, which identified the invader as a version of a well-known strain of malware that exploits vulnerabilities in the popular programs Adobe Reader and Microsoft Office. Vancouver Sun, D4

When danger lurks in Heidi Klum
An appetite for entertainment can be your ticket to - a fraudster's website that will try to steal personal information or inflict viruses, spyware and spam on your computer. Type the name of your favorite celebrity on an internet search engine and you're presented with an array of websites promising news or images of the star. Many sites are legit; others are run by scammers. Waterloo Region Record, C7

Cyberschool enrolment secure move for students
Jordan Jueckstock and his wife Jessica applied to the University of Tulsa's Cyber Corps Program after receiving an email from a professor with the subject line "Do you want to be a MacGyver?" References to the TV secret agent aside, the Jueckstocks got full scholarships and a stipend to attend the two-year master's program, paid by the U.S. government. In return, the former software developers, both in their mid-20s, must work for a federal agency for at least two years after graduation. Vancouver Sun, B10

Are CIA's 'vengeful librarians' following you online?
In an anonymous industrial park in Virginia, in an unassuming brick building, the CIA is following tweets - up to 5 million a day. At the agency's Open Source Center, a team known affectionately as the "vengeful librarians" also pores over Facebook, newspapers, TV news channels, local radio stations, internet chat rooms - anything overseas that anyone can access and contribute to openly. Waterloo Region Region, A11

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L’APPLICATION DE LA LOI

RCMP sets aside $4M for Olympic-related lawsuits
The RCMP has set aside $4 million to deal with 2010 Olympics-related lawsuits, according to Treasury Board documents tabled in the House of Commons. The money is for a potential liability relating to "vendor contracts and loss of business during the Vancouver Olympics in 2010," according to the 2011-12 supplementary estimates. Edmonton Journal, A12

Go to court to block bill, province urged
As tensions mount between Quebec and Ottawa over the federal government's proposed law to abolish the longgun registry, a wide-ranging group of activists and politicians gathered at Dawson College on Friday to urge the province to take legal action to save the registry and its vast database. Montreal Gazette, A7; Calgary Sun

Canada Revenue Agency probe must go deeper, NDP says
The investigation into alleged corruption at the Canada Revenue Agency must cover the entire country to clear suspicions about the integrity of the tax-collection agency, the opposition says. The government responded that it is fully co-operating with the RCMP, which recently expanded a probe into allegations concerning the CRA's offices in Montreal to the rest of its operations in Quebec. Globe and Mail, A8; Ottawa Sun

Manitoba: Boy, 9, fatally shot by brother on reserve
A nine-year-old boy died when he was shot by his older brother Thursday night on the Sagkeeng First Nation, RCMP said Friday. The boy was shot once in the upper body by his 14-year-old brother inside his family's home just before 7 p.m. Thursday, RCMP said. He was pronounced dead on arrival at hospital. Ottawa Citizen, A3; Globe and Mail; National Post; Edmonton Sun

Weapons must be kept unloaded, according to strict rules
Canada has strict gun storage regulations, which are aimed at preventing the kind of tragedy that occurred Thursday evening at Manitoba's Sagkeeng First Nation. Under the federal Firearms Act, individual gun owners must keep the weapons unloaded and in such a way that they're not easily accessible to ammunition. And that goes for even unrestricted firearms. Winnipeg Sun, 3

One of these jerseys costs $375 and the other costs $40
It is right and good to revel in the satisfaction of a job done well. Which is approximately what those charged with stemming the flow of counterfeit merchandise at the Vancouver 2010 Olympics did as they tracked the lower-than-feared presence of ersatz goods during that golden February fortnight. "Then, a few days after the Games end, the phone rings," said Lorne Lipkus, a Toronto-based lawyer whose firm led the Vancouver Olympic committee's anti-counterfeiting efforts. It was a contact at the RCMP's Border Integrity unit reporting a seizure of "a few hundred" Team Canada hockey jerseys at a B.C. postal terminal. Globe and Mail, S1

Heroin issue worth revisiting
An opinion piece states, “The Cancer Society charged that morphine was as good as heroin in most cases. But what if you were not one of those "most cases?" And some doctors publicly criticized the use of heroin, while admitting they had never used it. The RCMP worried about security problems if heroin was legalized. So I travelled to England and was told by Scotland Yard this was not a problem…” StarPhoenix, E7

Flash of buffoonery: Cops investigate laser being pointed at airplane near Fort McKay
Pointing lasers at air-craft is no laughing matter, say Mounties after someone pointed a laser from Suncor's operations near Fort McKay at an airplane Thursday night. Wood Buffalo RCMP say a witness onboard a small commuter plane travelling from Fort Chipewyan to Fort McMurray noticed a green laser that was pointed at the aircraft sometime around 8:15 p.m. Edmonton Sun, 5

Gun shop owner loses licence, faces trafficking charge
A Winnipeg gunsmith has been slapped with two dozen criminal charges following a raid earlier this week on his Fort Garry shop that netted more than 400 guns. As a result of the largest firearms seizure in Winnipeg since 2002, Sean Beiko, the 38-year-old owner of Moreguns Supply, has been charged with 24 weapons-related charges including firearms trafficking, possessing restricted and prohibited weapons and accessories, improper storage, and possessing at least one gun with an altered serial number. Winnipeg Sun, 13; Edmonton Journal

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

Dignity of the murdered
An editorial piece states, “The question before the Missing Women Inquiry in Vancouver is whether police and prosecutors in effect allowed the killing of women to go on and on because they held dismissive or discriminatory

attitudes toward prostitutes and drug addicts. The inquiry, headed by Wally Oppal, a former appeal court judge and a former provincial attorney-general, has been beset by controversy. But it may still prove worthwhile if it gets to the bottom of why police seemed unable to track the stories circulating in the Downtown Eastside of a notorious pig farm - and if it airs the stories of the murdered women that have not been told yet in a public forum…" Globe and Mail, F8

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

Silent flood of Roma: Hungarians top refugee claims in Canada, drawing skepticism of need
When Jason Kenney made a surprise appearance at a roundtable with Roma community leaders and asylum-seekers last weekend, the Citizenship and Immigration Minister wanted answers: What is driving the record, silent flood of Hungarian Roma refugee claimants streaming into Canada, and why are so many ultimately abandoning or withdrawing their claims? . . . A record number of Hungarian refugee claimants arrived at Pearson International Airport in September and October, with an unprecedented 91 asylum-seekers landing in a single day on Oct. 26, according to data obtained from the Canada Border Services Agency. National Post, A6

Canada to let in 25,000 parents, grandparents
The federal government is making good on an election promise to repair Canada's broken family reunification system by boosting the number of parents and grandparents accepted into Canada, imposing a moratorium on new applications and introducing a new "supervisa" for extended visits. Ottawa Citizen, A5

INTERNATIONAL / INTERNATIONAL

Israelis board Canadian aid ship
A Canadian ship's effort to breach Israel's naval blockade of Gaza was quashed when Israeli forces boarded the vessel Friday, but activists say the setback won't discourage them from trying again. The Tahrir, which made a previous failed attempt to reach the blockaded Palestinian territory this summer, was intercepted two days after it left Turkey for Gaza. Waterloo Region Record, A5; Globe and Mail; London Free Press; Edmonton Journal

Engineer with ties to Vancouver jailed in Indonesia after employer accuses him of corporate espionage
A Canadian engineer with ties to Vancouver has been imprisoned in Indonesia accused of corporate espionage. Canada's foreign affairs department and a United Nations organization that deals with corporate human rights violations are looking into the case of Rick van Lee, who was imprisoned following a dispute with his employer, one of the largest pulp and paper producers in Southeast Asia. Vancouver Sun, A4

Des milliers de soldats sollicités pour la sécurité
La présence de milliers de soldats britanniques sera requise sur les sites olympiques pendant les Jeux de Londres en 2012. Une étude de sécurité a démontré que les autorités pourraient avoir besoin de doubler le nombre de gardes dans les stades et autres sites olympiques. Les discussions avec le ministère de la défense sont amorcées, alors que des études ont suggéré que les 10000 agents de sécurité sous contrat pour les jeux ne seraient pas suffisants. Le Droit, 47

OTHER / AUTRE

Occupy Toronto walks in solidarity with Tibet
Occupy Toronto protesters joined forces with pro-Tibet demonstrators for a rally in front of the Chinese consulate. The event, which began at Occupy Toronto's headquarters at St. James Park at noon Friday, saw about 300 people march north to the consulate's St. George-Bloor Sts. area offices. Toronto Star, GT2

Social media spreads protest from Wall Street to world
This revolution is being Tweeted. Occupy Wall Street has spread around the United States and Canada with keyboard-clicking quickness as participants tap into Twitter, Facebook and microblogging site Tumblr to call people to the streets to protest what they see as a broken global financial system. Calgary Herald, E2

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

Cameron, Bud

From: Cameron, Bud
Sent: November-04-11 2:36 PM
To: Pitcher Robert
Subject: Next week

can you prepare two slides on CEA; one with bullets about our involvement in GridEx as only GC participant; and one with a few bullets about our engagement with CAPP and the Anonymous event. This is for Windy because it is likely that Robert will ask about these things.

Bud Cameron, CD, MSc
Manager, Cyber Security Programs | Gestionnair, Programmes de sécurité cybernétique
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 +1 613-949-8317
Facsimile | Télécopieur +1 613-954-3097
Bud.Cameron@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Dincoy, Rana

From: Pitcher Robert
Sent: November-04-11 10:59 AM
To: Dincoy, Rana; Cameron, Bud; Beaudoin, Luc S
Cc: Klassen, Nathan; Bendelier, Kenneth
Subject: RE: Draft Weekly Summary for Execs
Attachments: PS-SP-#510655-v1-WEEKLY_SUMMARY_FOR_EXECS_-_WEEK_OF_OCTOBER_24__2011 - Rob Comments.DOC

Thanks Rana,

I'm busy today so I have to limit my comments to what I was able to come up with to this point. I got as far as the first Federal government and analysis section. You'll see my comments and changes in the attachment. Also, Flashes was spelled wrong in the disclaimer. That mistake has somehow manifested itself in the original draft. So in case it's missed.

Overall, I like what we're trying to do with this document, as the document has certainly improved since its inception. However, I still feel there's lots of room for improvement. The summary up front idea is good, and I see the point of moving the disclaimer to the back. However, I think it looks odd on a page by itself, suggest moving it up in line with the feedback comment.

I rewrote the one section on the federal government. As you can see, the tone I took is much different that the original. The information contained in this was misleading, and in my opinion, was not accurate. This was continued into the analysis section of that event as well. This is a critical mistake in my mind. Unless this was a detailed targeted attack using Gadaffi as a lure, then we can not say that. I looked at the email in question and it is labelled "Gadaffi love blood!". That in my experience, is not an advanced attack. I see other hints of similar mistakes in some of the following sections, but I don't have time to rewrite each one.

Here's some of the issue in my mind. I can write my analysis and articulate my understanding of each of these issues as it's what I've been dealing operationally for the past 5 to 6 years. If you don't fully understand the issue at hand, then it's possible to phrase this stuff in a way that is not accurate. What this process needs is a way to vet the information being presented by those that KNOW the information being analysed. And that is the issue. A process needs to be adapted that effectively marries the policy side with the technical side in the production of this report. And that's the challenge…

I do not feel this document is the best we can do. A lot of good work has been done on this to date, and I applaud the collective effort that got it to where it is today, and the leadership from Rana for pushing this task along. However, I know we can do better. If today is the deadline for getting this right, then we need to push that deadline out, as I don't' think we can resolve these issues by this afternoon.

Regards,
Robert Pitcher
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 949-8318
Fax/télécopieur: (613) 996-0995
Email/Courriel: Robert.Pitcher@ps-sp.gc.ca
Website/Site Internet: http://www.ps-sp.gc.ca

From: Dincoy, Rana
Sent: November 4, 2011 9:58 AM
To: Cameron, Bud; Beaudoin, Luc S
Cc: Klassen, Nathan; Bendelier, Kenneth; Pitcher Robert
Subject: Draft Weekly Summary for Execs
Importance: High

Hello,

please find attached the reference in RDIMS for the Weekly Summary, for your review and comments today. You have access rights to the document for reading. If you have specific suggestions, I suggest make your changes (in track changes please), save it as a different version, if you can, and let me know you have comments. If that doesn't work, save to a saved copy of that document or and just e-mail it to me.

Thanks guys!

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

Klassen, Nathan

From: Bendelier, Kenneth
Sent: November-04-11 8:01 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description: **Microsoft mum on Duqu fix in November.** "Microsoft said it is looking into a reported zero day vulnerability in Windows used by the Duqu malware to spread, but is not committing to a patch for the problem in time for November's scheduled update. "Microsoft is collaborating with our partners to provide protections for a vulnerability used in targeted attempts to infect computers with the Duqu malware," the company said in a statement attributed to a member of the company's Trustworthy Computing effort. "We are working diligently to address this issue and will release a security update for customers through our security bulletin process.""
Reference: http://threatpost.com/en_us/blogs/microsoft-mum-duqu-fix-november-110211

2. Item Description: **Microsoft announces workaround for the Duqu exploit**. "Microsoft have posted security advisory 2639658 to address the recently disclosed Windows kernel vulnerability (CVE-2011-3402) exploited by the Duqu malware. Microsoft has determined the flaw is in the processing of embedded True Type Fonts (TTFs)."
Reference: http://nakedsecurity.sophos.com/2011/11/04/microsoft-announces-workaround-for-the-duqu-exploit/
http://technet.microsoft.com/en-us/security/advisory/2639658

3. Item Description: **Web credential authority rebuked for 'poor' security**. "Microsoft, Google, and Mozilla will banish yet another web authentication authority from their software after learning that it issued secure sockets layer certificates that could be used to attack people visiting Malaysian government websites. Digicert Malaysia, an intermediate certificate authority that was certified by parent authority Entrust, issued 22 certificates with weak private keys and other serious deficiencies, the companies said. The lapses, which also included a failure to include revocation details and EKU, or extended key usage, designations, constituted a breach of obligations all CAs are required to follow to ensure the security of the SSL system. "There is no indication that any certificates were issued fraudulently, however, these weak keys have allowed some of the certificates to be compromised," Jerry Bryant, a spokesman in Microsoft's Trustworthy Computing group, wrote in a blog post. "The subordinate CA has clearly demonstrated poor CA security practices and Microsoft intends to revoke trust in the intermediate certificates."
Reference: http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/

4. Item Description: **Has your account been pwned? New website will tell you:** "Security researchers have set up a website that allows punters to check whether or not their email addresses have appeared in data dumps slurped from compromised databases. Hacking attacks on sites including Gawker and the network of Sony's gaming division have led on to the publication of hundreds of thousands of users' credentials online, sometimes (but not always) by activists at Anonymous."
Reference: http://www.theregister.co.uk/2011/11/03/pwnedlist/

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Klassen, Nathan

From: Cameron, Bud
Sent: November-04-11 7:53 AM
To: Klassen, Nathan; Dincoy, Rana
Subject: RE: Your feedback on the "overview" for this week's summary

let's meet after the 915 ops meeting.

From: Klassen, Nathan
Sent: November 3, 2011 3:11 PM
To: Dincoy, Rana
Cc: Cameron, Bud
Subject: RE: Your feedback on the "overview" for this week's summary

Hi Rana,

Txs for the opportunity to comment -- my suggestions are in the attached document. I will flip some ideas to you and Bud tomorrow (i.e. tying the weekly reports to the three strategic pillars identified in Canada's Cyber Security Strategy).
Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Dincoy, Rana
Sent: November 3, 2011 1:19 PM
To: Klassen, Nathan
Subject: Your feedback on the "overview" for this week's summary

What do you think of the overview for this week's summary? By the way, we're going to start having having a classified and an unclassified version of the weekly summary starting next week...

OVERVIEW:

- **Reported Incidents:**
  - Potential G20 related targeted attacks spoofing federal e-mail accounts
  - Compromised computers in a provincial government network
  - Canadian police personnel computer user information posted on a hacker website
  - Phishing reports where threat actors tried to lure computer users to their malicious web sites by pretending to be reputable Canadian companies in the financial and transport sector.
  - Compromised computers in energy, health and education organizations' networks
  - Intrusion attempts into a Canadian Internet Service Provider's core infrastructure
  - Recruiting "money mules" in Canada on-line
- **Threat Warnings:**
  - Hacker group Anonymous urging sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on Nov 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5.

- **Other CCIRC Products released:** An update to a previous Cyber Flash on security patches for Oracle products affecting Entrust functionality.
- **Noteworthy International News:** Japanese missions around the world victim of targeted cyber attacks; Chinese military suspected of hacking US satellites; Finland wants cyberwar weapons; Japanese defence contractor hacked.

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

Klassen, Nathan

From: Pitcher Robert
Sent: November-03-11 3:24 PM
To: Klassen, Nathan
Subject: RE: Your feedback on the "overview" for this week's summary

Cool man. Nice way to copy bud and leave room for your ideas in a follow up email.

From: Klassen, Nathan
Sent: November 3, 2011 3:18 PM
To: Pitcher Robert
Subject: FW: Your feedback on the "overview" for this week's summary

FYI

From: Klassen, Nathan
Sent: November 3, 2011 3:11 PM
To: Dincoy, Rana
Cc: Cameron, Bud
Subject: RE: Your feedback on the "overview" for this week's summary

Hi Rana,

Txs for the opportunity to comment -- my suggestions are in the attached document. I will flip some ideas to you and Bud tomorrow (i.e. tying the weekly reports to the three strategic pillars identified in Canada's Cyber Security Strategy).
Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Dincoy, Rana
Sent: November 3, 2011 1:19 PM
To: Klassen, Nathan
Subject: Your feedback on the "overview" for this week's summary

What do you think of the overview for this week's summary? By the way, we're going to start having having a classified and an unclassified version of the weekly summary starting next week...

OVERVIEW:

- **Reported Incidents:**
  - Potential G20 related targeted attacks spoofing federal e-mail accounts
  - Compromised computers in a provincial government network
  - Canadian police personnel computer user information posted on a hacker website
  - Phishing reports where threat actors tried to lure computer users to their malicious web sites by pretending to be reputable Canadian companies in the financial and transport sector.
  - Compromised computers in energy, health and education organizations' networks

- Intrusion attempts into a Canadian Internet Service Provider's core infrastructure
- Recruiting "money mules" in Canada on-line

- **Threat Warnings:**
  - Hacker group Anonymous urging sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on Nov 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5.
- **Other CCIRC Products released:** An update to a previous Cyber Flash on security patches for Oracle products affecting Entrust functionality.
- **Noteworthy International News:** Japanese missions around the world victim of targeted cyber attacks; Chinese military suspected of hacking US satellites; Finland wants cyberwar weapons; Japanese defence contractor hacked.

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

Klassen, Nathan

From: Klassen, Nathan
Sent: November-03-11 3:18 PM
To: Pitcher Robert
Subject: FW: Your feedback on the "overview" for this week's summary
Attachments: Nate's comments -- What do you think of the 'overview' for this week's summary.doc

FYI

From: Klassen, Nathan
Sent: November 3, 2011 3:11 PM
To: Dincoy, Rana
Cc: Cameron, Bud
Subject: RE: Your feedback on the "overview" for this week's summary

Hi Rana,

Txs for the opportunity to comment -- my suggestions are in the attached document. I will flip some ideas to you and Bud *tomorrow* (*i.e. tying the weekly reports to the three strategic pillars identified in Canada's Cyber Security Strategy*).
Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca

From: Dincoy, Rana
Sent: November 3, 2011 1:19 PM
To: Klassen, Nathan
Subject: Your feedback on the "overview" for this week's summary

What do you think of the overview for this week's summary? By the way, we're going to start having having a classified and an unclassified version of the weekly summary starting next week...

OVERVIEW:

- **Reported Incidents:**
  - Potential G20 related targeted attacks spoofing federal e-mail accounts
  - Compromised computers in a provincial government network
  - Canadian police personnel computer user information posted on a hacker website
  - Phishing reports where threat actors tried to lure computer users to their malicious web sites by pretending to be reputable Canadian companies in the financial and transport sector.
  - Compromised computers in energy, health and education organizations' networks
  - Intrusion attempts into a Canadian Internet Service Provider's core infrastructure
  - Recruiting "money mules" in Canada on-line
- **Threat Warnings:**
  - Hacker group Anonymous urging sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on Nov 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5.

- **Other CCIRC Products released:** An update to a previous Cyber Flash on security patches for Oracle products affecting Entrust functionality.
- **Noteworthy International News:** Japanese missions around the world victim of targeted cyber attacks; Chinese military suspected of hacking US satellites; Finland wants cyberwar weapons; Japanese defence contractor hacked.

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

What do you think of the overview for this week's summary? By the way, we're going to start having having a classified and an unclassified version of the weekly summary starting next week...

SUMMARY~~OVERVIEW~~:

- -**Noteworthy International News:** Japanese missions around the world victim of targeted cyber attacks; Chinese military suspected of hacking US satellites; Finland wants cyberwar weapons; Japanese defence contractor hacked.
    - So what? – i.e. what did CCIRC, GoC, international community do about it?

- **Threat Warnings:** Hacker group Anonymous urging sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on Nov. 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov. 5.
    - So what? – i.e. what is / did CCIRC, GOC, international community do about it?

- **Reported Incidents: (1)** A federal department received a targeted G20 email containing malicious software.
    - ~~***Reported Incidents*:**~~
    - ~~Potential G20 related target~~(2)~~ed attacks spoofing federal e-mail accounts~~
- ~~Compromised computers in a p~~ Provincial government computer networks compromised; (3) Canadian energy, health, and education networks compromised; (4) Attempts to break into a Canadian internet service provider's core infrastructure; and (5) Individuals tried to lure Canadians to malicious websites (specifically in the financial and transport sectors).

So what? i.e. what are the impacts to Canada? What did CCIRC / GoC / international community do about it? ~~network~~

- ~~Canadian police personnel computer user information posted on a hacker website~~
- ~~Phishing reports where threat actors tried to lure computer users to their malicious web sites by pretending to be reputable Canadian companies in the financial and transport sector.~~
- ~~Compromised computers in energy, health and education organizations' networks~~
- ~~Intrusion attempts into a Canadian Internet Service Provider's core infrastructure~~
- ~~Recruiting "money mules" in Canada on line~~

~~Threat Warnings:~~

- ~~Hacker group Anonymous urging sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on Nov 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5.~~

Formatted ... [1]
Formatted ... [2]
Formatted ... [3]
Formatted: Bullets and Number ... [4]
Formatted ... [5]
Formatted ... [6]
Formatted: Bullets and Number ... [7]
Formatted ... [8]
Formatted ... [9]
Formatted ... [10]
Formatted ... [11]
Formatted ... [12]
Formatted ... [13]
Formatted ... [14]
Formatted ... [15]
Formatted ... [16]
Formatted ... [17]
Formatted ... [18]
Formatted ... [19]
Formatted ... [20]
Formatted ... [21]
Formatted ... [22]
Formatted ... [23]
Formatted ... [24]
Formatted: Bullets and Numbe ... [25]
Formatted ... [26]
Formatted ... [27]
Formatted ... [28]
Formatted ... [29]
Formatted ... [30]
Formatted ... [31]
Formatted ... [32]
Formatted ... [33]
Formatted ... [34]
Formatted ... [35]
Formatted: Bullets and Numbe ... [36]
Formatted ... [37]
Formatted ... [38]
Formatted ... [39]
Formatted ... [40]
Formatted ... [41]
Formatted ... [42]
Formatted ... [43]
Formatted ... [44]
Formatted ... [45]

- **Other CCIRC Products released:** An update to a previous Cyber Flash on security patches for Oracle products affecting Entrust functionality.
- ~~**Noteworthy International News:** Japanese missions around the world victim of targeted cyber attacks; Chinese military suspected of hacking US satellites; Finland wants cyberwar weapons; Japanese defence contractor hacked.~~

Formatted: Underline

Formatted: Bulleted + Level: 1 + Aligned at: 0.63 cm + Tab after: 1.27 cm + Indent at: 1.27 cm

Formatted: Bullets and Numbering

Comment [T1]: I don't understand

Formatted: Default Paragraph Font, Font color: Black

Page 1: [1] Formatted	Template	03/11/2011 1:48:00 PM

Tab stops: Not at 7.62 cm + 15.24 cm

Page 1: [2] Formatted	Template	03/11/2011 1:55:00 PM

Underline

Page 1: [3] Formatted	Template	03/11/2011 1:48:00 PM

Bulleted + Level: 1 + Aligned at: 0.63 cm + Tab after: 1.27 cm + Indent at: 1.27 cm, Tab stops: Not at 7.62 cm + 15.24 cm

Page 1: [4] Change	Template	03/11/2011 1:48:00 PM

Formatted Bullets and Numbering

Page 1: [5] Formatted	Template	03/11/2011 1:49:00 PM

Tab stops: Not at 7.62 cm + 15.24 cm

Page 1: [6] Formatted	Template	03/11/2011 1:49:00 PM

Bulleted + Level: 2 + Aligned at: 1.9 cm + Tab after: 2.54 cm + Indent at: 2.54 cm, Tab stops: Not at 7.62 cm + 15.24 cm

Page 1: [7] Change	Template	03/11/2011 1:54:00 PM

Formatted Bullets and Numbering

Page 1: [8] Formatted	Template	03/11/2011 2:11:00 PM

Indent: Left: 0.63 cm, Tab stops: 1.27 cm, List tab + Not at 2.54 cm

Page 1: [9] Formatted	Template	03/11/2011 2:10:00 PM

Underline

Page 1: [10] Formatted	Template	03/11/2011 2:01:00 PM

Font: Italic

Page 1: [11] Formatted	Template	03/11/2011 1:57:00 PM

Font: (Default) Times New Roman

Page 1: [12] Formatted	Template	03/11/2011 1:57:00 PM

Font: 12 pt

Page 1: [13] Formatted	Template	03/11/2011 2:13:00 PM

Font: Bold, Underline

Page 1: [14] Formatted	Template	03/11/2011 2:56:00 PM

Font: Not Bold

Page 1: [15] Formatted	Template	03/11/2011 2:56:00 PM

Font: Not Bold

Page 1: [16] Formatted	Template	03/11/2011 2:56:00 PM

Font: Not Bold

Page 1: [17] Formatted	Template	03/11/2011 2:56:00 PM

Font: Not Bold

Page 1: [18] Formatted	Template	03/11/2011 2:13:00 PM

Font: Bold, Underline

Page 1: [19] Formatted	Template	03/11/2011 1:57:00 PM

Font: 12 pt, Bold

Page 1: [20] Formatted	Template	03/11/2011 2:01:00 PM

Font: Italic

Page 1: [21] Formatted	Template	03/11/2011 2:14:00 PM

Indent: Left: 0.63 cm, Bulleted + Level: 4 + Aligned at: 5.08 cm + Tab after: 5.71 cm + Indent at: 5.71 cm, Tab stops: 1.27 cm, Centered + Not at 5.71 cm + 7.62 cm

Page 1: [22] Formatted	Template	03/11/2011 3:05:00 PM

Indent: Left: 0.63 cm

Page 1: [23] Formatted	Template	03/11/2011 3:04:00 PM

Font: (Default) Times New Roman

Page 1: [24] Formatted	Template	03/11/2011 3:04:00 PM

Bulleted + Level: 2 + Aligned at: 2.54 cm + Tab after: 3.17 cm + Indent at: 3.17 cm, Tab stops: 1.27 cm, Centered + Not at 7.62 cm

Page 1: [25] Change	Template	03/11/2011 3:04:00 PM

Formatted Bullets and Numbering

Page 1: [26] Formatted	Template	03/11/2011 3:04:00 PM

Indent: Left: 0 cm, First line: 0 cm

Page 1: [27] Formatted	Template	03/11/2011 3:05:00 PM

Font: 12 pt

Page 1: [28] Formatted	Template	03/11/2011 3:05:00 PM

Font: (Default) Times New Roman

Page 1: [29] Formatted	Template	03/11/2011 3:05:00 PM

Font: 12 pt

Page 1: [30] Formatted	Template	03/11/2011 3:05:00 PM

Font: (Default) Times New Roman

Page 1: [31] Formatted	Template	03/11/2011 3:05:00 PM

Font: 12 pt

Page 1: [32] Formatted	Template	03/11/2011 3:05:00 PM

Font: (Default) Times New Roman

Page 1: [33] Formatted	Template	03/11/2011 3:05:00 PM

Font: 12 pt

Page 1: [34] Formatted	Template	03/11/2011 3:05:00 PM

Font: (Default) Times New Roman

Page 1: [35] Formatted	Template	03/11/2011 3:04:00 PM

Bulleted + Level: 2 + Aligned at: 2.54 cm + Tab after: 3.17 cm + Indent at: 3.17 cm, Tab stops: 1.27 cm, Centered + Not at 7.62 cm

Page 1: [36] Change	Template	03/11/2011 1:59:00 PM

Formatted Bullets and Numbering

Page 1: [37] Formatted	Template	03/11/2011 3:05:00 PM

Font: 12 pt

Page 1: [38] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Font: (Default) Times New Roman

Page 1: [39] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Font: 12 pt

Page 1: [40] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Font: Not Bold

Page 1: [41] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Font: (Default) Times New Roman

Page 1: [42] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Font: 12 pt

Page 1: [43] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Font: (Default) Times New Roman

Page 1: [44] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Indent: Left: 0 cm, First line: 0 cm

Page 1: [45] Formatted	**Template**	**03/11/2011 3:05:00 PM**

Font: 12 pt

Hayward, Jane

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-03-11 8:16 AM
To: * DGOPS-CCIRC; * Media Monitoring / Suivi des médias; * NCSD / DGCN; Allison, Catherine; Baker, William V.; Black, Dave; Bronson, Jessie; Carmichael, Julie; Champoux, Martin; Chomyshyn, Nicholas; Clarfield-Henry, Alexis; Crépeault, David; CSIS Media Monitoring; De Curtis, Laura; Dunn, John; Durand, Stéphanie; Duschner, Gabrielle; Dussault, Josée; Eke, Darren; Flack, Graham; Gilbert, Monica; Hannan, Andrew; Jager, Jennifer; Jarrette, Amy; Johnson, Mark; Leonidis, Nelly; MacKenzie, Sara; McAllister, Andrew; Panthaky, Jasmine; Patry, Line; Patton, Michael; RCMP Emerging Trends; Roberts, Shane; Robinson, N.; Slade, Nancy; Spendlove, Jim; Sreblowski, Myles; Stanfield, Charles; Stewart, Christena; Swift, Andrew; Tomlinson, Jamie; Verret, Scott; Wadasinghe, Cheryl; Woolridge, Theresa
Subject: Cyber Security Media Summary - 2011-11-03

Cyber Security Media Summary / Revue de presse sur la sécurité cybernétique
November 3, 2011 / le 3 novembre 2011

Print media

Child-porn site visitors revealed
The online "hacktivist" group Anonymous claimed on Wednesday to have published the Internet Protocol addresses of nearly 200 visitors to child pornography forums. Windsor Star, C2

Online media

Britain warns against state-sponsored cyberattacks
British Foreign Secretary William Hague warned foreign governments against state-sponsored cyberattacks Wednesday, hinting at a more confrontational approach if they don't stop. Hague, who was speaking at the close of a two-day conference on cybersecurity, was careful not to identify any countries by name, even when asked repeatedly about China. He told reporters in London that Britain had not hosted a "judgmental conference" where participants sat around pointing fingers. Associated Press

UK says governments' Internet power grab will fail
Attempts by China, Russia and others to gain more control over the Internet are doomed to failure, Britain said on Wednesday, after hosting a major conference on cyberspace that it said sent a clear signal to authoritarian governments. Reuters

UK cyber police imprison Ukranian malware masterminds
The Metropolitan Police's eCrime Unit has locked up two Ukranian cyber thieves who led "a systematic and highly sophisticated" 13-man operation that bilked nearly £3,000,000 from hundreds of unwitting victims. MyCE

Narcos, Meet Hackers: 2 'Anonymous' Groups Spar
One of the world's most secretive movements is taking aim at a just as clandestine mafia, right out in the open. Bloggers and tweeters claiming to belong to the hacker movement "Anonymous" say they plan to expose collaborators of Mexico's bloody Zetas drug cartel, even if some of them seem to have backed away from the plan out of fear. Associated Press

Phone scam on the rise, personal information at risk
If you haven't already received this phone call, chances are you will. The caller claims to work for Microsoft, or another computer company, and tells you something is wrong with your computer, but they can fix it. If you grant the caller access to your computer they might install malware allowing them to maintain control of and turn your computer into a "zombie". They add it to other zombie computers to create what's called a "Botnet", an army of computers secretly under the control of one person. The criminals that send out things like Nigerian letters, job scams and ads for porn sites and bogus

products now need your computer to stay in business. Through the botnet, criminals can remain untraceable and avoid getting shut down by internet providers for sending out billions of emails. CTV Calgary

Social botnet steals Facebook data with fake profiles
Researchers have demonstrated how a type of program called a socialbot can be used to harvest vast amounts of personal data from Facebook users. Socialbots are computer programs designed to mimic the activity of 'real' Facebook profiles, tricking users into making friends with them and mining their accounts for personal data. thinq_

After phishing crackdown, cyberattackers switch weapons
Aggressive action by large IT infrastructure and platform providers helped drive down the volume of phishing attacks over the past summer, but new threats continue to emerge and grow, according to recent threat trend reports. Government Computer News

Stuxnet Poses Thorny Issue For Cyberdefenders
A year ago, the existence of Stuxnet, the world's first cyber superweapon, first emerged. Many experts suspect the U.S. government had at least a hand in its creation. The development and use of offensive cyberweapons may create challenges for a nation's cyberdefenders — and could be a big policy issue in the nascent era of cyberwarfare. NPR

Mystery code spreads, but is it 'son of Stuxnet'?
The malicious computer code that bears similarities to Stuxnet — the worm that sabotaged Iran's nuclear program and prompted speculation about U.S. and Israel involvement — has now spread to eight countries, according to researchers, but there's still widespread disagreement on whether it is, in fact, the "son of Stuxnet." Washington Post

Duqu Malware Exploits Windows Zero-Day Kernel Bug, Attacks Via Microsoft Word Document
Researchers have concluded that the Duqu Trojan, the possible son the Stuxnet, is using a zero-day Windows kernel vulnerability to spread infection. Microsoft confirmed the kernel bug and is working on a fix. When an infected Word document is opened, Duqu can gain access to spread throughout the network. Symantec reported that includes spreading via a 'file-sharing C&C protocol' to infect computers that can't connect to the Internet. Network World

No quick patch to kill Duqu, turn back clock to when viruses weren't smarter than your apps
An opinion piece states, "…It didn't come from Windows (or Microsoft). Duqu probably came from the same people who wrote Stuxnet, or at least people with access to the Stuxnet source code, according to analyses by Symantec and the CrySyS Lab in Budapest, which discovered Duqu. Duqu shares a lot of code with Stuxnet and shares Stuxnet's flair for elegant, creative ways to exploit a weakness or find a way around it. It also shows the same effort to keep the virus covert for as long as possible while it does its work, often in very subtle ways, the reports said…" IT World

Hayward, Jane

From: Turner, Jessica on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: November-03-11 8:08 AM
To: * DMS/ RPQ
Subject: Daily Media Summary / Revue de presse quotidienne

Daily Media Summary / Revue de presse quotidienne
November 3, 2011 / le 3 novembre 2011

MINISTER / MINISTRE

Justice criminelle - Cinq provinces se joignent au Québec et à l'Ontario

Après le Québec et l'Ontario mardi, voici que cinq autres provinces demandent au gouvernement conservateur de les dédommager pour les coûts carcéraux qu'engendrera son projet de loi en matière de justice criminelle. Une sixième, le Nouveau-Brunswick, pourrait s'ajouter ce matin. C'est donc maintenant la quasi-totalité des provinces qui sont inquiètes des répercussions financières du projet de loi C-10. Les cinq autres récalcitrantes se rangent en deux catégories. Terre-Neuve et l'Ile-du-Prince-Édouard exigent qu'Ottawa paye la facture. La Colombie-Britannique, le Manitoba et la Nouvelle-Écosse se disent quant à eux inquiets des coûts et veulent «discuter» avec le gouvernement fédéral d'un dédommagement futur. A la période de questions, le NPD a interrogé à de nombreuses reprises le gouvernement sur cette question. **Le ministre de la Sécurité publique, Vic Toews**, a préféré répliquer que les citoyens voulaient être protégés. «***Il y a des bénéfices à mettre derrière les barreaux les violeurs et les criminels dangereux. Cela signifie que les Canadiens seront protégés***.» A une seule reprise **M. Toews** a fait référence à l'aspect financier de son projet de loi. Il a alors évoqué l'appui du Manitoba, la province qu'il représente. «***Ils sont prêts à payer le prix***», a soutenu **M. Toews**, apparemment non informé des revendications du ministre Swan. Le Devoir, A1

L'ambassade se désintéresse du retour de Khadr

Ce sont eux qui ont signé l'entente prévoyant le probable retour d'Omar Khadr au Canada, mais un an après sa signature, les ambassadeurs canadien et américain s'en lavent les mains. Le dernier mot revient au pouvoir exécutif et c'est aux gouvernements des deux pays de prendre la décision définitive. «C'est entre les mains de notre **ministre fédéral**», a rétorqué l'ambassadeur du Canada à Washington, Gary Doer, de passage à Ottawa hier pour participer à une conférence aux côtés de son homologue américain. La veille, aux Communes, **le ministre** en question, **Vic Toews, à la Sécurité publique**, se contentait d'affirmer que sa décision serait prise en vertu de la Loi sur le transfèrement international des délinquants. Pas d'indice, donc, quant à sa volonté de respecter la garantie offerte 12 mois plus tôt par le ministre des Affaires étrangères de l'époque, Lawrence Cannon, qui avait certifié aux Communes que son gouvernement allait «mettre en oeuvre» l'accord conclu entre le gouvernement américain et le clan d'Omar Khadr. « Le non-respect de cet engagement serait de nature à porter atteinte à la confiance des citoyens dans nos institutions et à nuire à l'image du Canada à l'étranger», y plaide Claude Provencher, directeur général du Barreau. M. Provencher rappelle que la Cour suprême a reconnu en janvier 2010 que les droits constitutionnels de Khadr ont été violés lors d'interrogatoires menés par des responsables canadiens en 2003 et 2004. «Le Canada a l'obligation de réparer et de mettre fin à ces violations aux droits de Khadr», indique-t-il dans cette missive adressée au ministre des Affaires étrangères John Baird et à son collègue **Vic Toews**. Le Devoir, A3

Conservatives are NOT making it better

An opinion piece states, "...Last week, I also watched an amateurish It Gets Better video made by members of the Conservative Party of Canada...With that lyric in mind, I reflect on what the Conservative Party of Canada has taught our children about LGBTQ Canadians:...**Public Safety Minister Vic Toews,** who appears in the video, and several other Conservative MPs spoke out against Bill C-250, which amended the hate propaganda sections of the Criminal Code to expand the current definition of protected groups to include sexual orientation. LESSON: Lesbians, gays and bisexuals should not be protected against hate...Hamilton Spectator, A13

NATIONAL SECURITY / SÉCURITÉ NATIONALE

Record number of dubious money transactions flagged

The government agency responsible for monitoring money laundering and terrorist financing in Canada referred a record number of suspicious financial transactions to the RCMP, Canada's spy agency and other federal departments for investigation last year, according to a report released Wednesday. The Financial Transactions and Reports Analysis Centre of Canada uses information received from banks and other financial institutions to identify financial transactions that could be associated with organized crime or terrorism. Edmonton Journal, A14; * Le Devoir; * The Guardian (The Telegram, Waterloo Region Record)

Iranian financier transfers $3-million house to daughter
As Canadian officials look at ways to revoke his citizenship and remove him, a top Iranian financier who fled here from Tehran amid a major bank scandal has off-loaded his real-estate holding in Toronto, records show. On Oct. 7, nine days after he flew to Canada, Mahmoud Reza Khavari and his wife paid off the mortgage on their $3-million Toronto home and gave it for a token $2 to their daughter, Parandis Khavari, land registry documents show. In addition to being linked to the fraud scandal, Mr. Khavari's bank has been blacklisted for years by Canada, the United States and the European Union, which allege that Melli used shell companies and other deceptive practices to finance terrorism and fund Iran's nuclear and missile programs. Some U.S. security analysts say Mr. Khavari is a trove of intelligence about illicit Iranian banking and called on Canadian officials to question him. Globe and Mail, A7

NEWS ONLINE POLL
An online poll by Sun News states, "Q.The al-Qaida-linked al-Shabaab released an audio recording over the weekend calling for terrorist attacks against Canada. Should Canadians be concerned about terrorism on our own soil? Yes 93%, No 7%...London Free Press, B2

U.S. to test body scanners
The U.S. Transportation Security Administration will study the health risks of the full-body scanners that use X-rays, administrator John Pistole said Wednesday. The TSA has said the scanners are safe, based on external health studies, but the agency has never conducted its own research, Pistole said. A report published Tuesday by ProPublica questioned the research used to determine the safety of the scanners. Calgary Herald, D2

*** A bien y penser**
Un lettre déclare, « Le gouvernement Harper me désespère avec sa mesquinerie bornée et son incohérence. Non satisfait d'abroger le registre des armes d'épaule, il refuse aux provinces et aux corps policiers le droit d'en utiliser les données, tout en légiférant pour durcir la loi envers les criminels. Puis il s'entête à punir Omar Khadr, mais il fait la leçon aux membres du Commonwealth qui ne respectent pas les droits de la personne. Quelle crédibilité! » La Presse, A25

CYBER SECURITY / CYBERSÉCURITÉ

*** Child-porn site visitors revealed**
The online "hacktivist" group Anonymous claimed on Wednesday to have published the Internet Protocol addresses of nearly 200 visitors to child pornography forums. Windsor Star, C2

LAW ENFORCEMENT AND POLICING / LA POLICE ET DE L'APPLICATION DE LA LOI

G20 indignity comes to light
So what happens if you are restrained in tight handcuffs for 24 hours while being caged with 40 others who also have to go to the bathroom? Tommy Taylor, who was detained although never at a G20 protest, knows the indignity. Toronto Sun, 14

Cartels built into the system
Quebec is not alone. A Gazette survey of construction fraud around the world shows collusion and corruption are part of the industry everywhere. The Gazette, A1

Full pundit
An opinion piece states, "...Cost-benefit analysis aside, gun registration is a potentially useful crime-solving tool. You sold it in large part by explicitly linking law-abiding gun-owners to the murder of 14 women by a misogynist nutter, and then you told them to "get over themselves." It was never going to work." National Post, A17

A SEASON IN HELL / THE CALL HOME / RESCUE MISSION

Ottawa is bungling rescue missions by not telling families in Canada whether their loved ones are alive or dead, a Canadian diplomat once held hostage overseas says. In some scathing criticisms, Mr. Fowler says the Mounties should not be trusted to be in control of Canada's negotiations to free hostages abroad. Officials from the national police force "never understood the extent to which West Africa was not Western Canada," he writes in his memoir. He adds that "the RCMP seemed to have decided that our families could not be trusted with the knowledge we were alive." Globe and Mail, A6

*** Store offers reward for bomb threat tips**
Speaking outside his deserted, besieged store guarded by police tape Wednesday, Shawn Hamilton could barely contain his frustration. A series of explosive packages has been found in the store since Friday. It was open periodically on the weekend, but closed Monday after an employee found a fourth device. Three more were uncovered by bomb squad officers Tuesday. The organized-crime unit is investigating how the packages, which were sophisticated enough to cause serious bodily harm or death, got into the store, just off the Gardiner Expressway at Islington Ave. Toronto Star, GT4

*** Strong contender drops out of race for top Mountie**
The short list of candidates for the RCMP commissioner's job is down to three after a leading contender withdrew from the race, the Star has learned. Luc Portelance, the current border security chief and past deputy operations director at CSIS, took his name out of the running, according to several sources close to the search for a replacement for outgoing commissioner Bill Elliott. Toronto Star, A4

*** End intrusive bill**
A letter states, "I was deeply disappointed in your editorial, Put end to war over Bill C-68 (SP, Oct. 28). Initially the article accurately reviewed the history of the Liberals' 1995 Firearms Act, referred to as Bill C-68, and accurately indicated how utterly divisive this unjust law has been. But when the editorial referred to Stephen Harper's "cold-blooded determination to erase all evidence of it," the writers seem to have fallen into Harper's well-devised propaganda of having people equate the long-gun registry with Bill C-68..." The StarPhoenix, A10

*** Store offers reward for bomb threat tips**
Speaking outside his deserted, besieged store guarded by police tape Wednesday, Shawn Hamilton could barely contain his frustration. A series of explosive packages has been found in the store since Friday. It was open periodically on the weekend, but closed Monday after an employee found a fourth device. Three more were uncovered by bomb squad officers Tuesday. The organized-crime unit is investigating how the packages, which were sophisticated enough to cause serious bodily harm or death, got into the store, just off the Gardiner Expressway at Islington Ave. Toronto Star, GT4

*** G20 jail photos raise 'alarm bells'**
A photo depicting the cramped conditions inside the G20 temporary jail raise "alarm bells," police services board chair Alok Mukherjee said Wednesday. Toronto Star, GT1

*** Charge for data**
A letter states, "Re: Put end to war over Bill C-68 (SP, Oct. 28). This editorial makes a sensible suggestion regarding the data from the long-gun registry: Sell the data to whichever provinces/territories want to buy them for their own use. Sure, it was a huge money pit that should never have happened, but it's done now. The money has been spent. Why not recoup some of the costs through the sale of data to those that want them rather than just throwing the information away?..." The StarPhoenix, A11

*** Police overwhelmed by child porn on web: expert**
Even with more funding and more resources, law enforcement agencies will continue to lose the fight against child pornography and Internet predators due to the overwhelming number of cases, an international conference on sexual offenders heard Wednesday. Edmonton Journal, A14

*** Crime spree**
With the same pair of bank robbers suspected in at least three heists within an hour Wednesday morning, police put all officers on alert to catch them. Calgary Sun, 4

*** Cops raid gun shop**
Surprise and curiosity in a south Winnipeg industrial strip mall after police swooped in Wednesday for a dramatic takedown and started hauling guns out of a business that appears nondescript. Winnipeg Sun, 3

*** Voxpop**
Here's how 2,854 readers responded to: Should the Occupy Calgary protesters be forcibly removed from Olympic Plaza? YES 85% NO 15%. Calgary Herald, A17

*** Long-gun registry keeps criminals honest, so to speak**
An opinion piece states, "...Without registration, guns are too easily able to make their way into the hands of exactly the people we should be keeping them away from. The Conservative tough-on-crime stance is difficult to reconcile with making gun control changes that open the door to easier criminal ownership of guns in Canada. At the moment, statistics suggest legal gun ownership and gun crime are very different worlds. Once guns can move more freely in the hands of criminals, how long will that continue to be true?" Winnipeg Free Press, A11

*** Police cleared by police in fatal shooting**
An external police investigation into the 2010 shooting death of 22-year-old Alvin Wright has determined no criminal offence was committed by the Langley RCMP. Times Colonist, A2; The Province; Vancouver Sun

*** NDPers who voted to kill gun registry punished by leader**
Two NDP MPs who voted to kill the federal gun registry were aware they would be punished for their actions, a party spokesman says. Red Deer Advocate, A5

*** Man faces charges after smokes seized in C.B**
Customs and Excise officers seized 91 cases, or close to a million cigarettes, Saturday, from a truck, camper trailer and shed at a Margaret Street property here. Chronicle-Herald, A9

*** Éliminons l'argent liquide**
Un article d'opinion déclare, « L'économie souterraine, ce fléau qui se traduit par le travail au noir, les impôts et les taxes de vente impayés, le blanchiment d'argent, fait très mal aux budgets des gouvernements, donc à nous tous. Nous n'avons pas d'idée précise des sommes d'argent que nos gouvernements se font soutirer par cette économie souterraine. Selon certains experts, c'est en milliards de dollars annuellement que les fonds publics sont privés par ces pratiques déloyales... » La Presse, A25

*** Steve Duquette arrêté après une cavale de deux ans et demi**
Recherché depuis l'opération SharQc d'avril 2009, le membre en règle du chapitre de Sherbrooke des Hells Angels Steve Duquette est tombé hier soir aux mains de l'Escouade régionale mixte de l'Estrie Estrie. La Tribune, 8 (Journal Montreal)

*** Peu d'arguments juridiques permettront à Québec de gagner**
Québec devrait rapidement demander une injonction pour empêcher le gouvernement Harper de détruire les données du registre des armes à feu, croient deux juristes. La Presse, A16 (Le Droit)

*** Truth on $2b cost of registry comes out**
A letter states, "The huge cost overruns of the long gun registry were always dismissed as a myth perpetuated by the pro-gun lobby. Amazingly, all anybody had to do to get the anti-gun groups to admit it cost $2 billion was to suggest it be scrapped." Hamilton Spectator, A13

*** Sixième vote unanime**
Pour une sixième fois, l'Assemblée nationale a réitéré son unanimité, hier, face à la nécessité de maintenir le registre des armes à feu. Journal Montreal, 12

BC MISSING WOMEN INQUIRY / ENQUÊTE SUR LES FEMMES DISPARUES DE LA C.-B.

*** Sex workers need protection to testify, lawyer says**
Sex workers who testify at the inquiry into the Robert Pickton serial murder case should have their identities protected and shouldn't be subjected to cross-examination from police counsel, says a lawyer at the hearings. Jason Gratl, an independent lawyer appointed to represent the broad interests of Vancouver's Downtown Eastside, says sex workers are especially vulnerable and afraid of the legal system, making them extremely reluctant to come forward. Globe and Mail, S3 (Red Deer Advocate, The Telegram)

*** Family lost two women - 18 years apart**
Lorelei Williams' life has been bracketed by the disappearance of her aunt - who looks just like Lorelei - and her beloved cousin, Tanya Holyk, whose remains were found on the farm of convicted serial killer Robert Pickton. Sitting in the Missing Women Commission of Inquiry for the past two weeks, Williams has been struck by the fact that, even though the disappearances occurred 18 years apart, "my family felt both times the police did nothing. The Province, A16

*** RCMP wants to place ban on inquiry info**
The RCMP lawyer at the Missing Women inquiry is seeking a sweeping ban on sensitive information contained in documents that are expected to be made public soon. Cheryl Tobias, the federal lawyer representing the Mounties, has filed an application seeking to ban third-party information such as the names of suspects in the police investigation that led to the 2002 arrest of serial killer Robert Pickton. The application was made earlier but was put off until Wednesday so as not to interrupt the testimony of family members of Pickton's victims. Starphoenix, C6 (Times Colonist)

BORDER SECURITY / SÉCURITÉ FRONTALIÈRE

City man faces long U.S. term - Admitted to conspiracy and money laundering
A Winnipeg man is facing at least 10 years in prison after cutting a deal with U.S. justice officials that has put his hometown police on alert. Jerome Catacutan admitted last month in a Fargo courtroom to charges of conspiracy and money laundering. He was arrested in Hawaii in August and transferred to a prison in North Dakota, where he remains without bail. Winnipeg Free Press, A4

*** "Ti-Pon" a été renvoyé en Haïti**
Ses manoeuvres de la dernière chance pour éviter l'expulsion se sont soldées par des coups d'épée dans l'eau pour le chef du gang de la rue Pelletier, Bernard "Ti-Pon" Mathieu, qui a été renvoyé en Haïti sans tambour ni trompette il y a deux semaines, a appris le Journal. Journal de Montréal, 4

COMMUNITY SAFETY AND PARTNERSHIPS / SÉCURITÉ DE LA POPULATION ET PARTENARIATS

Bill C-10
A divide is emerging between Eastern and Western Canada over the federal government's law-and-order agenda, as a debate heats up over the costs of the anti-crime measures and the substance of the bill itself. Quebec has moved to form a united front among all the provinces to fight the bill. Ontario Premier Dalton McGuinty has joined forces with Quebec Premier Jean Charest, allowing Canada's two largest provinces to speak with one voice in pressuring Ottawa to pick up the tab for higher costs the proposed laws would impose on the provinces. The Globe and Mail, A4, Leader-Post ;* The Vancouver Sun, * The Telegram (The Chronicle Herald)

FEDERAL CRIME AGENDA
An editorial states, "Ottawa's crime agenda could cost the provinces billions of dollars over the next few years, and those expensive chickens are now coming home to roost. Quebec and Ontario say they will refuse to pay. And who can blame them? The tough-on-crime omnibus bill now before Parliament is hardly a sterling example of co-operative federalism. It is heavy-handed federal policy-making, which (along with some previous crime bills) will cost the provinces dearly...The provinces have had limited say, through discussions among attorneys-general and their deputies, in Ottawa's plans, unlike, say, in health care, where major reforms and extra cash are typically put on the table at the same time..." The Globe and Mail, A18

Sex offenders and schools
A letter states, "Hysteria over pedophiles working in schools is understandable but an overreaction...This is not to say that we shouldn't be concerned, but we should not succumb to fearmongering that would eliminate pardons for anyone convicted of an offence involving a child. Although a learning environment is not appropriate employment for these people, eliminating the chance of finding decent work is an equally bad idea. The sensible compromise is to leave things as they stand..." The Gazette, A22

*** Crime and the provinces**
An editorial states, "Generally speaking, the level of government that enacts legislation should bear the political burden of raising the taxes necessary to pay for it. That isn't always practical in a federal system, which is one reason we have transfer payments...No one seems to have a dollar figure yet for what the omnibus crime bill would cost the provinces - never mind a figure broken down province by province. But it seems a fair bet that there will be a cost, and a significant one. The Conservatives, for their part, argue that they've already increased transfer payments to the provinces, but that was never intended to cover the costs of the omnibus crime bill. They also argue that crime costs society, but that's neither here nor there if their proposed changes don't significantly decrease crime - and it's hard to see how they will..." Ottawa Citizen, A14

*** One-day stay then back to jail**

A Winnipeg man who disappeared from a halfway house one day after he was released from prison has been sentenced to another 60 days in custody. Derek Hall, 24, pleaded guilty Wednesday to one count of being unlawfully at large. He was previously convicted of aggravated assault and sentenced to 30 months in prison. Hall told court he left the halfway house because he didn't want to live with sex offenders. Winnipeg Sun, 18

*** Sexual assault anomaly**
An editorial states, "Attitudes toward sexual assault and rape have come a long way in Canada... The remarks a Manitoba judge expressed in convicting a Thompson man -- the "clumsy Don Juan" -- of sexually assaulting a young woman indicate that not only is there far to go yet, but the law on consent is not clearly understood even within the courts...The Women's Legal Education and Action Fund is arguing the conviction should be upheld and that the court must recognize there are systemic discriminatory issues and attitudes still at play in sexual assault cases that lead jurists to blame victims..." Winnipeg Free Press, A10

*** Prisoners come to orchards' rescue**
Putting prisoners to work for private business is hardly a new idea in much of the U.S., but it has generated plenty of controversy. Paul Wright, founder and editor of Prison Legal News, a publication that has tracked the experiments, said the prison-labour plans often are attractive to politicians who want to appear tough on crime and appeal to voters by boasting that "we're making the bad guys work." But he said they have a poor track record. While the labour might be cheaper, Wright said that states often are forced to pick up the costs of security, transportation and other expenses, making the plans tantamount to "a not-so-subtle taxpayer subsidy" for employers. The Vancouver Sun, B12

*** Stabbing his neighbour earns man cell time**
A Whitehorse man will spend another 54 days in custody after he was sentenced recently for stabbing a neighbour with a small knife earlier this year. Justice Michael Cozens ruled George Vittrekwa should receive 1.5 days' credit for each day he spent in pre-trial custody since being arrested. The judge ruled Vittrekwa's circumstances justify an exception to the federal government's new Truth and Sentencing Act. That legislation limits the credit that may be granted to an offender for his or her time in pre-trial custody for a maximum of one day for each day in custody. Whitehorse Daily Star, 5

*** L'inévitable collaboration fédérale-provinciale**
Un éditorial déclare, « Depuis l'élection du 2 mai où ils sont devenus majoritaires à la Chambre des communes, les troupes de Stephen Harper peuvent ignorer les avis contraires qui circulent dans l'espace public... Mais quand les critiques du projet de loi omnibus sur la justice criminelle (C-10) viennent d'une province, elles ont un poids non négligeable. Les provinces sont des partenaires du fédéral dans l'administration de la justice et leur collaboration est essentielle. Voici que le Québec, par la voix de son ministre de la Justice, proteste avec véhémence au sujet de la direction que le fédéral souhaite emprunter. Ottawa ne peut agir aveuglément dans des secteurs comme la réhabilitation des prisonniers d'âge mineur, les peines minimales, les libérations conditionnelles, etc., a accusé M. Fournier. Neuf initiatives regroupées en un seul projet de loi qui ne pourra faire l'objet d'aucun examen sérieux, les conservateurs tirant profit de leur majorité parlementaire pour écourter tout débat et écarter tout amendement qui viendrait diluer la portée de C-10... » Le Droit, 14

*** Bill targets young offenders**
A letter from the Minister of Justice and Attorney General of Canada states, "We agree that Canadians lose confidence in the justice system when serious, violent offenders, including young offenders, are not given sentences that reflect the severity of their crimes. Canadians are increasingly concerned about crime, which is why our government has a strong mandate to keep our streets and communities safe. Bill C-10, the Safe Streets &Communities Act, provides additional tools for the courts when dealing with violent and repeat young offenders. Our proposed amendments will ensure that the protection of society is a primary goal of Canada's youth criminal justice system..." Toronto Star, A22

*** Prisoner charged with escaping custody, kidnapping appears in court**
A serving federal prisoner accused of overpowering a female corrections officer and dropping her off by the side of a rural road east of Bowden while returning from a day trip was in Red Deer provincial court on Wednesday. Fowler was being escorted back to Drumheller Institution by the corrections officer after the man convicted of second-degree murder was given a day pass to visit his family in Buck Lake, 15 minutes southeast of Drayton Valley on Oct. 18. Red Deer Advocate, A2

*** Tremblay veut se marier**
Condamné à répétition pour violence envers des femmes, Jean-Guy Tremblay refait surface dans la région de Québec et veut bientôt se marier avec une nouvelle conjointe malgré l'avis contraire des intervenants, qui désapprouvent cette autre relation tumultueuse. Toujours considéré comme dangereux, il est aussi connu pour ses nombreuses condamnations pour agression, séquestration et harcèlement criminel contre des femmes. Libre depuis décembre 2010, il fait l'objet

d'une surveillance de longue durée jusqu'en juillet 2016 par la Commission nationale des libérations conditionnelles (CNLC). Le Journal de Montreal, 5

PUBLIC SERVICE / FONCTION PUBLIQUE

Tories' math way off?
Parliament's budget officer suggests the Conservatives are gambling with an election promise to balance the books by 2014. Kevin Page appeared before the Commons finance committee Wednesday to defend his view that the cards don't stack up in Prime Minister Stephen Harper's favour to erase the deficit in three years. Toronto Sun, 28

*** Public pension plans need closer look**
A letter to the editor states, "It's kind of funny to have one article showing there is enough money in the Canada Pension Plan (CPP) to fund it for 75 years, while another suggests public-sector pensions will bankrupt the country. The happy state of the CPP is supposed to be due to good investments, while the sorry state of public-sector pensions is supposed to be due to bad investments. If there is such a difference, it needs to be understood and corrected...The situation needs clarification as to which plans may be in the worst trouble, but it appears the federal PSP is in good shape. Finally, pension plans are set up under actuarial procedures that are supposed to protect pensioners and employers. The employers, however, manage the plans. Perhaps it's time for a closer look as to how they are regulated." Hamilton Spectator, A12

INTERNATIONAL / INTERNATIONAL

*** Double flu infections raise concern**
A rare case of people being infected with both swine and seasonal flu has been documented in Cambodia, raising concern about the possibility of a potent combination strain, said a study out Wednesday. Ottawa Citizen, C9

*** Tensions rise over Iran's nuclear ambitions**
Iran is attempting to engineer and test nuclear weapons at banned production sites in defiance of United Nations sanctions, according to a report to be released next week. The Iranians, despite a fourth round of UN sanctions last year and further punitive measures from the European Union and the U.S., have remained defiant. Hopes that the Stuxnet computer virus attack by Western powers on Iran's nuclear technology would prove crippling have faded. The virus succeeded in crippling a number of Iranian centrifuges but analysts now think the effects have worn off and production of highly enriched uranium has accelerated again. Vancouver Sun, B5

*** 'Merchant of Death' arms dealer found guilty**
A jury Wednesday found a Russian arms dealer, dubbed the "Merchant of Death," guilty of conspiring to sell a huge arsenal to U.S.-designated terrorists. Viktor Bout, 44, who was extradited from Thailand to the U.S. in 2010, was found guilty on all four counts including conspiring to kill U.S. service personnel and to sell anti-aircraft weapons. The Province, A35

OTHER / AUTRE

Does Occupy Montreal have any solutions to offer?
An opinion piece states, "The Occupons/Occupy Montreal protest, like the 1,500 others worldwide linked to the Occupy Wall Street phenomenon, is beginning to lose energy and momentum. These static vigils inside of public squares and parks aren't going to be enough to sustain meaningful public interest for very much longer. The Occupy brand needs to write a new chapter, and become more dynamic...Occupons/Occupy Montreal has its work cut out for it. But to accomplish its goals, it needs to get out of Victoria Square and interact with more people more often in more different locations than they are doing now." Montreal Gazette, A22

*** 'Buck stopped with me,' Baird says Tony Clement insists no decisions were made about G8 summit spending during his meetings with Parry Sound-Muskoka mayors**
Cabinet ministers Tony Clement and John Baird both say, in hindsight, they should have done things differently in awarding nearly $50-million to build sidewalks, gazebos and sports facilities in Mr. Clement's riding as a nod to the legacy of the G8 summit. Mr. Clement, the Treasury Board president, told a Commons committee on Wednesday that he should

have let federal bureaucrats assess and select the best proposals from the hundreds submitted by mayors in Parry Sound-Muskoka, where the meeting of world leaders was held in 2010 at a Huntsville resort. "The border infrastructure fund was topped up," so the money was not diverted from border infrastructure, Mr. Baird said. But "in hindsight, the estimates could have included a line regarding the top-up of this fund." Globe and Mail, A5; Leader-Post (Starphoenix, Ottawa Citizen, Windsor Star, Calgary Herald); Edmonton Sun (London Free Press, Calgary Sun, Winnipeg Sun, Toronto Sun, Ottawa Sun, Kingston Whig-Standard); Waterloo Region Record; La Tribune (Le Droit); La Presse

*** Canada slips to 6th on the bribery index**
Canada's international Boy Scout image has been tarnished with the release of a report that shows Canadian companies are not above bribing foreign officials in order to seal a deal. Transparency International's Bribe Payers 2011 Index released Wednesday shows that Canada, which was tied with Belgium just three years ago for being least likely to bribe, is now tied for sixth place with Australia. Toronto Star, B3

*** Des pièges pour suicidaires**
Pas besoin de surfer très loin sur le web pour tomber sur de véritables clubs de suicide, où des désespérés portant les mêmes lunettes noires se donnent rendez-vous ou des recettes pour mettre fin à leurs jours. Les jeunes les visitent apparemment de plus en plus, et font ainsi des tentatives beaucoup plus sérieuses. A Ottawa, une étudiante de 18 ans a même cédé aux pressions d'un prédateur qui espérait filmer ses derniers instants. Le Droit, 2 (Le Nouvelliste); La Presse

s.16(2)(c)

Klassen, Nathan

From: Bendelier, Kenneth
Sent: November-03-11 8:02 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description: **Socialbots' steal 250GB of user data in Facebook invasion.** "Programs designed to resemble humans infiltrated Facebook recently and made off with 250 gigabytes of personal information belonging to thousands of the social network's users, researchers said in an academic paper released November 1. The 8-week study was designed to evaluate how vulnerable online social networks were to large-scale infiltrations by programs designed to mimic real users, researchers from the University of British Columbia Vancouver said in the paper, titled "The Socialbot Network: When bots socialize for fame and money." The 102 "socialbots" researchers released onto the social network included a name and profile picture of a fictitious Facebook user and were capable of posting messages and sending friend requests. They then used these bots to send friend requests to 5,053 randomly selected Facebook users. Each account was limited to sending 25 requests per day to prevent triggering anti-fraud measures. During that initial 2-week "bootstrapping" phase, 976 requests, or about 19 percent, were accepted. During the next 6 weeks, the bots sent connection requests to 3,517 Facebook friends of users who accepted requests during the first phase. Of those, 2,079 users, or about 59 percent, accepted the second round of requests. The increase was due to what researchers called the "triadic closure principle," which predicts that if two users had a mutual friend in common, they were three times more likely to become connected. Researchers found social networks were "highly vulnerable" to a large-scale infiltration, with an 80-percent infiltration rate."
Reference: http://news.cnet.com/8301-1009_3-20128808-83/socialbots-steal-250gb-of-user-data-in-facebook-invasion/

2. Item Description: **PandaLabs Report – Q3 2011**. "The new PandaLabs Report Q3 11 is out. Take a look at what has happened in the computer security field during the last 3 months. In this quarter 5 million new malware samples have been created and the record of new Trojans has been broken as it the preferred category by cybercriminals to carry out their theft of information. The Anonymous Group, who starred in the second quarter, has continued making the headlines in this period, due to the arrest of some members, theft of data from different web sites and operation PayPal. The PandaLabs report also includes information about cybercrime, cyberwar, social networks, Mac and cell phones, social networks and a wide section to explain about exploits. The highlight of this third quarter is the record set in the creation of new Trojan samples. 3 out of 4 new malware samples created by cybercriminals are Trojans and this is just another proof that they are focused on stealing users information."
Reference: http://pandalabs.pandasecurity.com/pandalabs-report-q3-2011/
http://press.pandasecurity.com/wp-content/uploads/2011/10/PandaLabs-Report-Q3-2011.pdf

3. Item Description: **Poison and EyeStye, by the numbers**. "The latest MSRT release included coverage for two more malware families, one being Win32/EyeStye, which we discussed earlier this month, and the other being Win32/Poison. In tandem with our efforts to provide an antidote to the scourge of Win32/Poison infections via the MSRT, we've also today published a detailed MMPC Threat Report on the same family. This Microsoft Malware Protection Center (MMPC) Threat Report provides an overview of the Win32/Poison (Poison Ivy) family of malware. The report examines the background and functionality of Poison Ivy, and provides telemetry data and analysis."
Reference: http://blogs.technet.com/b/mmpc/archive/2011/11/01/poison-and-eyestye-by-the-numbers.aspx

4. Item Description: **First joint EU-US cyber security exercise:** "The first joint cyber security exercise between the European Union and United States is being held today in Brussels, with the support of the EU's Network and Information Security Agency (ENISA) and the US Department of Homeland Security. The day-long table-top exercise, Cyber Atlantic 2011, is using simulated cyber-crisis scenarios to explore how the EU and US would engage each other and cooperate in the event of cyber-attacks on their critical information infrastructures. In the first scenario, a targeted stealthy cyber attack (Advanced Persistent Threat) attempts to exfiltrate and publish online, secret information from EU Member States' cyber security agencies. The second simulation focuses on the disruption of supervisory control and data acquisition (SCADA) systems in power generation infrastructures. More than 20 EU Member States are involved in the exercise, 16 of them actively playing, with the European Commission providing high-level direction."
Reference: http://www.net-security.org/secworld.php?id=11884

5. Item Description: **Following WordPress into a Blackhole:** "When we looked into the recent wave of WordPress site hacks, our investigation took two separate paths: uncovering the TimThumb vulnerability and the Black Hole Toolkit used to exploit it. Now it is time to talk more in detail about what the Blackhole Toolkit is. For starters, the Blackhole exploit kit is used to spreading malicious software to users through hacked legitimate sites. It was most likely made by Russia developers. The big clue for this is that operators can switch between Russia and English languages. The full version of this toolkit costs around $1500 on the black market. However, bargain hunters can find a stripped down version for the free online. But, much more important than acquiring Blackhole is finding out how to get rid of it. More precisely, simply finding out if you have been infected. So, how can website owner recognize that his page was infected and has been blocked by an antivirus program because it is being misused as a redirector to site with Blackhole exploit kit? And how do they compromise your site?"
Reference: https://blog.avast.com/2011/10/31/following-wordpress-into-a-blackhole/

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Dincoy, Rana

From: Dincoy, Rana
Sent: November-01-11 9:53 AM
To: Bendelier, Kenneth; Cameron, Bud; Pitcher Robert
Cc: Klassen, Nathan
Subject: RE: Big ideas for strat products

That's an excellent point. However, we are in a position, I believe to look at incidents/news CCIRC has seen recently and single out something important. For example, September's issue of the month for govt execs, would have been, in my opinion, "what the compromise of certificate authorities means" because of the Diginotar saga. I believe NCSD did a BN on this for the ADM. Once I finish really looking at last week's activities, I will have a suggestion for October. Does anything particular stick in your minds for October?

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

From: Bendelier, Kenneth
Sent: October 31, 2011 6:18 PM
To: Cameron, Bud; Pitcher Robert; Dincoy, Rana
Subject: Re: Big ideas for strat products

Silly question, why not ask the clients?

The provinces mentioned a few things but, in reality, they are the purview of CSEC.

From: Cameron, Bud
Sent: Monday, October 31, 2011 02:20 PM
To: Pitcher Robert; Bendelier, Kenneth; Dincoy, Rana
Subject: Big ideas for strat products

Seeking your ideas for "issue of the month" type papers (Reports in the CCAP taxonomy).
DDOS, APT soon to be done, what other topics would be of interest and relevance to our clients?
I was thinking that one on Anonymous might be useful.
I will put the question to the Gov IRT forum and see what they say...

Bud Cameron, CD, MSc
Manager, Cyber Security Programs | Gestionnair, Programmes de sécurité cybernétique
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 +1 613-949-8317

Public Safety Canada | Sécurité publique Canada

TLP:GREEN

Canada

INFORMATION REPORT
CCIRC Cyber Awareness Product:11-R-002

Denial of Services Mitigation Guidelines

s.16(2)(c)

Issued: 1-Nov-2011

DISCLAIMER

This publication is **UNCLASSIFIED - For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in 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.

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 Flashed marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information, or Technical
- **Operational Summary:** Daily, Weekly, GovIRT

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 @ [redacted]

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

AUDIENCE:

This Information Report is intended for IT professionals and managers within federal, provincial/territorial and municipal governments; critical infrastructure; and other related industries. The recipients of this product may further distribute it to technical stakeholders within their organisation.

PURPOSE

The purpose of this Information Report is to provide IT security personnel with an introduction to Distributed Denial of Service attacks (DDoS), their modus-operandi and the recommended steps to help with the preparation, identification, containment, recovery and continuous improvement efforts required to limit associated organisational risk. This document may be used by system administrators, Computer Security Incident Response Teams (CSIRTS), IT security operations centers and other related technology groups.

ASSESSMENT

Denial of Service Attacks (DoS) are common malicious network actions aimed at disrupting the availability of computing resources from legitimate users. These types of attacks, especially Distributed Denial of Service Attacks (DDoS), have recently gained in popularity due to the availability of DOS-rental services from botnet operators, as well as the availability of various free and easy to use hacking tools. The latter have enabled activists using hacking to support their claims, also known as hacktivists, to efficiently recruit large number of followers to perpetrate cyber attacks, increasing both their distribution and power. Well known examples of denial of service attacks include hacking group "Anonymous" use of the Low Orbit Ion Cannon DDOS tool in support of Wikileaks[1] and attacks against national infrastructures such as Korea[2] , Georgia[3] and Estonia[4].

DOS AND DDOS DEFINITION

A DoS attack is an attempt to make a computer resource unavailable to its intended users[5]. A DDoS attack occurs when multiple systems simultaneously flood a networked computer resources, rendering it inaccessible. A DDOS, in contrast with a DOS, comes from many sources, often hundreds or even thousands. As a result, mitigation actions against a DDOS are more difficult to coordinate and associated traffic more damaging to the target.

DDoS attacks often use stateless protocols such as UDP and ICMP, but stateful protocols can also be used when the connections are not fully established such as a TCP SYN flood. Both techniques make it easier for the attacker to use spoofed IP addresses and harder to determine the source of the attack.

---

[1] Introduction to LOIC: http://en.wikipedia.org/wiki/LOIC
[2] http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems
[3] http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/
[4] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[5] Definition: http://en.wikipedia.org/wiki/Denial-of-service_attack

FIVE STEPS TO DEFEND AGAINST DDOS ATTACKS

Preparation

Preparation is the most important step in defending against a DDoS attack. Clear and complete procedures and guidelines should be established well before an attack takes place. Any organisation may fall victim to DDOS attacks, either directly or indirectly. Having a solid plan in place will help reduce the risk and lessen the impact should an attack occur.

Identification

Indicators that your organization may be under a DDoS attack could include poor network performance, services becoming inaccessible or system crashes. Being able to identify and understand the nature of the attack and its targets will help in the containment and recovery process. For this purpose, organisation require tools providing visibility over their managed Information Technology (IT) Infrastructure. Often, prior to a DDoS attack, a reconnaissance of the target is performed by the attacker. This may include scanning the target network for known exposed vulnerabilities or sending malformed packets to the target host to analyse changes in response time. This reconnaissance activity may be hard to detect, especially as it may take place well before the attack itself. A knowledgeable attacker will also ensure scan traffic does not meet the threshold required to trigger alarms from network monitoring tools. However, there may be available intelligence increasing the likelihood of a DDOS attack to an organisation. A good example are the Anonymous Operations (aka "anonops")[6] , which broadly advertise their motivation.

Containment

Having a pre-determined containment plan before an attack for a number of scenarios will significantly improve response speed and limit damages resulting from a DOS attack. For example, containment strategy for a mail server may differ than for a web server. Underestimating the importance of this phase can result in mistakes and significant collateral damages. Understanding the nature of DDOS attacks and documenting associated decision making process is therefore critical. An organisation should clearly identify its network perimeter and exposed assets. Load balancers, Deep-Packet Inspection Firewall, content caching, content hosting geographic diversity, dynamic DNS service and ISP-based DDOS protection services are amongst various tools an organisation may leverage to contain an on-going DDOS attack.

Recovery

Depending on the containment strategy employed and the sensitivity to its collateral impact, an organisation may be under different pressure to recover from a DDOS attack. Understanding the characteristics of the attack is required for an appropriate recovery. DDOS may exploit limits in the following resources:

- Server queue length
- Server computing resources
- Client tolerance to level of service variability
- Bandwidth

A DDOS attack may exploit any or a combination of these limitations. An organisation equipped with a flexible provisioning model for these resources may be able to rapidly adapt and sustain long-term DDOS attacks. Some attacks may however leverage vulnerabilities in protocols or software and

[6] http://anonops.blogspot.com/2011/09/tar-sands-action-september-3-press_04.html

achieve unexpected impact as a result. [7] An organisation equipped with packet capture capability may be able to identify the delivery method of the attack and potentially design an accurate Intrusion Prevention System / Firewall signature. Despite mitigation efforts, some DDOS attacks may be persistent over time. An organisation using connexion logs and other tools may be able to provide a list of potentially offending IP addresses (if not spoofed) to their upstream ISP, law enforcement and national Computer Emergency Response Team (CERT) to coordinate mitigation/investigation of the offending sources.

Lessons Learned

Lessons learned is a very important step but often overlooked. Lessons learned activities should take place as soon as possible following an incident. All decisions and steps taken throughout the incident handling cycle should be reviewed. All procedures should be reviewed to see where improvements may be made.

May be the most challenging part of performing Lessons Learned review consist in documenting the impact and cost the incident caused to the organisation. Although time consuming, this step is essential to allow organisations to properly justify security resources and assess their return on investment. Damages to an organisation include tangible metrics, such as loss in sales and productivity, as well as intangible metrics, such as reputation and brand.

By performing this review after each incident, organisations will enable continuous improvement and potentially significant reduction in the impact of incidents.

CHECKLIST

The following checklist is intended to help organisation during the various mitigation phase of DDOS attacks. Many of these mitigations are applicable to other types of cyber attacks as well and should be considered accordingly.

1	Identify your most critical assets and the services they provide. • Are they up to date with the latest patches? • Do they run any unnecessary services? Such as Telnet, FTP, etc.
2	Establish procedures with your Internet Service Provider (ISP) to determine how they can assist your organization during a DDoS attack. Know what Service Level Agreement exists and what costs may be incurred.
3	Establish 24/7 contact information for your ISP and alternate methods for communications.

[7] http://www.theregister.co.uk/2011/08/24/devastating_apache_vuln/

4	Deny all obviously spoofed traffic. Example is internal IP addresses shouldn't be coming in or going out of your network.
5	Establish procedures on how to segregate your networks in an event of a DDoS attack to contain it. Use network devices best suited to defend against DoS attacks (e.g. routers)
6	Disable all unneeded services and restrict all unnecessary access to all critical hosts.
7	Create a whitelist of the source IPs you must allow if you need to prioritize traffic during an attack.
8	Document your network topology including all IP addresses. Keep it up to date.
9	Review your Business Continuity Plan (BCP) and ensure senior management and legal team understand the significance of a DDoS attack and their roles.
10	Understand "normal". Baseline network traffic and CPU, connection and memory utilization of critical hosts such that network monitoring tools may trigger on drastic changes
11	Acknowledge that your organization may be attacked. Seek and obtain management's approval for the development and implementation of policies, plans and procedures to defend against DoS attacks. Identify and obtain resources to implement these plans.
12	Assign responsibility. Identify who plays a role in defending against a DoS attack and ensure they are aware of this responsibility. This should include personnel from critical business functions, IT operations, network and IT security teams, legal advisors and media relations staff. Ensure an up-to-date point of contact list, with primary and alternate personnel, is maintained. As the network may the unavailable, including mobile devices, ensure alternate communications mechanisms are in place,
	Conduct exercises. The worst time to test plans and procedures is during an attack.

1	Determine if you are the target or a collateral victim.
2	Understand the logical flow of the attack.
3	Determine what type of traffic is being used, such as IP addresses, ports, and protocols.

4	Consider using network analysis tools to determine the type of traffic being used in the attack. Ex. TcpDump, Wireshark, Snort, etc.
5	Review any available logs to understand the attack and what is being targeted.
6	Notify the appropriate personnel. This may include senior management and the legal team.

1	Contact your ISP provider to implement filtering.
2	Block the traffic as close to the network cloud as possible. (Router, firewall, load balancer, etc.)
3	Relocate the target to another IP address if a particular host is being targeted. This is a temporary solution.
4	If a particular application is being targeted, consider disabling it temporary.
5	Identify and correct the vulnerability or weakness that is being exploited. An example of this may be an unused service that is accidently left enabled on a public facing device or unpatched operating system.
6	Implement filtering based on the characteristics of the attack. An example may be blocking IMCP echo packets.
7	Implement rate limiting for certain protocols, allowing a certain number of packets per second for a specific protocol or to access a certain host.

1	Confirm that the DDoS attack has finished and services are reachable again.
2	Confirm that your networks are back to your baseline performance.
3	If necessary, patch and update all affected machines.
4	If possible, identify the source of the attack. Enlist the help from your ISP.
5	Review logs for signs of reconnaissance.

1	Create or update the following documents: • Standard Operating Procedures • Emergency Operating Procedures • Business Continuity Plans

RECOMMENDATIONS

CCIRC recommends that organisation assess their risk exposure to Denial of Service attacks which may be caused accidentally or intentionally and consider mitigation advice herein provided and implement them accordingly in light of the specific IM/IT environment.

REFERENCES

1. US-CERT, Understanding Denial of Service Attacks
http://www.us-cert.gov/cas/tips/ST04-015.html

2. NIST, Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

3. GovCERT.NL, Factsheet: Protect your online services against dDoS attacks
http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html

4. Societe Generale DDoS Incident Reponse
http://cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf

REPORTING

Any Canadian Critical Infrastructure Operator wishing to report incidents may do so using the CCIRC Cyber Duty Officer PGP encryption key, found at:
http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx
Associated reports should be sent to:
cyberdo@ps-sp.gc.ca.

Potentially malicious files/samples may be shared with CCIRC by sending them zipped and protected with the password "infected" via email to:
malware@ccirc-ccric.gc.ca

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.

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.

Klassen, Nathan

From: Bendelier, Kenneth
Sent: November-01-11 7:57 AM
To: [redacted]
Subject: Noteworthy and Not Worthy

CYBER NEWS:

1. Item Description: **Symantec uncovers Nitro attacks targeting chemical industry.** "Symantec has revealed a large-scale targeted cyber attack designed primarily to steal information from chemical and defense companies, including 27 in the United States. Dubbed "Nitro", the campaign started in late April focused on human rights groups, before moving onto the motor industry, according to the Symantec Nitro attacks report. The attack moved onto the chemical industry in late July, targeting 29 companies and another 19 in sectors such as defense, the report said. The attackers used the common ploy of sending certain members of a target organization an e-mail with a malicious attachment disguised as a meeting invitation or security update. "The emails contained an attachment that was either an executable that appeared to be a text file based on the file name and icon, or a password-protected archive containing an executable file with the password provided in the email," the report said. "In both cases, the file was a self-extracting executable containing PoisonIvy, a common backdoor Trojan developed by a Chinese speaker." Once the infected machine was connected to the command and control server, attackers could traverse the network, infecting additional computers in search for the domain administrator's credentials, and from there locate servers containing intellectual property. Eventually the content is uploaded to a remote site. The attacks were spread geographically, but most infected machines were located in the United States (27), Bangladesh (20), and the United Kingdom (14). Symantec traced the attacks to a virtual private server (VPS) based in the United States, but registered to a "20-something male" in Heibei, China dubbed "Covert Grove". The male claimed the VPS, which cost him $32 a month to rent, was set up for legitimate purposes, but Symantec researchers found evidence that may point to the contrary. "When prompted regarding hacking skills, Covert Grove immediately provided a contact that would perform 'hacking for hire'. Whether this contact is merely an alias or a different individual has not been determined," the researchers concluded."
References: http://www.v3.co.uk/v3-uk/news/2121298/symantec-uncovers-nitro-attacks-targeting-chemical-industry
http://blog.trendmicro.com/the-significance-of-the-nitro-attacks/
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

2. Item Description: **Theres-Something-Phish-Y-About-This-Email-From-Apple**. "Today, I received an email from Apple telling me that there was a change in my account information. Seeing that I had already changed it a few weeks ago, I was rather curious to see what this email from "Apple" had to say. After opening the message, I was surprised to see an uncanny and almost identical resemblance with the legitimate email from Apple I got a few weeks back."
Reference: http://blog.trendmicro.com/theres-something-phish-y-about-this-email-from-apple/

3. Item Description: **New Tor release fixes de-anonymization attack.** "The Tor Project has released a new version of its client software to fix a serious vulnerability that allows an attacker to strip users of their anonymity on the network. The new version also includes many other security and privacy fixes. The attack that enables the anonymity stripping requires a specific set of conditions to be in place, and the new version of Tor removes two of those components from the equation, which is enough to prevent the attack. It relies on the fact user clients will reuse their TLS certificates when connecting to different Tor relays, which can enable an attacker to identify a specific user by his certificate. "The attack relies on four components: 1) Clients reuse their TLS cert when talking to different relays, so relays can recognize a user by the identity key in her cert. 2) An attacker who knows the client's identity key can probe each guard relay to see if that identity key is connected to that guard relay right now. 3) A variety of active attacks in the literature ... allow a malicious Web site to discover the guard relays that a Tor user visiting the website is using. 4) Clients typically pick three guards at random, so the set of guards for a given user could well be a unique fingerprint for her. This release fixes components #1 and #2, which is enough to block the attack; the other two remain as open research problems," a Tor Project's spokesman said in a message announcing version 0.2.2.34."
Reference: http://threatpost.com/en_us/blogs/new-tor-release-fixes-de-anonymization-attack-102811

///////end///////

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique

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

Cameron, Bud

From: Cameron, Bud
Sent: November-01-11 6:38 AM
To: Bendelier, Kenneth
Subject: Re: Big ideas for strat products

[redacted]

From: Bendelier, Kenneth
Sent: Monday, October 31, 2011 06:17 PM
To: Cameron, Bud; Pitcher Robert; Dincoy, Rana
Subject: Re: Big ideas for strat products

Silly question, why not ask the clients?

[redacted]

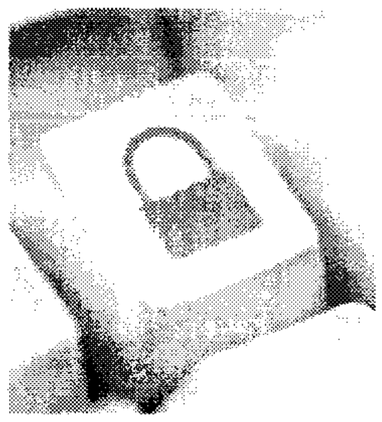
From: Cameron, Bud
Sent: Monday, October 31, 2011 02:20 PM
To: Pitcher Robert; Bendelier, Kenneth; Dincoy, Rana
Subject: Big ideas for strat products

Seeking your ideas for "issue of the month" type papers (Reports in the CCAP taxonomy).
DDOS, APT soon to be done, what other topics would be of interest and relevance to our clients?
I was thinking that one on Anonymous might be useful.
I will put the question to the Gov IRT forum and see what they say...

Bud Cameron, CD, MSc
Manager, Cyber Security Programs | Gestionnair, Programmes de sécurité cybernétique
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 +1 613-949-8317
Facsimile | Télécopieur +1 613-954-3097
Bud.Cameron@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-002



For the Week of

22 - 28 Oct 2011

Issued: 4 Nov 2011

HIGHLIGHTS:

- **Threat Warnings:**
  - Hacker group Anonymous urged sympathizers to participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5 - ITAC assesses the risk to be low.
- **Reported Incidents:**
  - Federal agency spammed with a suspicious e-mails referencing Gaddafi;
  - Targeted attacks on a Canadian Internet Service Provider's core infrastructure;
  - On-line recruitment of Canadian money launderers;
  - On-line posting of Canadian police personnel computer user information;
  - Computers in provincial governments, energy companies, universities and a hospital's networks compromised; and
  - Computer users lured to malicious web sites by threat actors impersonating reputable Canadian bank and airline organizations.
- **International News:** Chinese military suspected of hacking US satellites; Japanese missions around the world experienced targeted cyber attacks; Finland wants to build offensive cyber capability.

PURPOSE

UNCLASSIFIED
DRAFT

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered or reported to the Canadian Cyber Incident Response Centre (CCIRC), any notable international news and any CIRC information products issued during the week.

NOTABLE INCIDENTS– 22 THROUGH 28 OCTOBER 2011:

Government Systems.

Federal Government. CCIRC received a report of employees in a federal agency receiving e-mails, with the subject line referencing Mohammed Gaddafi and Allah. CCIRC forwarded information on this incident to the Cyber Threat Evaluation Centre (CTEC), the cyber incident handler for the federal government.

Analysis: CCIRC has no information to indicate whether this federal departmental was targeted specifically by these e-mails. However, referencing popular news items and events is a common tactic used to lure internet users into opening e-mails with malicious content.

Provincial Government. CCIRC received reports on potential compromises of computers on three provincial government systems.

Analysis: CCIRC has no information to indicate that these were targeted attacks on the provinces. Reports indicated that the computers in question were infected with malicious software commonly used by cyber criminals.

Police. CCIRC discovered that user account information for a number of Canadian police organizations was posted on a hacker website. CCIRC sent information to the RCMP for evaluation and notification of the affected police agencies.

Analysis: CCIRC has no information whether police computer networks were compromised as a result of this activity. A similar incident for a Canadian provincial police force and a number of American police organizations occurred earlier in 2011.

Canadian Critical Infrastructure:

Financial Sector.

Phishing. CCIRC received nine phishing reports and actioned the one that continued to pose a threat. In this incident, a threat actor, impersonating a well-known Canadian bank, was luring computer users via e-mail, to a website hosted in Australia. CCIRC notified the bank, Google phishing, the Anti-Phishing Working Group and Microsoft, so internet users may be alerted if they encounter these websites.

Threats by Anonymous. Anonymous, the famed hacker group, urged sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on November 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on November 5. As of the date of this writing, CCIRC learned the operation to hack the TMX computers on November 7 has been cancelled.

Analysis: Anonymous is a loosely organized hacker group that has the capacity to organize and launch a Distributed Denial of Service (DDOS) attack that could potentially bring down a website. However, the Integrated Threat Assessment Centre (ITAC) does not believe there is a high risk of a cyber attack on November 5.

When Anonymous called for a November 7 attack on the TMX computers, CCIRC contacted major Canadian financial institutions. They confirmed their awareness of the potential threat from Anonymous, and that their internet service providers were prepared to mitigate any DDOS attack. As of the date of this writing, the cyber attack on TMX has been called off.

On-line recruitment for money laundering. CCIRC learned of an on-line recruitment campaign in Canada for money laundering, originating from abroad. CCIRC sent summary and technical details sent to the RCMP Anti-fraud centre as well as the RCMP High-Tech Crime Branch for possible further investigation.

Telecommunications Sector.

Intrusion attempt – Internet Service Provider Core Infrastructure: A Canadian internet service provider informed CCIRC and other Canadian telecommunication companies about recent brute force hacking attempts against their routers, at the rate of 60-100 attempts each day. The attacks appear to be coming from internet service providers in China and Romania, but the attacker cannot be identified conclusively with the available information. The reporting internet service provider has taken mitigation measures.

Analysis: Routers of an internet service provider are used to route internet traffic of its subscribers, and possibly other internet users. Having control of a router on the Canadian telecommunication network would enable a hacker to intercept Canadians' communications and information going through that router, and use that information for a variety of malicious purposes.

Energy Sector. CCIRC received infection reports on computers of three energy sector organizations. These organizations are: A large of oil & gas producer, a service & equipment provider to the oil and gas sector, and a provincial electricity producer. CCIRC notified all three organizations of the potential infections.

Health. CCIRC received a computer infection report for a Canadian hospital and notified the organization's IT department.

Transportation. CCIRC received a report of phishing attempts in the aviation sector. Threat actors were seeking on-line customer credentials for an airline.

UNCLASSIFIED
DRAFT

CCIRC Product: CCIRC released Alert AL11-501 to IT professionals and managers in its stakeholder community. This Alert informs stakeholders about the work-around solution and update released by Entrust, created when it was discovered that a Java software updated interfered with the functionality of some Entrust products.

International News

Chinese military suspected of hacking US satellites. According to a publicized portion of the draft US-China Economic and Security Review Commission annual report, computer hackers, possibly from the Chinese military, interfered with two US government satellites four times in 2007 and 2008. There is currently no public information about the nature of the hackers' interference with these satellites, which are used for earth climate and terrain observations. The report, which is to be released next month, states the interferences occurred through a ground station in Norway.

Japanese missions around the world experienced targeted cyber attacks. Open sources report that at least dozens of computers used at Japanese missions in nine countries, including Canada, have been compromised since this past summer. Many of the compromises were found to allow a remote hacker to gain access and steal confidential information. The Japanese Foreign Ministry is investigating this incident and assessing its impact.

Finland wants cyber war weapons. Open sources report Finland has joined Sweden in planning to include counter-offensive capability for cyber attacks as part of its defence strategy. The new strategy would be presented to parliament and formalized in 2013.

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

NOTES

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 Flashed marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
10 Feb 2012	DirtJumper DDoS controller in Canada	2628	[redacted] s.19(1) s.20(1)(c)	Multiple	CCIRC received a request for assistance from CERT Australia in taking down Controller domain registered by a Canadian organization. [redacted] Whois comes back that EvoPlus LTD/evonames.com is the registrar. *Tech detail:* Network whois Ip: 195.3.147.30 AS41390 (Latvia, LV) Queried whois.evonames.com with "sadasdnwqjrrww.net"... Domain Name: SADASDNWQJRRWW.NET Abuse email: abuse@ru-tld.ru DOMAIN SUSPENDED DUE TO VIOLATION OF OUR TOS Registrant: [redacted] --Registrant is Ukranian CCIRC issued takedown request to EvoPlus, advised LE, CIRA and CERT Australia	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					Update: Site is now down	
7 Feb	Sendspace storing stolen data	2623			Canadian victims – 600 IP addresses Cyberflash sent 9 Feb 2012 "CCIRC has received reports of malicious activity involving the use of malware designed to collect and upload Microsoft Office documents to Sendspace.com. Sendspace is a file-hosting website that offers users the ability to send, receive, track and share large files. The attack begins by compromising the host with a malicious file named "Fedex_Invoice.exe". The file name used for this particular malware suggests that it is being used for a spam campaign, specifically one that uses messages disguised as a FedEx shipment notification. The malware attempts to access the following websites to download additional files: hxxp://south78483825.ru/hhh/index.php etc…. The malware searches the local drive of an affected system for Microsoft Word and Excel files. The documents are then archived and password-protected using a random-generated password in the user's temporary folder. After creating the archive, the malware	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					sends the archive to the Sendspace.com website. Upon successfully uploading the archive, the malware sends the generated download link and archive password to the C&C server: hxxp://south78483825.ru	
6 Feb	Fraudulent GoC website – possibly malicious	2621	Govt	N/A	Hosted in Dallas, Texas Was previously listed on MDL 2011/07/02 for trojan Renos Was previously on a malware list TrendMicro=Malicious site URL Query= malicious reputation TrustedSource=High Risk 61 domains also point to this IP address Murphy, Gregg (2/10/2012 1:11 PM): Sent request to CIRA asking for their assistance in deactivating the hrsdc-cic-gc[.]ca domain. Murphy, Gregg (2/6/2012 2:33 PM): Confirmed that site was collecting sensitive private information. Sent takedown request to abuse@softlayer.com and cc'd us-cert.	Ask Gregg what CIRA can do to deactivate the domain
8 Feb 2012	Possible APT Hop Host – Technology Institute	2624	Educational		Information received from a trusted source regarding a potential hop host in a post-secondary school ( ). Source recommended reviewing logs from that host for the past 2 weeks looking at port 443 traffic and any other unusual ports. No specific domains or IP addresses are	

s.16(2)(c)

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					available. It is suspected that during the early morning hours of Feb 6th, ftp activity using possibly valid credentials from unusual domains or IP addresses may have occurred. It is also suspected that changes were made to the server file store prior to Feb 6th. Suggested [redacted] review any changes to the file store or new ftp accounts that were recently created	
7 Feb 2012	Ransomware – GoC logos being used – CSIS logo	3458	Govt/Public	N/A	Reports of popups on computers saying they have been looking at child porn and their browser will be shut down unless they pay money. Logo for CSIS is being used on the messages. --Website hosted in Moldova Update: Passed to LE – RCMP investigating	
9 Feb 2012	Canadian IP listed on Zeus tracker	2626	N/A		It is part of a FastFlux botnet Hosting provider in BC, Drop URL is in Russia Email delivery to abuse contact failed. Emailed parent co. Sent takedown request to hosting provider, cc'd LE Incident now closed	
2 Feb 2012	Info compromise (Canadian Credit card info on Pastebin)	2616	General Public	Unknown	Appears to be a continuation of the Stratfor incident 6 Canadians listed in the post – they don't use GoC email addresses	
8 Feb	IRC botnet	3461	Energy		An energy partner ([redacted] reported that the Botnet in which they had participated three months ago was still active. (They provided information about an active IRC channel for the Raumoni Perl Bot controller). They were involved in a similar event 3	■

s.16(2)(c)
s.20(1)(c)

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					months ago (CE11-2508). CCIRC Ops asked Technical Team to investigate so that victims can be identified/notified. Bot channel:ircu.uk.to:81 [redacted]	
30 Jan	DNS Changer Malware	2605	Provincial govt (2), energy (1), finance (1), telecom (18), Health (1), Transport (1), universities (14), college/tech instit (2), other industries (1), other institutions (2)	43	It may be time to do some statistical analysis for who mitigated and who didn't… Luc dissuaded me last week.	Discuss with Editorial Board
1 Feb	DNS Changer Malware	2615	01B Provincial; 02A Telecoms; 02B Finance; 02C Energy; 02D Transportation; 02H Health; 05 Academia s.20(1)(c)		Notifications sent to IT security or technical contacts in the following organizations: Provincial: 2 provinces [redacted] Telecom: 17 companies [redacted] Finance: 2 banks [redacted] Energy: 2 company [redacted] Transportation: 1 company [redacted] Health: 2 organizations [redacted] Academia: 15 universities [redacted]	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					Laurentian, Laval, Memorial, Montreal, Ottawa, RISQ, St. FX, Toronto, Waterloo and Western Ontario)	
3 Feb	DNS Changer Malware	2619	01B Provincial; 02A Telecoms; 02B Finance; 02C Energy; 02D Transportation; 05 Academia		Provincial: 3 provinces (BC, EDNet NS and NB Department of Education) Telecom: 21 companies (Allstream, Bell, Broad-Connect, COGECO, EastLink, EIDNet Wireless, Fibrenoire Internet, iWeb, Mohawk Internet Technologies, MNSi Internet, Netelligent, Niagara Wireless, Northwestel, Primus, SASKTEL, Shaw, SOGETEL, TekSavvy, Thunder Bay Telephone, Urban Networks and Videotron) Finance: 1 bank (Scotiabank) Energy: 1 company (Ontario Hydro) Transportation: 1 company (Vancouver Airport) Academia: 12 universities (Brock, Calgary, Grant MacEwan, Manitoba, McGill, Montreal, Ottawa, RISQ, Toronto, Waterloo, Western Ontario and York) Thu 02/02/2012 2:47 PM **Media Report: Half of Fortune 500s, US Govt. Still Infected with DNSChanger Trojan** http://krebsonsecurity.com/2012/02/half-of-fortune-500s-us-govt-still-infected-with-dnschanger-trojan/	
7 Feb 2012	DNS Changer Malware	2622	Provincial, Telecom, Finance, Energy,	33	Dns-ok.ca site now up, hosted by CIRA CCIRC one of the four CERTS in the world	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
			Transportation, Education		that have this kind of site for public (NL, US, Germany)	
31 Jan	Phishing	2611	Financial	1	[redacted] – registrant of malicious website is in Russia Notification sent to Bank's phishing intake, google safe browsing & APWG	
1 Feb	Phishing	2612	Financial	1	[redacted] – registrar is in NL, hosted by AMEN France Network	
1 Feb	Phishing	2614	Financial	1	[redacted] – hosted in Colorado Reported by RCMP (still Anti-Fraud Centre?) Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE Hosted by NTT America, Inc in Greenwood Village, Colorado.	s.20(1)(c)
2 Feb	Phishing	2617	Financial	1	[redacted] Hosted in the US Notification sent to Bank's phishing intake, google safe browsing & APWG	
30 Jan 2012	Phishing	2602 & 2603	Financial		[redacted] site hosted in Colorado, USA Two Different IP addresses Reported to [redacted] phishing intake, Google Phishing Filter Service & APWG	
9 Feb	Phishing	2627	Financial	1	[redacted] hosted in Vietnam Couldn't notify APWG because we don't have enough info – only got the two links hxxp://www[.]dipcare[.]com[.]vn/WBB6/https/businessbanking[.][redacted].]com/WBB/ hxxp://www[.]tradecare.com[.]vn/WBB6/https/businessbanking[.][redacted].]com/WBB/	

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					Both links resolve to 203.162.71.16 AS7643 (Vietnam, VN)	
3 Feb	Phishing	2618	Financial	1	[redacted] hosted in the US Same domain we saw for [redacted] on previous day, same IP address	
6 Feb 2012	Phishing	2620	Financial	1	[redacted] - hosted in Berlin, Germany Notified [redacted] phishing intake, APWG, Google Safe Browsing	
30 Jan	Phishing	2604	Financial	1	[redacted] - site hosted in Berlin, Germany Reported to [redacted] phishing intake, Google Phishing Filter Service & APWG	
31 Jan	Phishing	2609	Financial	1	[redacted] site hosted in US Notification sent to Bank's phishing intake, google safe browsing & APWG	
31 Jan	Phishing	2068	Financial		[redacted] - site hosted in US Notification sent to Bank's phishing intake, google safe browsing & APWG	
31 Jan 2012	Website Defacement	2606	Provincial Govt (Dept Health)	1 [redacted]	Domain registered by the org listed on a well known defacement site as targeted for defacement using unspecified exploit techniques. Response from dept indicated defacement was identified by local IT staff on Sunday and default page was replaced with "under construction" until it was fixed by website support staff. No loss of personal data, no replacement of content. Website restored with correct permissions	

s.16(2)(c)
s.20(1)(c)

DATE	TYPE OF INCIDENT	INCIDENT/ACTIVITY #	SECTOR	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
31 Jan	Website defacement	2607	Website registered by a student & community organization		Sent notification to their hosting ISP [redacted]	
31 Jan	Website defacement	2610	Education	1 (the Pipeline Security Specialist training programme)	Notification sent to operator group and their hosting provider [redacted]	
1 Feb	Website defacement	2613	Health	1	[redacted] CCIRC observed that a website operated by/for the [redacted] medical centre was recently defaced. Notification sent to the domain technical contact ([redacted]	s.20(1)(c)
8 Feb	Website defacement –	2625	Govt		CCIRC observed that a website registered by a provincial government treasury department was recently defaced.	

Upcoming events:
Cyber security workshop – Toronto, Canada – 27-29 Feb 2012
Vulnerability: (second week of Feb)

- OSCommerce v3.0.2 – persistent cross-site scripting vulnerability
  - SPAM w child porn
  - Spoofing RCMP & CSIS
  - SQL injection attacks (Bruce) – not clear what the redirect does ACTION: Talk to Bruce

Cyber News from Dailys:

- **Millions caught up in Android botnet (30 Jan 2012) – Symantec found** trojan was packaged into at least 13 free games published by three different publishers on the official app download site – *not sure about the Canadian nexus, except that Canadians do use Android phones, and increasing malware for mobile phones is a trend that was spotted for 2012 by different security companies. Researchers from Lookout Security disagreed with Symantec saying it's just adware and not*

- **Anonymous hacks French Government Website as ACTA row rumbles on (31 Jan 2012)**
- **Many pcAnywhere systems still sitting ducks – more than 140,000 computers still at risk –** ACTION: CCIRC was supposed to ask for Canadian IPs. Follow up. (Note: This software still used by small businesses, early form of PC remote control for windows, probably still used for remote computer maintenance)
- **WikiLeaks buying boat to move servers offshore?** (2 Feb 2012)
- **Hackers exposing hate movements post names of 74 Canadians (Anonymous) 2 Feb 2012**
- **Google beefs up security on Android Market**
- **FBI Friday: Anonymous Hackers Release Internal Conference Call Recording**
- **DHS website hacked by Anonymous (7 Feb 2012) –** *website was back up within minutes* http://rt.com/usa/news/homeland-security-website-anonymous-473/
- **TeamPoison Hackers hit the UN (9 Feb 2012)**
- **Google to strip Chrome of SSL revocation checking – (9 Feb 2012).** The browser will stop querying CRL (certificate revocation lists and databases that rely on the Online Certificate Status Protocol – OCSP. Instead, Google will rely on its automatic update mechanism – maintain a list of certificates that have been revoked for security reasons. Google appealed to CA's to provide a list of those. This change will happen in months. ***This is potentially a new certificate model***

s.15(1) - Def

Moore, Bruce

From: Beaudoin, Luc S.
Sent: Friday, February 10, 2012 10:51 AM
To: Cameron, David M.; Turbide, Francois A; Moore, Bruce; Bendelier, Kenneth M.; Williston, Sandra
Subject: FW: Anonymous report

Classification: UNCLASSIFIED

very good spill on anonymous....

-----Original Message-----
From: [redacted] [mailto:[redacted]@cse-cst.gc.ca]
Sent: Thursday, February 09, 2012 12:26 PM
To: Beaudoin, Luc S.
Subject: Anonymous report

Classification: UNCLASSIFIED

Hi Luc,
Please find attached a copy of the Anonymous report. The report focuses on the tradecraft used, the targets and also the potential of GC being targeted.

<<Anonymous-CTA-GC-1111-01.DOC>>

Thank you for the information you had provided. It was very useful.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Beaudoin, Luc S.

From: [redacted]@cse-cst.gc.ca]
Sent: Thursday, February 09, 2012 12:26 PM
To: Beaudoin, Luc S.
Subject: Anonymous report

s.15(1) - Def
s.16(2)(c)

Anonymous-CTA-GC-1111-01.DOC (...

Classification: UNCLASSIFIED

Hi Luc,
Please find attached a copy of the Anonymous report. The report focuses on the tradecraft used, the targets and also the potential of GC being targeted.

<<Anonymous-CTA-GC-1111-01.DOC>>

Thank you for the information you had provided. It was very useful.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Beaudoin, Luc S.

From: [redacted]@cse-cst.gc.ca]
Sent: Thursday, November 10, 2011 11:13 AM
To: Beaudoin, Luc S.
Cc: [redacted]
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

Hi Luc,
I will talk to RCMP o[redacted]t, I am hoping to touch base with them next week. Would Thursday, Nov 17, at 11-12 work out for you? [redacted] would like to come by as well for this.

Thanks,
[redacted]

From: Beaudoin, Luc S. [mailto:l[redacted]
Sent: November 9, 2011 11:56 AM
To: [redacted] Singh, Gurbinder (RCMP); Alves de Jesus, Tiago (RCMP)
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

much more information on non-government targets. [redacted]

Could you come over here next week ? [redacted]

you should monitor the next Copyright-law debates related to digital content (Bill C-32 I believe)...UK and Aus equivalent of our intellectual property office (under IC I think) got attacked as soon as their equivalent laws came into effects.

L

-----Original Message-----
From: [redacted]@cse-cst.gc.ca]
Sent: Tuesday, November 08, 2011 3:38 PM
To: Beaudoin, Luc S.; [redacted] Singh, Gurbinder; Alves de Jesus, Tiago
Subject: RE: ANONYMOUS report

s.13(1)(a)
s.15(1) - Def
s.16(2)(c)

Classification: CONFIDENTIAL

Tiago, thank you for your response, please do pass along anything you find.
[redacted] thank you, for your response as well,

Luc, I was hoping to get a draft ready by the end of this month, this is an internal timeline and it is somewhat flexible. [redacted] If you do have some incidents that you suspect are Anonymous, I can work with you on trying to attribute them.

From: Beaudoin, Luc S. [mailto[redacted]
Sent: November 8, 2011 3:06 PM
To: [redacted]; Singh, Gurbinder (RCMP); Alves de Jesus, Tiago (RCMP)
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

CCIRC is interested in participating. We have had a number of incidents beleived to be associated with Anonymous. The danger is that we do not focus on attribution, so it may be difficult to validate the true actor behind some of these highly publicised events.

When do you need this by ?

-----Original Message-----
From: [redacted]@cse-cst.gc.ca]
Sent: Monday, November 07, 2011 4:43 PM
To: [redacted]Singh, Gurbinder; Alves de Jesus, Tiago; Beaudoin, Luc S.
Subject: ANONYMOUS report

Classification: CONFIDENTIAL

Hello,
I am the supervisor for [redacted] in CTEC. Your contact information has been

passed onto me by [redacted] My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

s.15(1) - Def
s.16(2)(c)

- Who are they
- Their targets
- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Beaudoin, Luc S.

From: [redacted]
Sent: Wednesday, November 09, 2011 10:07 AM
To: [redacted] Beaudoin, Luc S.; Singh, Gurbinder; Alves de Jesus, Tiago
Subject: RE: ANONYMOUS report

[redacted]

That is [redacted] is the my last name but that's OK

>>> "[redacted]cse-cst.gc.ca> 11/8/2011 3:37 pm >>>
Classification: CONFIDENTIAL

Tiago, thank you for your response, please do pass along anything you find. [redacted] thank you, for your response as well,

Luc, I was hoping to get a draft ready by the end of this month, this is an internal timeline and it is somewhat flexible. [redacted] If you do have some incidents that you suspect are Anonymous, I can work with you on trying to attribute them.

From: Beaudoin, Luc S. [mailto:[redacted]
Sent: November 8, 2011 3:06 PM
To: [redacted]; Singh, Gurbinder (RCMP); Alves de Jesus,

- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

s.15(1) - Def

s.16(2)(c)

Beaudoin, Luc S.

From: Alves de Jesus, Tiago [tjesus@rcmp-grc.gc.ca]
Sent: Tuesday, November 08, 2011 9:59 AM
To: [redacted] Singh, Gurbinder; Beaudoin, Luc S.
Subject: RE: ANONYMOUS report

Classification: CONFIDENTIAL

Good day,

The RCMP's NSCI program does not have any criminal intelligence, at this point in time, on ANONYMOUS. However, if any of our law enforcement partners, both domestic and International, pass on any information it would be my pleasure, if possible, to share it with you.

Have a great day,

Sincerely yours,

Tiago

Tiago Alves de Jesus,PhD
i/c Cyber Unit
National Security Criminal Operations
National Security Criminal Investigations
Royal Canadian Mounted Police

From: [redacted] cse-cst.gc.ca]
Sent: Monday, November 07, 2011 4:43 PM
To: [redacted] Singh, Gurbinder; Alves de Jesus, Tiago; Beaudoin, Luc S (GOC)
Subject: ANONYMOUS report

Classification: CONFIDENTIAL

Hello,

I am the supervisor for [redacted] in CTEC. Your contact information has been passed onto me by Chris Dugal. My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

- Who are they
- Their targets
- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

s.15(1) - Def

s.16(1)(c)

Beaudoin, Luc S.

From: [redacted]
Sent: Tuesday, November 08, 2011 [redacted]
To: [redacted] Beaudoin, Luc S.; Singh, Gurbinder; Alves de Jesus, Tiago
Cc: [redacted]
Subject: Re: ANONYMOUS report

[redacted]

Good morning [redacted]

[redacted]

>>> "[redacted]cse-cst.gc.ca> 11/7/2011 4:43 pm >>>
Classification: CONFIDENTIAL

Hello,
I am the supervisor for [redacted] in CTEC. Your contact information has been passed onto me by [redacted]. My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

> - Who are they
> - Their targets

> - Their tradecraft/behaviour (why do they target and when)
> - Canada related activities
> -Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

s.15(1) - Def

s.16(2)(c)

[redacted]

Beaudoin, Luc S.

From: [redacted]@cse-cst.gc.ca]
Sent: Monday, November 07, 2011 4:43 PM
To: [redacted] Singh, Gurbinder; Alves de Jesus, Tiago; Beaudoin, Luc S.
Subject: ANONYMOUS report

Classification: CONFIDENTIAL

Hello,
I am the supervisor for [redacted] in CTEC. Your contact information has been passed onto me by [redacted] My team will shortly start drafting a report focusing on the ANONYMOUS group. The basis of this report would be to understand the group and to assess the threat it poses to Canadian government.

A very rough format of the report is listed below:

- Who are they
- Their targets
- Their tradecraft/behaviour (why do they target and when)
- Canada related activities
-Immediate threat, and what would trigger them against us (this would be more of a prediction based on their historical behaviour)

Since your departments are interacting with clients at all levels, I was wondering if there would be anything you would be able to provide me with. Please let me know if you have any questions, concerns or where you can contribute.

Regards,

[redacted]

https://wiki.cse-cst.gc.ca/index.php/CTEC

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CTEC
CYBER THREAT EVALUATION CENTRE

ANONYMOUS

CTA-GC-1111-01

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2

OVERVIEW 3

STRUCTURE 3

CHOOSING TARGETS 4

PAST TARGETS/BEHAVIOUR 4

CANADA 8

TRADECRAFT 10

MITIGATION 12

The intended audience for this report is GC IT decision makers, security officers and technical practitioners.

EXECUTIVE SUMMARY

This report provides an overview of the hacktivist group, "Anonymous" and contains: information on its organizational structure, tradecraft, and targets; the threat to GC systems; and, CTEC's prevention and mitigation advice.

- "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 government regimes); and,
  - information accessibility (e.g. perceived government-mandated Internet censorship).
- Based on a view of previous targeting by "Anonymous", Government of Canada systems could be targeted due to:
  - government legislative initiatives (e.g. *Copyright Modernization Act*); and,
  - political initiatives that may result in activist opposition (e.g. environmental or social issues).
- Specific targets are chosen in a variety of ways, including:
  - through online polls following discussions in Internet Relay Chats (IRC[1]);
  - opposition to "Anonymous'" campaigns, such as the ongoing "Operation Anti-Security";
  - as a response to provocations made by companies, governments or other hacking groups; and,
  - as targets of opportunity, following searches for vulnerable systems.
- "Anonymous" uses a number of capabilities against its targets. These include, but may not be limited to Distributed Denial of Service (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 "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 federal departments 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 "zero-day[4]". Please refer to the "Mitigation" section and Annex 1 for details.

---

[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 denial-of-service (DoS) or a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised 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 to change the database content or to dump database information to the attacker.

OVERVIEW

Activist hackers have increasingly engaged in cyber threat activities to advance their own agendas. Most notably, "Anonymous" is a term that refers to a group of activist hackers, or "hacktivists," who pose 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-ops[5], LulzSec[6]) 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. In addition, the Anonymous movement has inspired copycat actions from other hacktivist groups, such as LulzRaft[7].

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.)

---

[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 website for the Conservative Party of Canada and for accessing private information about the party's donors. They have also been linked to web defacement of the website of Calgary-based energy company, Husky Energy.
[8] Unofficial spokespeople for Anonymous include Jake Davis (also known by his online nickname "Topiary,") Barrett Brown, etc. For more information on Jake Davis, please see http://nakedsecurity.sophos.com/2011/07/31/jake-davis-named-as-suspected-hacker-topiary-by-uk-police/. 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 which 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.

CHOOSING TARGETS

Since Anonymous is decentralized, new targets are determined in a variety of ways. Some of the most commonly utilized and documented methods of selecting targets are:

- through consensus among Anons using online polls. Following a discussion on an Internet Relay Chat (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; and,

- to "expose" poor security practices: for instance, Anonymous members may use "Google Hacking" to identify vulnerable targets of opportunity.

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. Its hacktivism efforts have recently been concentrated on the various Occupy[11] movements, on protesting Internet censorship and Internet filtering, on protesting against oppressive regimes, and on supporting WikiLeaks.

---

[10] HBGary Federal is a technology security company who 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, 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.

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 which it found embarrassing and was readily available on the Internet.

2009:

ANONYMOUS IRAN (Iran):

- *Action:* Creation of an Iranian Green Party Support site, Anonymous Iran, to provide covert resources and event updates to 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:* DDoS attack against the Australian Parliament's website and web defacement of the Prime Minister's website.
- *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 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].

[12] For more information, please refer to http://www.pcmag.com/article2/0,2817,2383018,88.asp.

OPERATION AVENGE ASSANGE (USA):

- *Action:* DDoS attacks against the 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 against the Government of the Republic of Zimbabwe's websites.
- *Reason:* To protest against censorship of WikiLeaks documents.

2011:

OPERATION TUNISIA (Tunisia):

- *Action:* DDoS attack on the Government of Tunisia's websites.
- *Reason:* To protest against Internet censorship; and to support the Arab Spring[13].

OPERATION SYRIA (Syria):

- *Action:* Web defacement of Syrian Defence Ministry website.
- *Reason:* To support the Arab Spring (Syrian uprising).

OPERATION EGYPT (Egypt):

- *Action:* DDoS attack against the Government of Egypt's website and the website of the National Democratic Party. Also released the names and passwords of email addresses of government officials.
- *Reason:* To support the Arab Spring (Egyptian revolution).

HBGARY FEDERAL (USA):

- *Action:* The defacement of HBGary's website, the deletion of company files and the publication of 68,000 employee emails.
- *Reason:* HBGary official provoked Anonymous by threatening to expose information about the group.

BANK OF AMERICA (USA):

- *Action:* The release of sensitive Bank of America documents online which allegedly prove cases of corruption and fraud at the bank.
- *Reason:* To protest in support of allegations of corruption and fraud within the US banking system.

---

[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.

OPERATION MALAYSIA (Malaysia):

- *Action:* DDoS attacks on 91 Government of Malaysia's websites.
- *Reason:* In response to the Malaysian government's censorship of sites like the Pirate Bay[14] and WikiLeaks.

OCCUPY WALL STREET (USA):

- *Action:* DDoS attacks 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 (USA):

- *Action:* The release of Guy Fawkes virus 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 (USA):

- *Action:* Domain name system (DNS) servers taken offline, removing Internet access for clientele in most of southwest America.
- *Reason:* To protest Cox Communications' attempted regulation of customer's data usage quota.

OPERATION BLACKOUT (USA):

- *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. 200 gigabytes of data were 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 governments and military departments). Anonymous planned to donate to charities using the stolen credit card information.

---

[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.

- *Reason:* Following the HB Gary 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 U.S. and elsewhere.[16]"

Ongoing:

OPERATION ANTISEC (NATO, Tunisia, Brazil, Australia, USA, Turkey, UK, and other countries):

- *Action:*
  - In USA: DDoS attacks against the Central Intelligence Agency's (CIA) website; the US Senate website was hacked, and information about its internal server structure was released.
  - In UK: DDoS attacks 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.

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].

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

[16] For the full explanation, please refer to Barret Brown's statement at http://www.zerohedge.com/news/anonymous-explains-why-27-million-stratfor-emails-were-hacked.
[17] CTEC has provided mitigation to employees of the affected departments.

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:

- In response to concerns about the environment, Anonymous has targeted companies related to the Keystone XL pipeline, and the Alberta Tar Sands project. Those targeted have included Canadian Oil Sands Ltd, Imperial Oil, Syncrude, and Suncor.

Future Activity
Although it is impossible to fully predict Anonymous' behaviour, based on prior targeting, there are a few government bills that would direct Anonymous' attention towards the Government of Canada.

Copyright Modernization Act:

- As a part of this bill, ISPs would be responsible for sending notices from copyright holders to Internet users alleged to have participated in illicit downloading and file-sharing online. The ISPs would also be required to retain records which establish the identity of the subscriber and disclose it in court if necessary. (Comment: This could be seen by Anonymous as an attempt to limit consumer rights. Previous protests against government-issued copyright laws in Australia and the USA resulted in Anonymous launching DDoS attacks on Australian government websites and the US Copyright Office.)

Lawful Access Package:

- The government's announcement to reintroduce Lawful Access legislation[18] that would require telecommunications companies, including ISPs to ensure intercept capabilities on their network. ISPs would also be required to disclose certain information on persons of interest to law enforcement authorities without a warrant under specific circumstances. (Comment: This could be seen by Anonymous as a violation of privacy. Similar perceptions have prompted Anonymous to take action against Facebook[19].)

[18] This legislation will be similar to the previous Bill C-50, Bill C-51 and Bill C-52.
[19] Operation Facebook was launched on November 5th, 2011 because Anonymous believes that "Facebook is the opposite of the Antisec cause."

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 includes a large number of members and all of their activities cannot be tracked and attributed to Anonymous.)

Open Source resources:

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:

1) LOIC:

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 would then disrupt the service of the victim's host. However, since LOIC could reveal the IP addresses of its users, it's traceability has prompted Anonymous to find other means of attacks.

2) Apache Killer:

The Apache DoS tool nicknamed the "Apache Killer" exploits a vulnerability which 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.

Anonymous-developed tools:

DoS/DDoS via SQL Injections:

#RefRef:

Anonymous developed and released a Perl DDoS tool in September, #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.

---

[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.

#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 anti-malware 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. HB Gary 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.

[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.

MITIGATION

Since Anonymous has a wide range of targets, it is difficult to measure which vulnerabilities are most frequently exploited by the group. However, as noted, the threats leveraged are generally limited to open source or well-known vulnerabilities. As a result, strong IT security practices will go a long way to defending against an Anonymous cyber threat.

In addition to best practices, including the implementation of CTEC's "Top 35 Mitigation Actions", the following mitigation is available for some of the tradecraft[23] specifically noted above:

1. DoS/DDoS attacks.
    a. Use network segmentation and segregation into security zones to protect high value assets using routers to spot and drop DDoS connections. For more information, please refer to number 16 of the "Top 35 Mitigation Actions" in Annex 1.
    b. If the DDoS is pointed at a specific IP, the target site could be blackholed. This typically requires working with upstream network providers to forward malicious traffic to a non-existent network interface, where the offending traffic will be dropped.
    c. In some cases, if a DDoS is anticipated, it may be possible to temporarily have additional bandwidth provisioned to your network. This will lessen the impact on the target for some DDoS incidents.

2. "Apache Killer."
    a. Apache has since released patches to fix this vulnerability. All users are recommended to upgrade to Apache 2.2.20 or higher. Also, please refer to the "Top 35 Mitigation Actions" numbers 1 and 2.

3. "#RefRef."
    a. Webcode should be hardened[24] against SQL injection to prevent the server from executing arbitrary SQL queries sent by unknown users.

Please see CTEC report "Government of Canada Top 35 Mitigation Actions, January 2012" for further information.

---

[23] Security analysts are still undergoing analysis on the Guy Fawkes virus; as such, we are unable to provide mitigation at this time. In addition, since URGE is not a hacking tool, there does not appear to be any mitigation actions provided at this time.
[24] Hardening minimises access between the public facing HTTP server and the SQL database. It also validates requests sent by external clients to the HTTP server.

Williston, Sandra

From:
Sent: February-10-12 6:42 PM
To:
Subject: RE: CIA Webstite Down

s.16(2)
s.19(1)
s.20(1)(c)

Ack. Tx.

From:
Sent: February-10-12 6:37 PM
To:
Subject: FW: CIA Webstite Down

FYI – Please see below

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: GOC-COG@PS-SP.GC.CA

From:
Sent: February-10-12 6:36 PM
To: GOC-COG; Darren.Sabourin@rcmp-grc.gc.ca; Kathy MacDonald; Scott.Foster@rcmp-grc.gc.ca; Tiago.Dejesus@rcmp-grc.gc.ca; tim.oneil@rcmp-grc.gc.ca
Subject: CIA Webstite Down

See: https://twitter.com/#!/YourAnonNews/status/168068014758039552 and http://rt.com/usa/news/anonymous-hacked-cia-hackers-049/

I attempted to access the site and it appears to be offline

[redacted]

s.20(1)(c)

Williston, Sandra

From: Mulder, Rene
Sent: February-10-12 11:06 AM
To: Bergeron, Dominic; Mack, Laurie; Bakri, Kareem
Subject: Re: Anonymous???

And... What about the anon chatter?

----- Original Message -----
From: Bergeron, Dominic
Sent: Friday, February 10, 2012 10:57 AM
To: Mulder, Rene; Mack, Laurie; Bakri, Kareem
Subject: RE: Anonymous???

Don't bother, daily reports are going to elio

-----Original Message-----
From: Mulder, Rene
Sent: February-10-12 10:57 AM
To: Mack, Laurie; Bergeron, Dominic; Bakri, Kareem
Subject: Anonymous???

I hear something's going on?
I'm gonna send Krul a report on XP systems. He just called me.

Mulder

s.16(2)(c)

Williston, Sandra

From: Bendelier, Kenneth
Sent: February-10-12 9:05 AM
To: Beaudoin, Luc
Subject: German Parliament

Of course, it's unconfirmed...

http://dagobertobellucci.wordpress.com/2012/02/08/germany-anonymous-hacks-into-german-parliament-website/

http://www.cyberwarzone.com/cyberwarfare/anonymous-hacks-german-parliament-website

http://www.mediafire.com/?lqmokhpicdqk69p

http://pastebin.com/[redacted]

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Williston, Sandra

From: Beaudoin, Luc
Sent: February-09-12 12:34 PM
To: [redacted]cse-cst.gc.ca' **s.15(1) - Def**
Subject: Re: Anonymous

Tx. I ll look it up...

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: [redacted]@cse-cst.gc.ca]
Sent: Thursday, February 09, 2012 12:28 PM
To: Beaudoin, Luc
Subject: RE: Anonymous

Hi Luc,
Just wanted to let you know that I have sent you a copy of the report on the high-side.

Thanks,
[redacted]

From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca]
Sent: November 17, 2011 2:19 PM
To: [redacted]@cse-cst.gc.ca'
Cc: [redacted]
Subject: Anonymous

some material to get you started....

consider this material FOUO within CSEC, containing 3rd party information exempted under section 20.1 and 13.1 of ATIA.

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

Dvorkin, Corey

From: Dvorkin, Corey
Sent: February-09-12 12:34 PM
To: Matz, Mark; Green, Amanda; Grigsby, Alexandre; Anderson, Ian; Bradley, Kees; Mohammed, Melanie
Cc: Gordon, Robert; Paul.Charlton@international.gc.ca; DONALD.NEILL@forces.gc.ca; SARA.SIXSMITH@forces.gc.ca
Subject: Worldwide Threat Assessment of the US Intelligence Community

http://www.dni.gov/testimonies/20120131_testimony_ata.pdf

Cyber is on pages 7-8

Alex: notice an entirely different approach as compared to a document we were just discussing.

Major Trends

Cyber threats pose a critical national and economic security concern due to the continued advances in—and growing dependency on—the information technology (IT) that underpins nearly all aspects of modern society. Data collection, processing, storage, and transmission capabilities are increasing exponentially; meanwhile, mobile, wireless, and cloud computing bring the full power of the globally-connected Internet to myriad personal devices and critical infrastructure. Owing to market incentives, innovation in functionality is outpacing innovation in security, and neither the public nor private sector has been successful at fully implementing existing best practices.

The impact of this evolution is seen not only in the scope and nature of cyber security incidents, but also in the range of actors and targets. In the last year, we observed increased breadth and sophistication of computer network operations (CNO) by both state and nonstate actors. Our technical advancements in detection and attribution shed light on malicious activity, but cyber intruders continue to explore new means to circumvent defensive measures.

Among state actors, China and Russia are of particular concern. As indicated in the October 2011 biennial economic espionage report from the National Counterintelligence Executive, entities within these countries are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property.

Nonstate actors are also playing an increasing role in international and domestic politics through the use of social media technologies. We currently face a cyber environment where emerging technologies are developed and implemented faster than governments can keep pace, as illustrated by the failed efforts at censoring social media during the 2011 Arab Spring revolutions in Tunisia, Egypt, and Libya. Hacker groups, such as Anonymous and Lulz Security (LulzSec), have conducted distributed denial of service (DDoS) attacks and website defacements against government and corporate interests they oppose. The well publicized intrusions into NASDAQ and International Monetary Fund (IMF) networks underscore the vulnerability of key sectors of the US and global economy.

Hackers are also circumventing network security by targeting companies that produce security technologies, highlighting the challenges to securing online data in the face of adaptable intruders. The compromise of US and Dutch digital certificate issuers in 2011 represents a threat to one of the most fundamental technologies used to secure online communications and sensitive transactions, such as online banking. Hackers also accessed the corporate network of the computer security firm RSA in March 2011 and exfiltrated data on the algorithms used in its authentication system.

Subsequently, a US defense contractor revealed that hackers used the information obtained from RSA to access its network.

Outlook

We assess that CNO is likely to increase in coming years. Two of our greatest strategic challenges regarding cyber threats are: (1) the difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively attributing them, and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks; and (2) the highly complex vulnerabilities associated with the IT supply chain for US networks. In both cases, US Government engagement with private sector owners and operators of critical infrastructures is essential for mitigating these threats.

Corey Michael Dvorkin
Senior Strategist / Conseiller principale
Cyber Policy / Politiques cyber
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 OP8
Tel: (613) 990-9608
corey.dvorkin@ps-sp.gc.ca

Dvorkin, Corey

From: Katie.Tolan@international.gc.ca
Sent: February-09-12 12:21 PM
To: Danaitis, Algis; Gordon, Robert; Bokwa, Lisa; Bolton, Stephen; Komm, Chantelle; Larose, Charlene; Currie, Chris; Dvorkin, Corey; Oldham, Craig; Durand, Stéphanie; Galadza, Larisa; Matrisciano, Giovanni; 'Glen.Linder@ps-sp.gc.ca'; Grabs, Robert; Veysey, Gregory; Randall, Jacqueline; Schwartz, Jo-Ann; Spallin, Julie; Moreau, Ken; Khouri, Lisa; Kubicek, Brett; Clairmont, Lynda; MacKinnon, Paul; Senft, Matthew; McAllister, Andrew; MacDonald, Michael; Namercia.DosSantos@ps-sp.gc.ca; Nap, Carole; Filion, Nathalie; Pagotto, Paul; Davies, Patricia; DesRochers, Patrick; Julianne Prokopich; Dincoy, Rana; Banerjee, Ritu; Lesser, Robert; Astravas, Rutha; Beaudoin, Serge C; Taschereau, Marc; Theilmann, Mike; Tolan, Katie; Jarmyn, Tom; Veilleux, Martine; Mahu, Vlad; Wong, Hazel; Wong, Suki; Leguerrier, Yves; Zuccolo, Claudia; Motzney, Barbara; Travers, Evan; 'Fergal.O'Reilly@ps-sp.gc.ca'; Green, Amanda; De Santis, Heather; Hirsch, Darryl; Davies, John; Kingsley, Michèle; Mohammed, Melanie; Thalakada, Nigel; Plunkett, Shawn; Bhupsingh, Trevor; Vershinin, Sergey
Cc: Julianne Prokopich
Subject: WASHINGTON UPDATE JAN 31-FEB 8, 2012
Attachments: 020912 CQ - Collins to File Backscatter Radiation Study Bill.docx; 020912 CQ - Cyber Bill Progress - Reid Is Fundamental.docx; 020912 CQ - Intel Agencies Working on Common IT Platform Internal Threat Detection.docx; 020912 CQ - Study Evaluates International Cybersecurity Preparedness.docx; 020912 CQ -Feasibility of Radiation-Scanning Mandate for Cargo Questioned.docx; 020912 CQ-Republican Pressure Builds on Holder.docx; 020912 Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps.docx

SUMMARY OF KEY ITEMS OF INTEREST:

PEOPLE: (1) **ICE Director John Morton** FEB 7 announced the appointment of **Andrew Lorenzen-Strait** as the **public advocate**. Lorenzen-Strait will be responsible for helping the public understand the prosecutorial discretion policy and other changes as well as addressing complaints about the changes (See ICE Section) (2) The Department of Justice announced FEB 3 **Luke McCormark** will become the DOJ's new chief information officer, starting in late March. (See DOJ Section)

STATEMENT FOR THE RECORD ON THE WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY: Director of National Intelligence (DNI) James R. Clapper delivered an unclassified **Statement for the Record on the Worldwide Threat Assessment** of the US Intelligence Community for the **Senate Select Committee on Intelligence** JAN 31. This statement provides extensive detail about numerous state and nonstate actors, crosscutting political, economic, and military developments and transnational trends, all of which constitute the nation's strategic and tactical landscape. The 30 page statement asserts that although **counterterrorism, counterproliferation, cybersecurity, and counterintelligence are at the immediate forefront of our security concerns**, the DNI notes that it is virtually impossible to rank—in terms of long-term importance—the numerous, potential threats to US national security. The United States no longer faces—as in the Cold War—one dominant threat. Rather, it is the multiplicity and interconnectedness of potential threats—and the actors behind them—that constitute the biggest challenge. Indeed, even the four categories noted above are also inextricably linked, reflecting a quickly changing international environment of rising new powers, rapid diffusion of power to nonstate actors and ever greater access by individuals and small groups to lethal technologies. DNI Clapper spoke of the duty of professionals in the Intelligence Community (IC) to work together as an integrated team to understand and

master this complexity. By providing better strategic and tactical intelligence, members of the IC can partner more effectively with other Government officials at home and abroad to protect vital national interests. In delivering the shorter, more succinct prepared remarks to the Committees, the DNI began by highlighting the global issues of Terrorism and Proliferation followed by a discussion of cyber threats. Excerpts follow.

The assessment within the Intelligence Community, according the DNI Clapper, sees the next two or three years as a **critical transition phase for the terrorist threat**, particularly for al-Qa'ida and like-minded groups. With Usama bin Ladin's death, the global jihadist movement lost its most iconic and inspirational leader. The new al-Qa'ida commander is less charismatic, and the death or capture of prominent al-Qa'ida figures has shrunk the group's top leadership layer. However, even with its degraded capabilities and its focus on smaller, simpler plots, al-Qa'ida remains a threat. As long as pressure is sustained on it, DNI noted the judgement that core al-Qa'ida will be of largely symbolic importance to the global jihadist movement. But regional affiliates, as the ones mentioned , and to a lesser extent, small cells and individuals, will drive the global jihad agenda.

Proliferation – that is, efforts to develop, acquire, or spread weapons of mass destruction – is also a **major global strategic threat.** Among nation-states, Iran's technical advances, particularly in uranium enrichment, strengthen the U.S. assessment that Iran is well capable of producing enough highly enriched uranium for a weapon, if its political leaders, specifically the Supreme Leader himself, choose to do so. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, illustrate the reach of the North's proliferation activities. DNI Clapper noted that there is no expectation Kim Jong Un, North Korea's new young leader, to change Pyongyang's policy of attempting to export most of its weapons systems.

Of interest, this year's **Statement for the Record, elevated the discussion of Cyber Threats to follow Terrorism and Proliferation.** The cyber threat is one of the most challenging ones faced. The DNI spoke of foreseeing a cyber environment in which emerging technologies are developed and implemented before security responses can be put in place. Among state actors, the U.S. IC is particularly concerned about entities within China and Russia conducting intrusions into U.S. computer networks and stealing U.S. data. And the growing role that non-state actors are playing in cyberspace is a great example of the easy access to potentially disruptive and even lethal technology and know-how by such groups. **Two of the greatest strategic cyber challenges are: First, definitive, real-time attribution of cyber attacks – that is, knowing who carried out such attacks and where these perpetrators are located. And second, managing the enormous vulnerabilities within the I.T. supply chain for U.S. networks**. (See ODNI Section for related links)

THIS WEEK IN WSHDC:

FEB 7 –Less than two months after American troops left, the State Department is preparing to slash by as much as half the enormous diplomatic presence it had planned for Iraq, a sharp sign of declining American influence in the country. Article

FEB 7 – Symantec confirmed that the pcAnywhere source code published on the Web Monday by hackers who tried to extort $50,000 from the company was legitimate. A company spokesman also said that Symantec expects that the rest of the source code stolen from its network in 2006 will also be made public. Article

FEB 7 – The director of the CIA, David H. Petraeus, may visit Myanmar later this year, officials said, in what would be the latest signal of warming relations with the United States as Myanmar emerges from years of military rule and diplomatic isolation. Article

FEB 6 – The Obama administration has closed the U.S. Embassy in Damascus and pulled all American diplomats out of Syria. Article

FEB 4 – Saboteurs stole passwords and sensitive information on tipsters while hacking into the websites of several law enforcement agencies worldwide in attacks attributed to the collective known as Anonymous. Breaches were reported this week in Boston, Syracuse, New York, Salt Lake City and Greece. Anonymous also published a recording on the Internet FEB 3 of a phone call between the FBI and Scotland Yard, gloating in a Twitter message that "the FBI might be curious how we're able to continuously read their internal communications for some time now." Article

FEB 2 –The Obama administration has more than doubled, to about 21,000 names, its secret list of suspected terrorists banned from flying to or within the United States, including about 500 Americans, The Associated Press has learned. The government lowered the bar for the list, even as it says it is closer than ever to defeating al-Qaida. Article

FEB 1 – China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal. Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms as well as Canada's Finance Ministry and the Treasury Board, according to Daniel Tobok, president of Toronto-based Digital Wyzdom. His cyber security company was hired by the law firms to assist in the probe. Article

JAN 31 –Some senior Iranian leaders are now more willing to carry out attacks inside the United States in response to perceived American threats against their country, Director of National Intelligence James R. Clapper Kr., said in prepared testimony to the Senate Intelligence Committee, pointing to last fall's suspected assassination plot against the Saudi ambassador to Washington. Article

WHITE HOUSE:

FEB 6 – President Obama issued additional sanction on the Government of Iran and Iranian financial institutions. Executive Order | President Obama's Statement on Syria

FEB 3 – President Barack Obama continued his commitment to improving employment among veterans by introducing an initiative to hire them as the country's first responders. Press Release

JAN 30 –In a rare official discussion of the covert drone program run by the CIA, President Barack Obama defended the United States' use of drones to strike suspected terrorists in Pakistan and elsewhere during a live web interview. Obama maintained that the drone program has not been responsible for a "huge" number of civilian casualties, and is "kept on a very tight leash" so as to be extremely targeted toward "active terrorists." Article

DHS:

FEB 7 – Joint testimony of David Heyman, Assistant Secretary for the Office of Policy, Rear Admiral Zukunft, Assistant Commandant for U.S. Coast Guard Office of Marine Safety, Security and Stewardship, and Kevin McAleenan, Acting Assistant Commissioner for U.S. Customs and Border Protection Office of Field Operations before the House Committee on Homeland Security, Subcommittee on Border and Maritime Security addressing supply chain security.

FEB 3 – Rand Beers, National Protection and Programs Directorate Under Secretary, before the House Committee on Energy and Commerce, Subcommittee on Environment and the Economy regarding the Department of Homeland Security's efforts to regulate the security of high-risk chemical facilities under the Chemical Facility Anti-terrorism Standards. Testimony

FEB 3 - Testimony of Alan Cohn, Policy's Deputy Assistant Secretary for the Office of Strategic Plans, before the House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management regarding how DHS is implementing a strategy to counter emerging threats. Testimony

FEB 1 –Secretary Janet Napolitano traveled to Indianapolis to highlight the Department's "If You See Something, Say Something™" public awareness campaign's continued partnership with the National Football League (NFL) to help ensure the safety and security of employees, players and fans during the regular season, and Super Bowl XLVI. Press Release

JAN 31 – As part of these ongoing efforts and in recognition of the one-year anniversary of the White House Startup America Initiative, the DHS announced a series of administrative reforms which will be completed in the future. These reforms reflect the Administration's continuing commitment to attracting and retaining highly-skilled immigrants. Fact Sheet

JAN 30 –DHS Secretary Janet Napolitano delivered the second annual State of Homeland Security Address at the National Press Club in Washington, DC. Napolitano's address highlighted DHS's accomplishments over the past year, and its goals and priorities going forward. Transcript of Address | Video – includes Q&A | The Hill

CBP:

FEB 6 – CBP announced the release of the updated Bonded Warehouse Manual for Customs and Border Protection Officers and bonded Warehouse Proprietors. Bonded Warehouses provide storage facilities for imported cargo that is pending importation into or exportation from the United States. The Bonded Warehouse Manual was last updated in 1990. Press Release

FEB 6 –DHS Secretary Janet Napolitano issued a final rule in the Federal Register which will permanently establish the Global Entry Trusted Traveller Program. FedReg Notice

JAN 31 – The work of CBP featured prominently in Homeland Security Secretary Janet Napolitano's address to Washington, D.C., journalists as she described how "our homeland security and our economic security go hand in hand." Press Release

JAN 31 - CBP and the Kootenai Tribe of Idaho announced the publication of a notice in the Federal Register designating the Kootenai Enhanced Tribal Card (ETC) as a travel document acceptable for entering into the United States through a land or sea port of entry. Press Release

ICE:

FEB 7 –ICE Director John Morton announced the department's first Public Advocate, ICE Senior Advisor Andrew Lorenzen-Strait. Lorenzen-Strait will serve as a point of contact for individuals, including those in immigration proceedings, non-governmental organizations and other community and advocacy groups, who have concerns, questions, recommendations or other issues they would like to raise. Blog Post Article

FEB 2 – Special agents and officers seize more than $4.8 million in fake NFL merchandise and seize 307 websites during 'Operation Fake Sweep' in Indianapolis. Press Release

FEB 2 – Five Los Angeles-area residents have been indicted for operating a human smuggling scheme that relied largely on non-Spanish speaking African-Americans to transport loads of illegal aliens from the U.S.-Mexico border to the Los Angeles area. Press Release

TSA:

FEB 8 –DHS Secretary Janet Napolitano and TSA Administrator John S. Pistole announced the expansion of TSA Pre√™, a passenger pre-screening initiative, to additional airports across the country following the program's success at seven pilot locations, including Baltimore/Washington International and Dulles. Press Release

FEB 7 –Testimony of John Pistole, Administrator of the Transportation Security Administration before the House Committee on Homeland Security, Subcommittee on Transportation Security addressing the TSA Screening Partnership Program.

ODNI:

JAN 31 – Unclassified statement and remarks delivered on the Worldwide Threat Assessment of the Un Intelligence Community for the Senate Select Committee on Intelligence. [See attached for transcript] Threats from cyber-espionage, computer crime, and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States, FBI Director Robert Mueller testified. Mueller along with ODNI Clapper spelled out for senators on the dire national security implications of threats to U.S. computer networks. But efforts to move a comprehensive cybersecurity bill through the chamber are still meeting resistance. ABC News

JAN 26 - In a tight budget environment, communication and collaboration have become more important to intelligence work than ever, and agencies are working on solutions such as an integrated, cross-agency information technology platform, Director of National Intelligence James Clapper said. (See attached for CQ Article)

DOJ:

FEB 4 – Attorney General Holder delivered remarks at the American Bar Association's National Summit on Indigent Defense in New Orleans.

FEB 3 – Attorney General Holder delivered remarks on "the sacred covenant" between citizens and their government at Tulane University's Law School. Remarks

FEB 3 – Luke McCormark will become the DOJ's new chief information officer, starting in late March. Press Release

FEB 2 – Attorney General Holder testified before the House Committee on Oversight and Government Reform on standards of integrity and professional at the DOJ.

AFGHANISTAN/PAKISTAN WAR:

FEB 7 –The CIA is expected to maintain a large clandestine presence in Iraq and Afghanistan long after the departure of conventional U.S. troops as part of a plan by the Obama administration to rely on a combination of

spies and Special Operations forces to protect U.S. interests in the two longtime war zones, U.S. officials said. Article

FEB 2 –Defense Secretary Leon Panetta said FEB 1 that the United States could end its combat mission in Afghanistan as early as mid-2013, more than a year before the deadline President Barack Obama laid out for withdrawing all U.S. troops from the country. His comments were the first time a U.S. official had put a date on when the United States would relinquish its central role in the conflict. Panetta said that the U.S. troops would play an "advise and assist" role to Afghan forces after mid-2013. Article

GAO

FEB 7 –Supply Chain Security
Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning
GAO-12-422T

FEB 3 –Department of Homeland Security
Additional Actions Needed to Strengthen Strategic Planning and Management Functions
GAO-12-382T

JAN 25 - Over the past decade, the DHS has spent more than $70 million assessing the effects of chemical, biological and radiological weapons. Yet that work has only guided only a portion of the department's emergency response plans, according to the GAO. Report

CONGRESS:

FEB 8 – The Subcommittee on Communications and Technology held a hearing on "Cybersecurity: Threats to Communications Networks and Private-Sector Responses."

Opening Statements: Chairman Walden

Witness List:

Larry Clinton, President and CEO, Internet Security Alliance

Bill Connor, President and CEO, Entrust

Robert Dix, Vice President of Government Affairs & Critical Infrastructure Protection, Juniper

James Lewis, Director and Senior Fellow, Technology and Public Policy Program, CSIS

Phyllis Schneck, Vice President and CTO, Global Public Sector, McAfee Inc.

FEB 7 –With five months until the DHS hits its deadline for scanning all U.S.-bound cargo for radiation, lawmakers are again floating the idea of ditching the mandate because of high costs, technological challenges and logistical issues, which remains far from being fulfilled. Based on the roughly $120 million the government has spent on six cargo-scanning pilot programs, DHS estimates the cost of full compliance to be around $16.8 billion, said Kevin McAleenan, acting assistant commissioner of CBP's Office of Field Operations. [See attached for CQ article]

FEB 6 –The House Homeland Security Subcommittee on Cyber-Security, Infrastructure Protection and Security Technologies marked up the cyber-security bill sponsored by Rep. Dan Lungren (R-Calif.) and unanimously approved it FEB 1. Lungren's Promoting and Enhancing Cyber-Security and Information Sharing Effectiveness Act (PRECISE). Article

FEB 3 –A growing chorus of House Republicans is supporting a legislative effort to express dissatisfaction with the job performance of Attorney General Eric H. Holder Jr. In late January, six lawmakers added their names to the list of cosponsors of a no-confidence resolution (H.R. 490) against Holder. It currently totals 90 GOP members. The lead sponsor, Rep. Paul Gosar, R-Ariz., has criticized the attorney general, saying Holder hasn't cooperated with congressional inquiries about the botched Bureau of Alcohol, Tobacco, Firearms and Explosives operation known as "Fast and Furious." [See attached for CQ article]

FEB 2 –The nation's spymaster said that his "highest legislative priority" is to extend surveillance powers Congress gave the intelligence community in a 2008 law. Committees in both the House and the Senate have already begun talks to grant his wish. [See attached for CQ article]

FEB 1 –Senator Susan Collins, ranking Republican on the Homeland Security and Governmental Affairs Committee, and a bipartisan group of her colleagues - Daniel Akaka (D-Hawaii), Carl Levin (D-Mich.), Tom Coburn (R-Okla.), and Scott Brown (R-Mass.) – introduced legislation to require an independent study of backscatter x-ray scanners and to require signs to alert travelers they have screening alternatives other than the backscatter machines. Article

JAN 30 - It's unusual for a Senate majority leader to become personally invested in a major legislative effort on a complex and technical topic with no obvious political payoff, particularly in an election year. But as the Senate tries to assemble a major bill to overhaul the nation's cyberdefenses, Nevada Democrat Harry Reid has emerged as the focal point. (See attached for CQ Article)

UPCOMING HEARINGS:

FEB 15 @ 2:30pm – The House Committee on Homeland Security will hold a hearing on, "An Examination of the President's FY2012 Budget Request for the Department of Homeland Security." 311 Cannon Bldg

FEB 16 @ 10:00am – The House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence will hold a hearing on "DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy" 311 Cannon Bldg

THINK TANKS:

FEB 7 – A study entitled *Muslim-American Terrorism in the Decade Since 9/11* study by Charles Kurzman from the Triangle Center on terrorism and Homeland Security at the University of North Carolina, Chapel Hill was released FEB 7.

FEB 2 – James Carafano and Jessica Zuckerman from The Heritage Foundation released commentary on the contradictory legislation governing cargo transit and port security, saying Congress should move toward fostering a more risk-based approach.

JAN 31 – Paul Rosenzweig from The Heritage Foundation published a WebMemo on the promoting cybersecurity through the PRECISE Act.

JAN 30 – Ben Rhodes, White House Deputy National Security Advisory for Strategic Communications discusses new national security challenges facing the Obama Administration at the Center for American Progress. Video

JAN 2012 - Heather Conley of the Center for Strategic and International Studies argues that U.S. Arctic policy must be given a sense of urgency and focus. This report analyzes the drivers of change in the region, examines the key Arctic security actors and institutions and explores the potential for a new security architecture for the Arctic. Read

JAN 2012 - Edward Alden and Bernard Schwartz of the Council on Foreign Relations report that the United States is getting ever closer to creating a system in which it will be more or less impossible to lie one's way into this country through the legal ports of entry. Read

JAN 30 –Two of the most feared aggressors in the cybersecurity world, Russia and China, lag behind the United States and other nations when it comes to digital defenses, according to a new study commissioned by the network security firm McAfee. [See attached for CQ article]

FEB 1 –Nearly a third of all terrorist attacks from 1970 to 2008 occurred in just five metropolitan U.S. counties, but terrorist events continue to occur in rural areas as well; there are 3,143 counties in the United States; researchers found 65 of these counties to be hot-spots for terrorism, that is, each of these counties experienced a greater than the average number of terrorist attacks between 1970 and 2008. Findings were found in a report published by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland.

JAN 31 –Companies including utilities, banks and phone carriers would have to spend almost nine times more on cybersecurity to prevent a digital Pearl Harbor from plunging millions into darkness, paralyzing the financial system or cutting communications, a Bloomberg Government study found. To achieve security capable of stopping 95 percent of attacks – considered by the Traverse City, Michigan-based Ponemon Institute to be the highest attainable level – those surveyed said they would have to boost spending to a group total of $46.6 billion from the current $5.3 billion. [See attached for article and related documents available on request]

UPCOMING EVENTS:

FEB 13 from 9:00-1:00pm– CSIS will host an event on, "Maritime Security: Confronting New and Non-Traditional Challenges in the Age of Austerity." Location: 1800 K St. NW B1 Conference Room

FEB 13 from 12:00-1:30pm – The Hudson Institute will host an event on, "Recent Developments in Cyberwarfare." Gen. James Cartwright (USMC, ret.) who served as Commander of the U.S. Strategic Command will deliver the keynote address. Location: 1015 15th St., NW 6th floor

FEB 22 from 10:00-12:00pm- the HSPI will host "A Conversation on Cyber Security Legislation with Michael Chertoff and Michael McConnell. Location: 1957 E St., NW 7th Floor RSVP

FEB 22 from 10:30-12:00pm – The Bipartisan Policy Institute will host FCC Chairman Julius Genachowski who will address new cyber security policies. Location: 1225 Eye St., NW Suite 1000

ARTICLES/ REPORTS OF INTEREST:

FEB 6 –A Look at the Secretive World of Air Marshals. CBS News. Article/Video

FEB 6 – U.K. Grants Bail to Radical Muslim Cleric. The Wall Street Journal. Article

FEB 4 – Border Patrol OT Up As Arrests Drop. Associated Press. Article

JAN 25 – The National Northern Border Counternarcotics Strategy: Closing a Window of Criminal Opportunity. HSPI: Security Debrief. Article

JAN 23 - The Next Homeland Security Secretary. Defense Media Network. Article

Kathleen Tolan
Counsellor
Public Safety and Border Security
Public Safety Canada
501 Pennsylvania Avenue, N.W.
Washington, D.C. 20001-2114
Tel: (202) 448-6338 Cell: 202 497-5898
Fax: (202) 682-7792
Email: katie.tolan@international.gc.ca

Williston, Sandra

From: Moore, Bruce
Sent: February-06-12 7:50 AM
To: [redacted]
Subject: FW: Anonymous info..

s.13(1)(a)
s.15(1) - Int'l
s.16(2)(c)

From CPNI.

Bruce

-----Original Message-----

[redacted]

[redacted]

s.13(1)(a)

Williston, Sandra

From: [redacted]
Sent: February-05-12 7:26 PM
To: Listserver NCSIP
Subject: Anonymous hacks Police websites, FBI

s.13(1)(a)
s.16(2)(c)

This message sent from: [redacted]

---

http://www.cbc.ca/news/technology/story/2012/02/03/tech-anonymouse-hacking-fbi.html

[redacted]

You are currently subscribed to [redacted]

To unsubscribe click here:
[redacted]
(It may be necessary to cut and paste the above URL if the line is broken)

or send a blank email to l[redacted]

Anderson, Windy

From: Bendelier, Kenneth
Sent: February-03-12 9:08 AM
To: [redacted]
Subject: Well, if anyone is looking to understand Anonymous TT&P

s.16(2)(c)

Description:
6 FEBRUARY 15 Action against Mining and Energy companies in South America.

Press: [redacted]

OpAmaZonaSave 3.0 - 06 February 15.00 gmt +1 [redacted]

Operation Green Rights [redacted]3.0 We start Soon! STAY TUNE for info about Operation.
6 FEBRUARY 15 gmt +1 [STATUS] STAY TUNE!! Press: [redacted]

HOW CAN I HELP ?

We need to investigate! Be creative!

INFO-BLOG:[redacted]
PRESS: [redacted]
on pastebin: (OpAmaZonaSave) [redacted] OpAmaZonaSave 2.0) [redacted] (OpAmaZonaSave 3.0) Message FOR Brazilian Government)
Manifesto: [redacted]
Twitter: [redacted]
Facebook: [redacted]
YouTube: [redacted]

PETITION against Belo Monte DAM (please sign) :) is one of the best weapon!
[*] [redacted]
[*]
[*]

INFO WEB(all links): http://titanpad.com/v8uczkqdQ0

IRC CHANNELL:

[redacted]

Targets Hacks & Vulnerable Links & HOW TO DDOS: [redacted]

VARIOUS GUIDE :

[redacted]

[redacted] s.16(2)(c)

If you need help of any kind /join #help

FAX - EMAIL - ATTACK: [redacted]

******HELP US!****** by MacKen

Source: [redacted]
Operation Green Rights [redacted] 3.0 We start Soon! STAY TUNE for info about Operation.
6 FEBRUARY 15 gmt +1 [STATUS] STAY TUNE!! Press: [redacted] (scroll down) please suggest new target!

******HELP US!******

We need to investigate! Be creative!

a.. INFO_BLOG: [redacted]
PRESS: [redacted]

on pastebin: (OpAmaZonaSave 1.0)
[redacted] (OpAmaZonaSave 2.0)
(OpAmaZonaSave 3.0)
(Message FOR Brazilian Government)
a.. FBpage:http://www.facebook.com/pages/Operation-Greenrights/168717439855964
a.. video 2.0: spread this [redacted]

PETITION against Belo Monte DAM (please sign) :) is one of the best weapon!
a.. [*] [redacted]
a.. [*]
a.. [*]

INFO WEB(all links): [redacted]

CABLE WIKILEAKS [redacted] (help to translate) !

a.. on pastebin [redacted]
a.. [redacted]
a..
a..

Targets Hacks & Vulnerable Links & HOW TO DDOS:
[redacted]

If you need help of any kind /join #help

FAX - EMAIL - TEL - ATTACK: [redacted]

Please suggest new targets ! POOL SOON!!! VOTE on possible other op

TARGET LIST and INFO (thanks) **s.16(2)(c)**

a.. www.agbioworld.com - Bio-Tech-->more info
a.. www.cmrlink.org - hate group -->more info http://www.ezemvelo.co.za/ -for the inhumane money tendor put out *to kill rhino for money.*

please watch this h[redacted] Wealthy man pays to kill rhino to corrupt owner of Ezemvelo nature reserve - WARNING GRAPHIC CONTENT
[redacted]

Source: [redacted]

OperationGreenRights & Iberoamerica [redacted] NFO WEB: please fell free to add links ! thank to all!
MainPAD: [redacted]

http://www.guardian.co.uk/environment/2012/jan/27/public-eye-awards-vale-barclays?newsfeed=true

http://www.guardian.co.uk/commentisfree/cifamerica/2012/jan/24/brazil-pinheirinho-eviction-inspiration

http://www.aljazeera.com/indepth/features/2012/01/20121201536676440O.html

http://news.mongabay.com/2012/0119-hance_belomonte_cofferdams.html

http://www.eenews.net/public/climatewire/2012/01/19/2

http://www.internationalrivers.org/en/blog/ian-elwood/2012-1-19/belo-monte-construction-shut-down-protestors

http://www.raoni.fr/news-260.php

http://www.forbes.com/sites/kenrapoza/2012/01/18/amazon-tribe-says-brazils-pandora-dam-polluting-river/

http://blog.cifor.org/7005/brazil-dominates-forest-related-news-coverage-in-latin-america-in-2011/

http://upsidedownworld.org/main/news-briefs-archives-68/3386-brazilian-government-pulls-plug-on-the-million-cistern-project

http://www.v-brazil.com/government/laws/titleVIII.html

http://www.cimi.org.br/site/pt-br/?system=news&conteudo_id=6030&action=read

http://www.giornalettismo.com/archives/178307/la-diga-che-distruggera-il-popolo-del-fiume/

http://www.scribd.com/doc/77007839/An-Investigation-of-International-Sustainable-Projects-Involving-Indigenous-Peoples-of-Amazon-Juliano-Klevanskis-UFMG

http://amazonwatch.org/work/belo-monte-dam

http://www.internationalrivers.org/en/node/6079

http://ipcst.wordpress.com/

http://www.survivalinternational.org/about/belo-monte-dam

http://www.dams-info.org/en

http://www.internationalrivers.org/blog-categories/986

http://www.internationalrivers.org/en/2011-11-9/court-rules-against-indigenous-rights-belo-monte-hearing

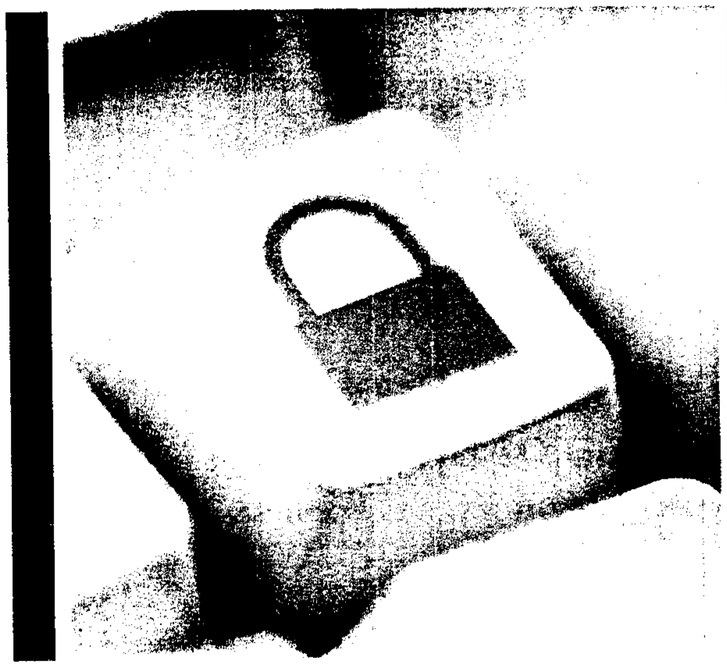
http://enviroleaks.org/2011/02/28/alstom-and-the-belo-monte-dam-let-the-leaks-begin/

Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
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

Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



Canadian Cyber Incident Response Centre

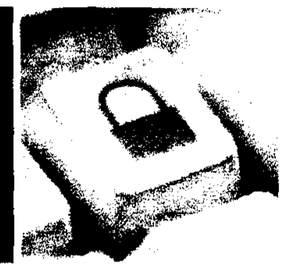
CTCP Update

Feb 2012

Canada

01020

CCIRC – Recent Changes



BUILDING A **SAFE** AND **RESILIENT CANADA**

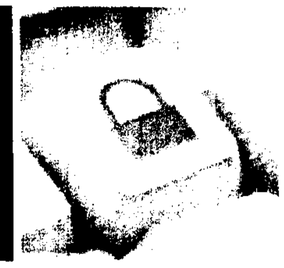
In October of 2011, CCIRC transferred from the Emergency Management Services (EMS) of the GC to the National Cyber Security Doctorate of Public Safety (NCSD)

NCSD and CCIRC now form the Operational and Policy based leadership roles within the Department of Public Safety, resulting in an improved alignment with National Cyber Strategy Pillars.

NCSD Subsections

- Canadian Cyber Incident Response Centre
- Technical Advice
- Policy
- Engagement and Partnerships

CCIRC – A New National Mandate



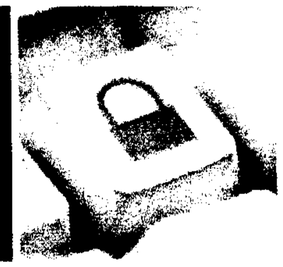
BUILDING A **SAFE** AND **RESILIENT CANADA**

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention, mitigation, and response to cyber events.

CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

CCIRC – Organizational Structure



BUILDING A **SAFE** AND **RESILIENT CANADA**

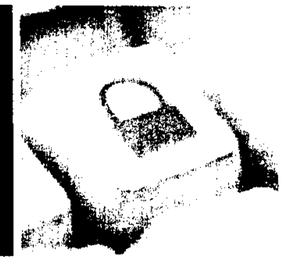
- Organized into three functions:

  - **Incident Handling** – assists partners in identifying, mitigating, and managing incidents

  - **Technical Support** – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis

  - **Strategic Initiatives and Situational Awareness** – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers

Public Safety Canada Agenda



BUILDING A **SAFE** AND **RESILIENT CANADA**

- Closely aligned to the pillars of Canada's Cyber Security Strategy:
  1. Secure Government systems.
     - Provide strategic policy leadership and establish clear federal roles and responsibilities
     - Strengthen the security of federal systems
     - Promote awareness throughout the Government of Canada
  2. Partner to secure systems outside the Government of Canada.
     - Engage with provinces and territories as owners, operators and regulators of critical infrastructure services, and as partners in education and awareness
     - Leverage and build upon public-private partnerships to secure critical infrastructure and promote awareness
     - Liaise with international partners on cyber security operational and policy issues
     - Work with academic and research institutions to educate, develop and foster innovation
  3. Help Canadians to be secure online.
     - Awareness of the need to act
     - Information about how to act
     - Protection from those who act criminally

- The department is responsible for the coordination of the overall Government of Canada's efforts in implementing the Strategy

Where CCIRC fits in *Canada's Cyber Security Strategy*

BUILDING A **SAFE** AND **RESILIENT CANADA**

Securing Federal Government Systems

Key actors:
- CSEC
- Shared Services
- TBS CIOB
- CF

Partnering to Secure Vital Systems Outside the Federal Government

Key actors:
- PS CCIRC, NCSD, CISCD
- CI Sector lead departments

Existing effort:
- PT, select CI (telecom, energy, finance)
- US CERTs

Future effort:
- trusted vendors
- international CERTs
- remaining CI sectors
- economic interests
- academia

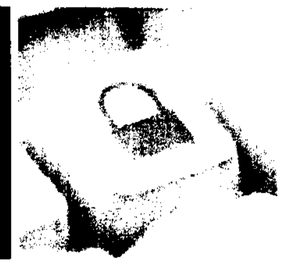
Helping Canadians to be Secure Online

Key actors:
- PS Communications
- law enforcement
- Industry Canada
- CRTC
- Privacy Commissioner
- Competition Bureau

Audiences:
- Home users
- Academia
- Small business

State-sponsored cyber espionage ← ***Risk*** → **Crime**

CCIRC – National Focus



BUILDING A **SAFE** AND **RESILIENT CANADA**

These partners…

Government S&I community

Critical Infrastructure

Provinces and territories

Five Eyes and International CERTs

Trusted vendors

Academia

Cyber security expert community

Open source

provide information to…

CCIRC

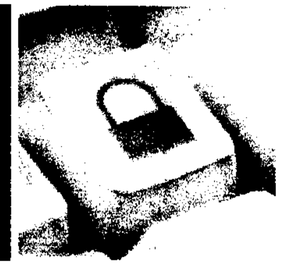
which provides these services:

Incident Handling and National Event Coordination and Assistance
- Direct technical assistance to partners and coordination of Government response to cyber events of national significance
- Audience: technical staff in partner organizations responding to cyber incidents
- Metric: 749 incidents responded to in 2011; 197 notifications to partners of compromised systems, 9 requests issued to shut down malicious systems in Nov/Dec 2011

Provision of Mitigation Advice
- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice
- Audience: technical staff in partner organizations
- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

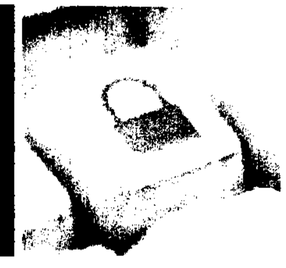
Reporting and Analysis
- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis
- Audience: technical staff, decision makers (under development)

Current challenges



- **Incident Handling and National Event Coordination and Assistance**
  - we can't say no – difficult to prioritize clients and services without clearly defined mission and mandate; prospective client base too broad
  - ambiguity of roles in an emergency – absence of a national emergency policy for cyber creates ambiguity for Government and Public Safety
  - limited profile – increased awareness of CCIRC and a credible brand will increase incident reporting
- **Provision of Mitigation Advice**
  - technology – lab infrastructure aging
  - people – attraction and retention of specialized, bilingual, TOP SECRET staff an ongoing challenge
  - policy – sharing sensitive information
  - accommodations – lack of long-term plan to obtain permanent and highly secure space hampers ability to handle classified information
- **Reporting and Analysis**
  - strategic analysis product for broader audience to be developed

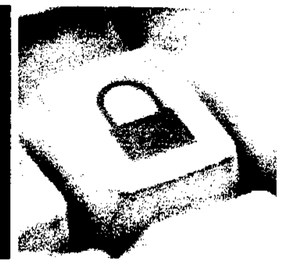
Progress in 2011



- Incident Handling and National Event Coordination and Assistance
  - 6 positions staffed this year; 8 remaining to attain full complement of 22; process underway for 4 more CS03s
  - working with U.S. on plan to inventory and explore potential alignment of information products (e.g., flashes, alerts, technical reports) (NCSD*)
- Provision of Mitigation Advice
  - initiated investment in lab infrastructure
  - development of an Industrial Control System (ICS) test-bed in conjunction with Defence R&D Canada and the private sector
  - launched development of secure web portal for info exchange with CI / PT
  - information-sharing MOUs under development with selected PTs and CI sectors (NCSD*)
- Reporting and Analysis
  - working with S&I community on potential joint products (NCSD*)

* Other divisions within NCSD engaged or leading

Near term objectives (January – March)

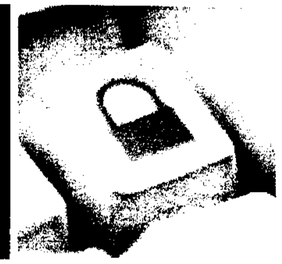


- Incident Handling and National Event Coordination and Assistance
  - initiate discussions with PTs on national cyber incident response (NCSD)
  - conduct federal tabletop exercises to clarify roles in a national response (NCSD/CCIRC)
  - consult U.S. on initial draft of Canada-U.S. Cyber Security Action Plan to consolidate and drive commitments under Beyond the Borders and other forums (NCSD)
  - launch anticipatory staffing for Cyber Defence initiative's potential 14 new FTEs for CCIRC with projected start date of April 1, 2012 (CCIRC)
  - develop standardized training regime and integration packages (NCSD)
- Provision of Mitigation Advice
  - increased engagement with PT and private sector partners (NCSD, CCIRC)
  - launch secure portal as repository for CCIRC products and mitigation advice (CCIRC)
  - work with corporate branch on short-term accommodations plan for CCIRC
- Reporting and Analysis
  - identification of partner requirements and defining new products and services (NCSD)

Medium term objectives (April - September)

- Incident Handling and National Event Coordination and Assistance
  - explore potential short-term personnel exchange with CSEC's Cyber Threat Evaluation Centre for new fiscal year
  - participate in and conduct cyber based exercises to support operational objectives: PTs and CI, Cyber Storm 4, CMX
  - begin implementation of alignment of information products with US-CERT
  - finalize plans with PS-Comms on CCIRC name change, re-branding, re-launching to enhance credibility, visibility, and help to address staff attraction and retention
  - initiate work to develop a cyber Emergency Support Function (ESF) under the Federal Emergency Response Plan (FERP)
- Provision of Mitigation Advice
  - work with corporate branch on long-term accommodations plan for CCIRC and NCSD
  - [redacted]
  - explore options for automation in lab testing and analysis, more technology
- Reporting and Analysis
  - pilot production of new products and services for new audiences (CCIRC)

NCSD: Policy Agenda



BUILDING A **SAFE** AND **RESILIENT CANADA**

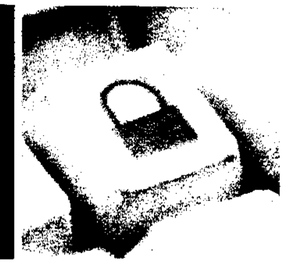
- Develop a Performance Measurement Strategy, as part of implementing Canada's Cyber Security Strategy
- Develop a Canadian position towards participation in emerging dialogue on norms and standards for international conduct in cyberspace (in anticipation of the United Kingdom Conference in November)
- Consider options for a cyber legislative review aimed at ensuring that the Government has flexibility, credibility and effectiveness in dealing with future cyber security challenges
- Following establishment of a forum of cyber security policy leads/interlocutors, strengthening the intergovernmental engagement on cyber security
- Partnerships: In partnership with lead departments, build on progress made with priority critical infrastructure sectors (Telecommunications (CSTAC); Energy) and engage with the Financial Sector

Communications: Public Awareness Campaign

BUILDING A **SAFE** AND **RESILIENT CANADA**

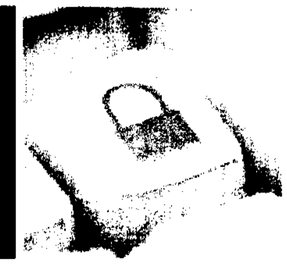
- A **multi-year cyber security public awareness campaign** will be the **cornerstone of a high profile and phased communications strategy** that will provide Canadians with information on cyber threats in order for them to take action to protect themselves and their personal information
- To this end, Public Safety is undertaking proactive communications initiatives, including a national public awareness advertising campaign (getcybersafe.gc.ca), international coordination of messaging and cyber incident management
- Public Safety Canada is the federal focal point for the coordination of cyber security communications activities
- Working Group allows for broad awareness of and contribution toward creative development, Web content, incident management and other core communications activities

Operational Partnerships



- Recent Partnerships Development:
  - Team Cymru;
  - Microsoft;
  - Canadian Electrical Association;
  - Canadian Association of Petroleum Producers;
  - CRTC – Enforcer for new Regulation to fight spam, phishing and vishing
    - Includes collaboration with:
      - Industry Canada
      - Competition Bureau
      - Office of Privacy Commissionnaire
      - Private Sector (Spam Reporting Centre Bid)

Operational Events

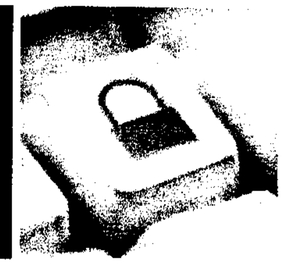


- Jul 2011 – Jan 2012
  - 387 managed events

- Hacktivism:
  - ACTA, SCADA, Israel-Palestine,
  - Pastebin and XSSed !

- Crimeware
  - SQL injections (ASP.net and other)
  - Wordpress
  - OWA account phishing
  - Black Hole, Zero-Access, Incognito, exploiting Java vulnerabilities
  - DNSChanger

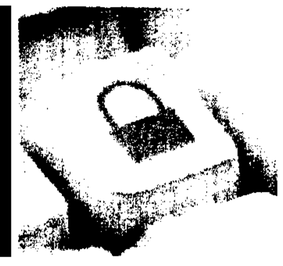
Operational Events



- APT:
  - Oil Industry (merger and acquisition)
  - G20 France
  - ShadyRAT (McAfee)
  - [redacted]
  - Certificate Authority Compromise (Diginotar)
  - DUQU (HU-CERT), NITRO (Symantec), LURID (Trend Micro), Htran (Secureworks)
- Vulnerabilities
  - ICS exposed to Web (Shodan and ICS-CERT)
  - cURL implementation in e-commerce sites.

s.16(2)(c)

DNSChanger

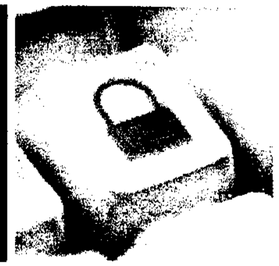


- An opportunity to Notify
  - FBI / Court Order to seize and provide DNS service: 8 Nov – 8 Mar
  - Victims damage mitigated.

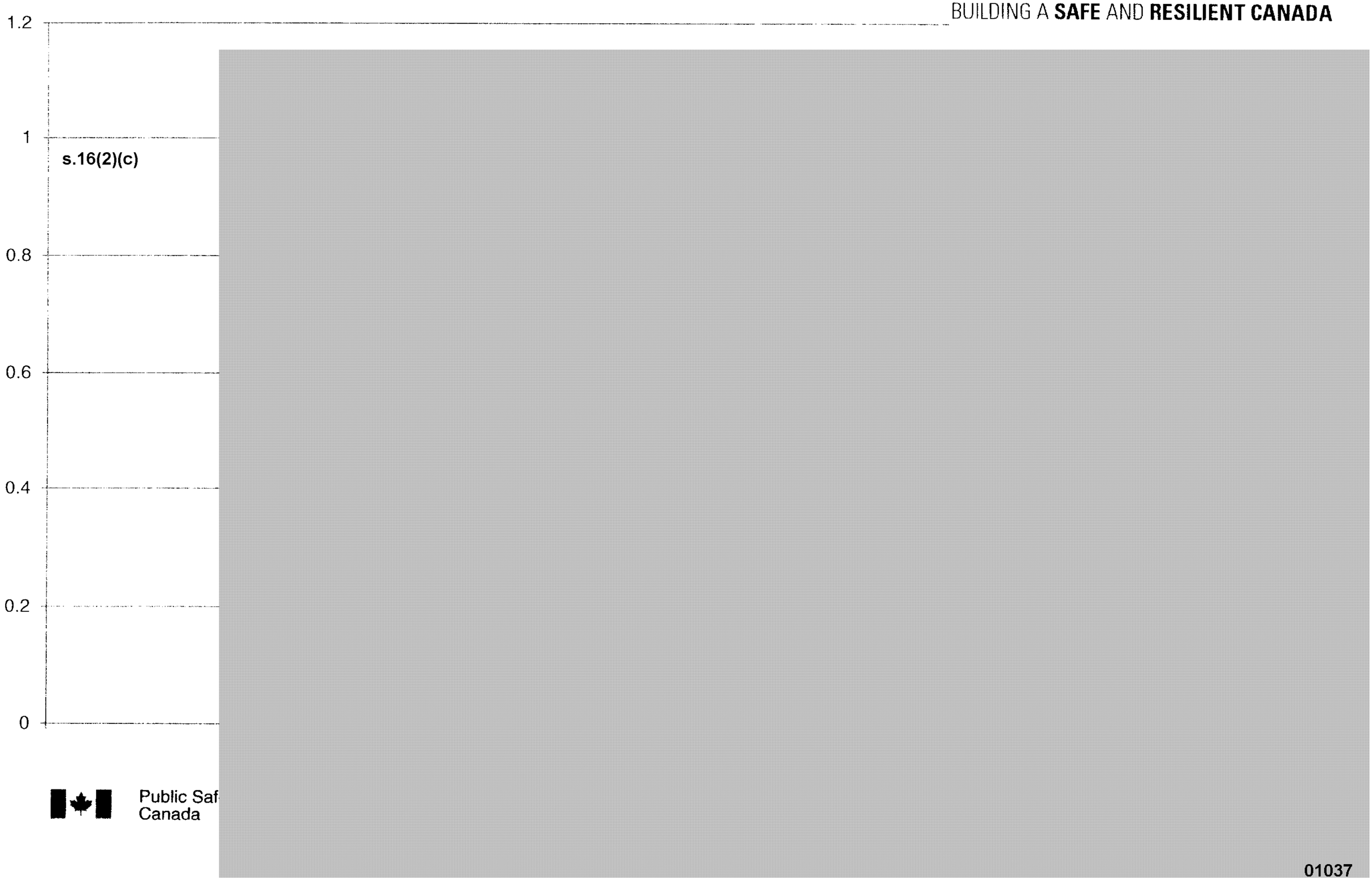
s.16(2)(c)

- Need to Notify
  - Vulnerable to future hostile activities
  - IP space pollution
- Initial count in Canada:
  - [redacted]
- Current:
  - [redacted]
- Rate: 1[redacted]
- CCIRC notifications: 2 to 5 times a week.

DNSChanger Remediation by CTCP



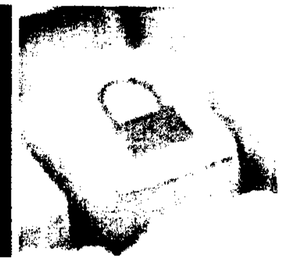
BUILDING A **SAFE** AND **RESILIENT CANADA**



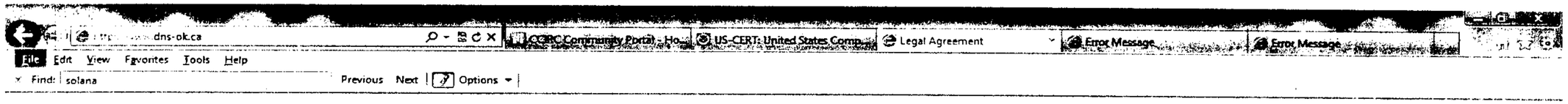
Public Saf
Canada

01037

DNSChanger Eye-Chart



BUILDING A **SAFE** AND **RESILIENT CANADA**



.ca | Canadians Connected
Canadiens branchés

Welcome
This page is hosted by the Canadian Internet Registration Authority (CIRA) and provides an online checker to indicate if your computer system may be affected by DNSChanger Malware — malicious code that was used by a criminal gang recently apprehended as part of the FBI Operation GhostClick. To learn more about this malware, please visit Public Safety Canada. Please note that this checker does not screen your computer for any other virus, malicious code or malware. CIRA encourages all Internet users to adopt best practices in anti-virus protection for personal and business computers.

About CIRA
CIRA is the member-driven organization that manages Canada's .CA domain name registry, develops and implements policies that support Canada's Internet community, and represents the .CA registry internationally.

Terms and Conditions
Please review and accept the following Terms and Conditions prior to using the DNSChanger Malware Checker (the "Checker").

PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND CIRA.

Access & Use of the Checker

CIRA is willing to allow access to, and use of, this free Checker only on the condition that you accept all of the terms contained in this agreement.

By clicking on the "I Accept," button, you are consenting to be bound by the terms of this Agreement. If you do not agree to these terms and conditions, then you should click the "Cancel" button, in which case you will not be able to access or use the Checker.

The Checker remains the property of CIRA and its licensors and is protected by copyright law. You

I agree Cancel

Bienvenue
Cette page est hébergée par l'Autorité canadienne pour les enregistrements Internet (ACEI). On y propose un vérificateur en ligne indiquant si votre système informatique est touché par le logiciel malveillant DNSChanger utilisé par un groupe de criminels récemment appréhendé dans le cadre de l'opération GhostClick du FBI. Pour en apprendre davantage sur ce logiciel malveillant, veuillez visiter Sécurité publique Canada. Nous vous prions de noter que cet outil de vérification ne recherche aucun autre virus ni programme ou logiciel malveillant. L'ACEI invite tous les internautes à adopter les pratiques exemplaires en matière de protection antivirus, et cela, tant pour leurs ordinateurs personnels que pour leur poste de travail en entreprise.

Au sujet de l'ACEI
L'Autorité canadienne pour les enregistrements Internet est un organisme sans but lucratif qui, dirigé par ses membres, gère le registre des noms de domaine .CA du Canada, élabore et met en œuvre des politiques à l'appui de la communauté Internet canadienne et représente le registre .CA sur le plan international.

Modalités
Veuillez examiner et accepter les modalités suivantes avant d'utiliser le détecteur de maliciel DNSChanger (le « détecteur »)

VEUILLEZ LIRE LES MODALITÉS DE LA PRÉSENTE ENTENTE. IL S'AGIT D'UN CONTRAT LÉGAL ET EXÉCUTOIRE INTERVENU ENTRE VOUS ET L'ACEI.

Accès au détecteur et son utilisation

L'ACEI est disposée à permettre l'accès à ce détecteur gratuit et son utilisation uniquement si vous acceptez l'ensemble des modalités prévues dans la présente entente.

En cliquant sur le bouton « J'accepte », vous consentez à être lié par les modalités de la présente entente. Si vous ne les acceptez pas, vous devez alors cliquer sur le bouton « Annuler », auquel cas vous ne pourrez avoir accès au détecteur ni l'utiliser.

Le détecteur demeure la propriété de l'ACEI et de ses concédants de licences et est protégé par

J'accepte Annuler

DNSChanger Eye-Chart

CANADA

Your computer system does not appear to be affected by DNSChanger Malware

A RED banner at the top and bottom of this page indicates your computer system appears to be using a Domain Name System (DNS) that was part of the criminal infrastructure seized during Operation GhostClick. You are encouraged to consult the following Public Safety Canada document for further information:
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-002-eng.aspx.

A GREEN banner at the top and bottom of this page indicates your computer system uses a DNS which is not known to be associated with the criminal DNS infrastructure associated with Operation GhostClick.

How does the checker work?

The GREEN or RED banners are determined based on the DNS request performed by your computer in order to obtain the Internet Protocol (IP) address associated with DNS-OK.ca. This request is forwarded to CIRA's DNS infrastructure by your DNS (typically provided automatically to your computer or home router by your Internet Service Provider). The IP address of your requesting DNS is compared to known Operation GhostClick IP addresses, which results in a RED or GREEN banner page.

If you have any questions or need clarification, please contact your Internet Service Provider (ISP).

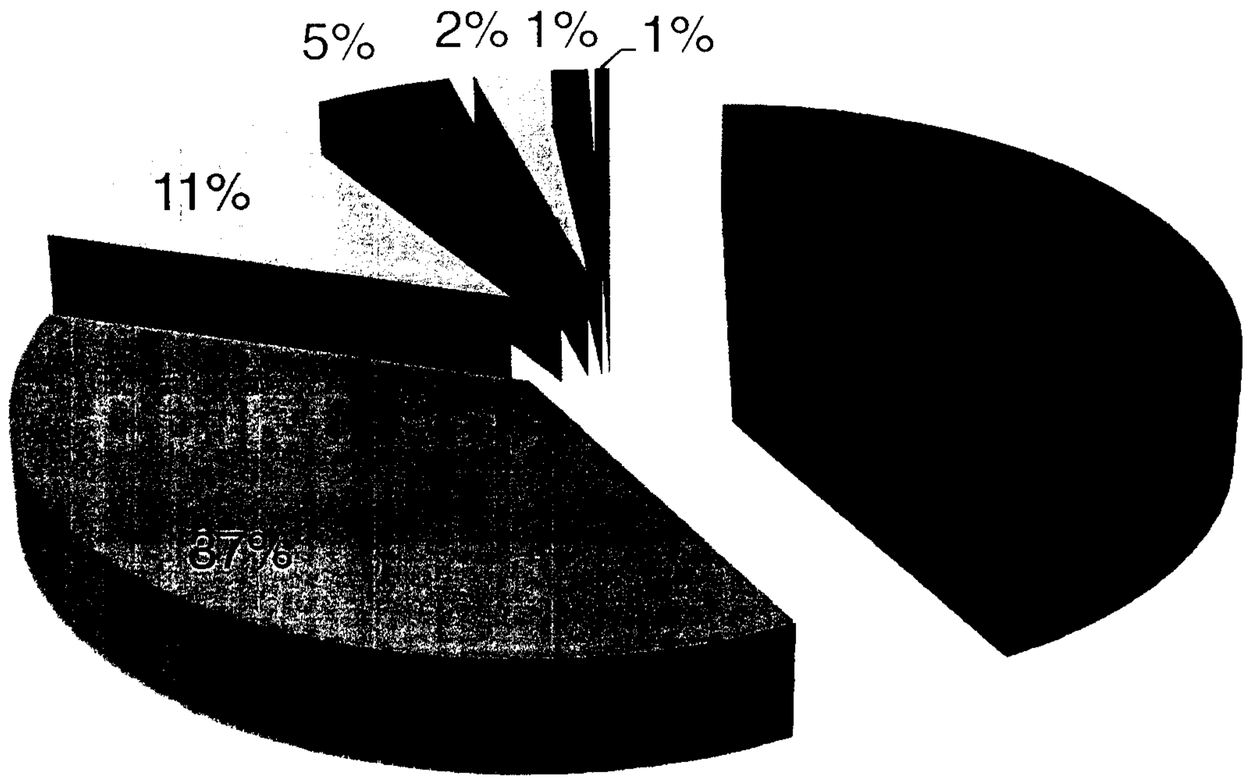
.ca

Your computer system does not appear to be affected by DNSChanger Malware

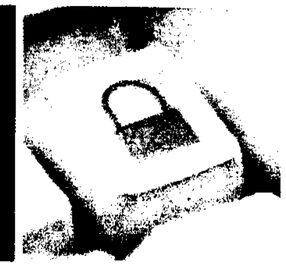
CCIRC Reported Events Jul 2011-Jan 2012

BUILDING A **SAFE** AND **RESILIENT CANADA**

Events

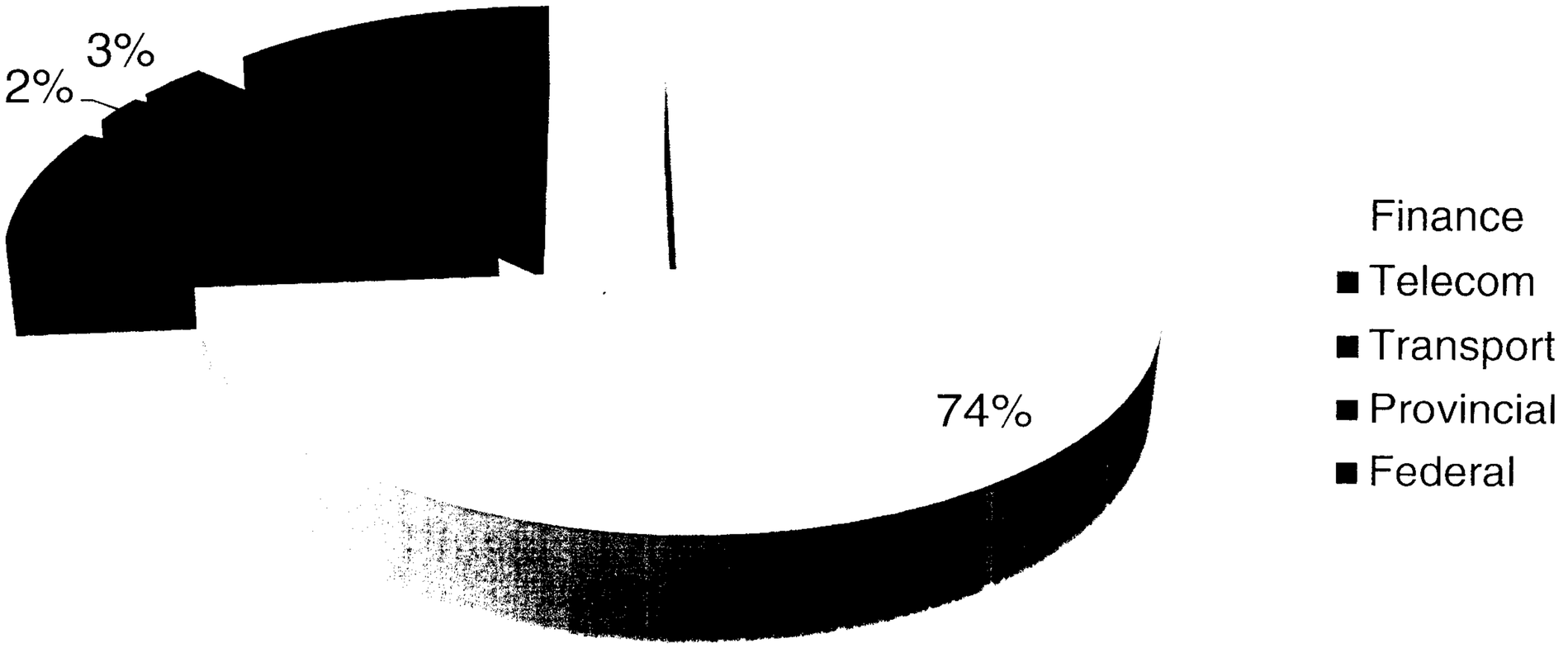


Phishing Reports

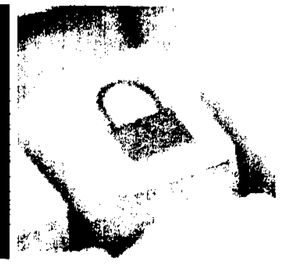


BUILDING A **SAFE** AND **RESILIENT CANADA**

Phishing Reports to CCIRC
Jul 2011 - Jan 2012

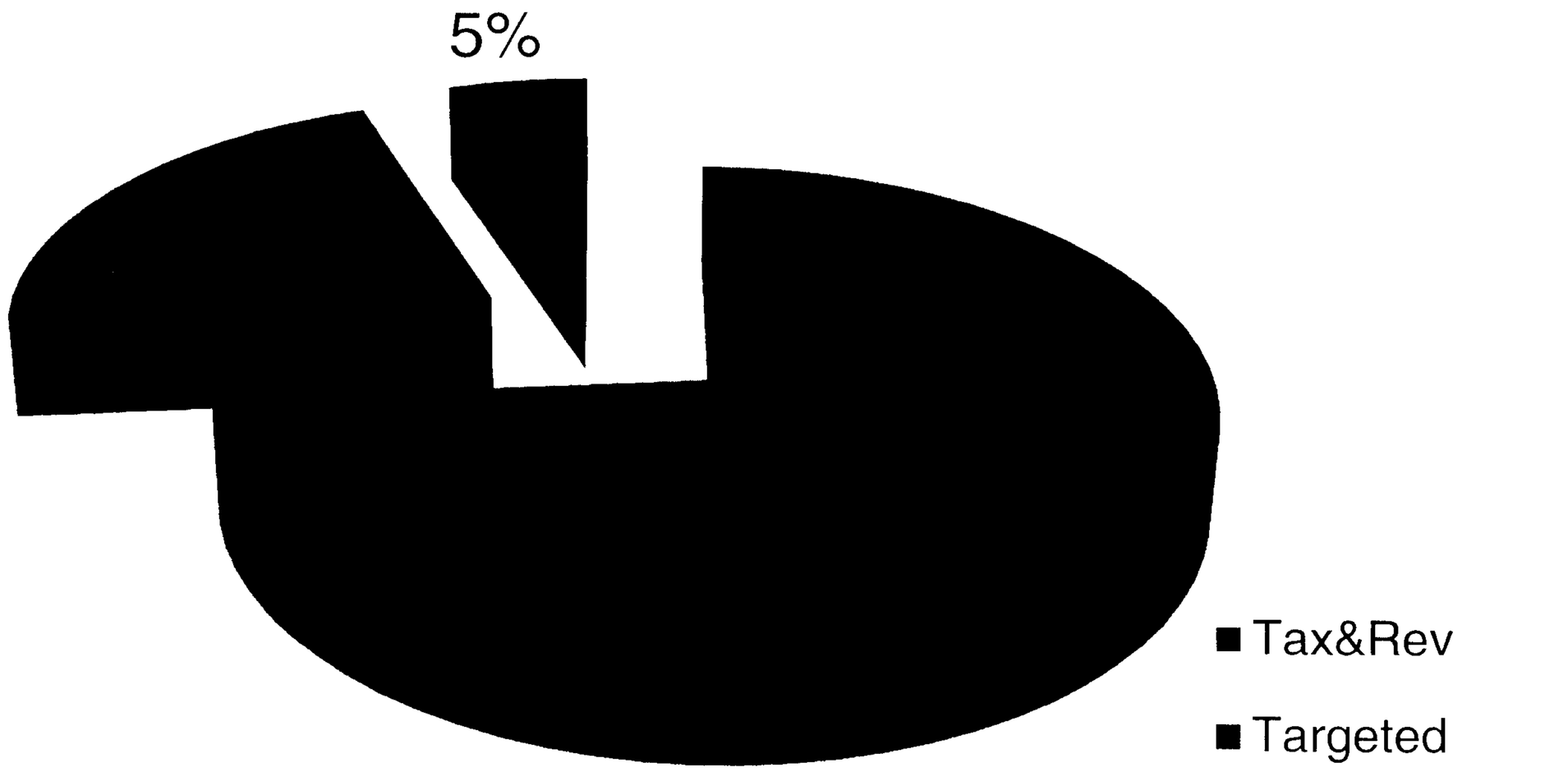


Phishing Reports

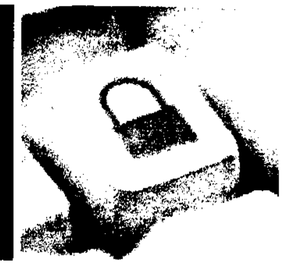


BUILDING A **SAFE** AND **RESILIENT CANADA**

Federal



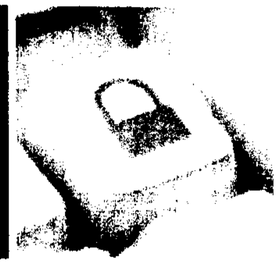
ATI requests...



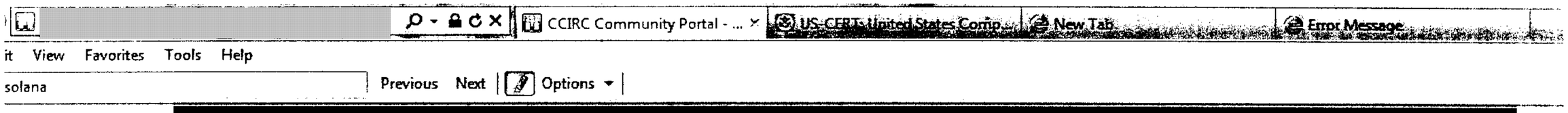
- "Malicious site hosted on MEMBER take down"
  - MEMBER exempted un 20(1)C -> Economic damage.

- If you are contacted by an ATI coordinator…

Canadian Cyber Community Portal



BUILDING A **SAFE** AND **RESILIENT CANADA**



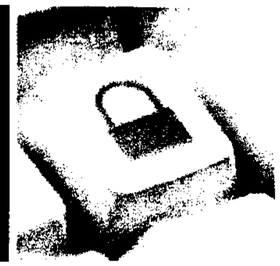
s.16(2)(c)

Government of Canada / Gouvernement du Canada

Canada

Public Safety Canada / Sécurité publique Canada

Technical Capabilities

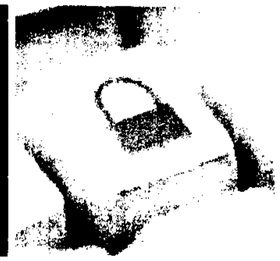


- Automated malware analysis tools being reviewed:

s.16(2)(c)

- implementation in the next quarter
-
-
- Significant overhaul of lab infrastructure

Questions?



BUILDING A **SAFE** AND **RESILIENT CANADA**

Williston, Sandra

From: CCIRC Internal Portal - CDO Watch and Operations <[redacted]
Sent: January-31-12 4:00 PM
To: Beaudoin, Luc
Subject: Activity Log

CCIRC Internal Portal - CDO Watch and Operations

Activity Log - Daily Summary

Modify my alert settings View Activity Log

Title	Modified	Modified by	
N&T 31 Jan 2012	1/31/2012 7:57 AM	Moore, Bruce	New!

Date/Time 1/31/2012 8:00 AM

Short Description N&T 31 Jan 2012

Issue Status Closed

Detail Description

Handler Moore, Bruce

Updates

CI Sector / Client Group

Context [redacted]

Projects

s.16(2)(c)
s.20(1)(b)

CF12-XXX Hackivist Group Anonymo...	1/31/2012 8:47 AM	Williston, Sandra	Edited

Short Description [redacted] CF12-001 Hackivist Group Anonymous - DDoS Activty Related to Copyrights and Intellectual Property] - Processing

Detail Description [redacted]
Processing for CF12-001

Updates

Williston, Sandra

From: CCIRC Internal Portal - CDO Watch and Operations [redacted]
Sent: January-26-12 4:00 PM
To: Beaudoin, Luc
Subject: Activity Log

s.16(2)(c)

CCIRC Internal Portal - CDO Watch and Operations

Activity Log - Daily Summary

Modify my alert settings View Activity Log

Title	Modified	Modified by	
Research - Scada Leverett report	1/25/2012 6:05 PM	Phlek, Vireak	New!

Date/Time	1/25/2012 6:00 PM
Short Description	Research - Scada Leverett report
Issue Status	Closed
Detail Description	Read the report and try to find some of the mentioned Canadian IP Scada machine facing directly in the internet. Using SHODAN search engine. What is missing is the ability do display more than 50 results and export the data into a file. Those are a paying option. More research to come. I have include the report and the partial result from my queries.
Handler	Phlek, Vireak
Updates	
CI Sector / Client Group	02F SCADA
Context	
Projects	

Research - Scada Leverett report	1/25/2012 6:08 PM	Phlek, Vireak	Edited

Detail Description

[redacted]

Read the report and try to find some of the mentioned Canadian IP(365) Scada machine facing directly in the internet.

Using SHODAN search engine. What is missing is the ability do display more than 50 results and export the data into a file. Those are a paying option.

More research to come. I have include the report and the partial result from my queries.

Updates

Research - Scada Leverett report 1/25/2012 6:10 PM Phlek, Vireak Edited

Updates

Research - Scada Leverett report 1/25/2012 6:15 PM Phlek, Vireak Edited

Updates Niagara Web server receiced the most hits : 725 out of 1211.
Obtain document on Niagara security from the web.

Research - Scada Leverett report 1/25/2012 6:20 PM Phlek, Vireak Edited

Updates

TAC/ Xenta511 is another popular one result in 106 hits for canadian SCADA.
Obtain doc from the cie as well.

N&T 26 Jan 2012 1/26/2012 8:02 AM Moore, Bruce **New!**

Date/Time 1/26/2012 9:00 AM

Short Description N&T 26 Jan 2012

Issue Status Closed

Detail Description

s.20(1)(b)

Handler Moore, Bruce

Updates

CI Sector / Client Group

Context

Projects

CF12-XXX ["Anonymous" DDoS Activ... 1/26/2012 9:27 AM Williston, Sandra Edited

Short Description CF12-XXX Hackivist Group Anonymous - DDoS Activty Related to Copyrights and Intellectual Property] - Processing

Updates

DDoS Mitigation Information Repo... 1/26/2012 10:16 AM Murphy, Gregg **New!**

Date/Time 1/26/2012 11:00 AM

Short Description DDoS Mitigation Information Report

Issue Status Active

Detail Description Publish a DDoS Mitigation Information Report.

Handler Williston, Sandra

Updates

CI Sector / Client Group

Context

Projects

[redacted]

s.16(2)(c)

1/26/2012 12:42 PM Moore, Bruce **New!**

Date/Time 1/26/2012 1:00 PM

Short Description [redacted]

Issue Status Closed

Detail Description

Handler Moore, Bruce

Updates

CI Sector / Client Group 01A Federal

Context

Projects

Possible copied and/or stolen pe...

1/26/2012 12:56 PM Murphy, Gregg **New!**

Date/Time 1/26/2012 1:00 PM

Short Description Possible copied and/or stolen personal information and credit card numbers

Issue Status Closed

Detail Description [redacted] requesting our assistance in having credit card numbers removed from pastebin.com [redacted] and [redacted]

Handler Murphy, Gregg

Updates Pastebin appears to be hosted by a Canadian ISP: WMD-GAME-SERVERS in Saint John, NB.

The sites are no longer active. Notified INTERPOL that no action was required on our part.

CI Sector / Client Group 07 Other Institutions

Context

Projects

Research into APT reported activ...

1/26/2012 1:07 PM Beaudoin, Luc S **New!**

Date/Time 1/26/2012 2:00 PM

Short Description Research into APT reported activity

Pages 1051 to / à 1052

are withheld pursuant to sections

sont retenues en vertu des articles

13(1)(a), 16(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: [redacted]
Sent: January-26-12 9:59 AM
To: Alain.Labossiere@ic.gc.ca
Cc: CYBERDO
Subject: RE: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

s.16(2)(c)

Hi Alain,

CCIRC will be releasing the Cyber Flash today.

Thanks,

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: Alain.Labossiere@ic.gc.ca [mailto:Alain.Labossiere@ic.gc.ca]
Sent: January-25-12 11:21 AM
To: [redacted]
Subject: RE: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

I cans end it to the CTCP folks, now or wait for your cyberflash?
(I want to follow protocol of course)

al

-----Original Message-----
From: [redacted] mailto:[redacted]
Sent: Wednesday, January 25, 2012 9:32 AM
To: Labossière, Alain: [redacted]
Subject: FW: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

---

From: Beaudoin, Luc S
Sent: Wednesday, January 25, 2012 9:31:51 AM (UTC-05:00) Eastern Time (US & Canada)
To: [redacted]
Subject: RE: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

OK.....could you do a cut-paste into a Cyber Flash ? (first this year) I think we need to do this.... Thoughts ? ETC ?

Luc

s.16(2)(c)

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: [redacted]
Sent: January-25-12 9:17 AM
To: Beaudoin, Luc S; Bendelier, Kenneth; Cameron, Bud; Clow, Patrick; Melanson, Daryl; Moore, Bruce; Murphy, Gregg; Phlek, Vireak; Turbide, Frank; Williston, Sandra
Subject: FW: [1st-t] US-CERT Technical Cyber Security Alert TA12-024A -- " Anonymous" DDoS Activity

FYI

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"

[redacted]

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
16 Jan 2012	Educational	2573	XSSed Notification – cross-site scripting vulnerability at a university website	one	University website	
26 Jan	Govt	2595	Websites vulnerable to exploits listed in Pastebin	Unknown	[redacted] notified CTEC, CERT Australia & DoD Australia	
23 Jan 2012	Other	2588	Website defacement	1	Ottawa dentist Sent notification to domain technical contact & hosting provider	
17 Jan	Various, includes health and maybe govt	2577	Website compromises – username, password posted online (pastebin)	5	[redacted](A forum for public-private sector discussions on how to manage the environmentally in an ethically, scientifically and financially sound way); [redacted]co (sells wholesale vitamins and food supplements); soccer league and 2 AA level hockey leagues CCIRC notified the orgs	s.16(2)(c) s.20(1)(c)
27 Jan	Security – Intl	2597	Cdn University IP attacking Virginia Police website	1	[redacted] IP belongs to a library computer open to all – it's possible that machine was compromised. Workstation is rebuilt at least once a day	
16 Jan	Educational	2574	Malware hosted on a Cdn university website	one	• CCIRC observed that malware was hosted on a [redacted] website • The file "photographer.exe" is detected by McAfee as Adware (Gabpath). This file will in-turn drop a 2nd binary (postalito.jpg.exe) on victim computers (Trojan Dropper). Mon 16/01/2012 10:40 AM A follow-up check confirmed that the malware was removed from the university website and is no longer being served. Moore, Bruce (1/13/2012 1:07 PM): Fri 13/01/2012 11:49 AM Deactivation request sent to the university (RCMP cc'd). The university was advised that their domain was added to the malc0de	

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
					blocklist, possibly resulting in decreased legitimate traffic to their website.	
20 Jan	Unsure	2587	Malware hosted on a Cdn IP	Unknown	Files are of the password stealing and backdoor Trojan variety (linked to botnets and stealing banking info) Sent takedown request to network's owner, cc'd LE & CTEC	
23 Jan	Other	2589	Malware hosted on a Cdn IP	1	[redacted] Script redirects user to domain hosted in US – domain registered to clickartists website services from CA but IP address belongs to [redacted]	
17 Jan 2012	Telecom	2576	Malware hosted on a Cdn IP (website hosting service server)	1	Sent deactivation request to iweb, cc'd RCMP [redacted] was warned that this domain was added to various block lists, possibly resulting in reduced legitimate traffic to this website.	
20 Jan	Provincial, Energy, Bank, Telecom, Health, Transport, education	2586	DNS Changer malware		The telcos are probably ISPs who have their customers' computer infections showing up on the Shadowserver Drone report	Check for repetition for orgs with other events – maybe ask Luc
16 Jan	Provincial, financial, energy, health and transportation	2575	DNS Changer Malware (Ghostclick) Shadowserver Drone Report	3 provinces, 1 bank, 1 energy co, two health orgs, one transportation	[redacted] again	Check to see if they're the same ones from previous weeks or if they're new cases
18 Jan 2012	Federal, Provincial, Energy, Finance,	2580	DNS Changer Malware	24	[redacted] == sent notification	

s.16(2)(c)
s.20(1)(c)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
	Health, Transportation, 12 universities					
24 Jan	Multiple	2592	DNS Changer malware	2 provinces, 1 energy co; 15 telecom cos' 1 Transportation; 10 universities	[redacted]	Ask someone in Ops re the eye-chart and the CCIRC-CRTC-CIRA initiative
19 Jan 2012	Financial	2581	Phishing	1	Came in through Phonebusters/anti-fraud centre Hosted in US Report sent to [redacted] Google Phishing Filter Service and APWG	
20 Jan	Financial	2584	Phishing	1	[redacted] Hosted in US Different origin and link than in event #2581 Came from phonebusters/anti-fraud centre	
20 Jan	Financial	2585	Phishing	1	[redacted] Hosted in US	
24 Jan	Govt	None	CRA Phishing		Email offering tax refund prompts user to click on link – site is no longer active as of this writing	Ask editorial board: Is this worth putting in the Weekly? I think so
26 Jan	Financial	2596	Phishing	1	[redacted] hosted in Culver City, California	
27 Jan	Financial	2598	Phishing	1	[redacted] Website hosted in Taiwan Report sent to [redacted] Google Phishing Filter service and APWG	
27 Jan	Financial	2599	Phishing	1	[redacted] Website hosted in Paris, France	

s.16(2)(c)
s.20(1)(c)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
27 Jan	Financial	2600	Phishing	1	[redacted] Hosted on a server in Case Western Reserve University in Cleveland, Ohio	
27 Jan	Public	12-3440	Phishing e-mail		Spoofing Service Canada, asking people to complete an information form. Domain registration appears dubious. Notified CTEC and recommended notifying SC	
[redacted]						Ask Luc or Bruce for more details – not much in the portal
					[redacted] **pinfi malware is spyware	
24 Jan	Govt	2593	APT	1?	Targeted e-mail with trojan attachment [redacted] Told CTEC & CSIS	
24 Jan	Govt	2594	FTP credentials of a federal dept posted on the Internet		Got it through the Yahoo phishing campaign? Potential impact: credential theft /unauthorized access	Ask Gregg to explain it a bit more – is this really serious?
27 Jan	Multiple (potential)	2601	Canadian SCADA Ips posted on Pastebin		ICS-CERT alerted CCIRC The Cdn SCADA IPs are public facing Most of the IPs were previously posted on pastebin (CE12-2583). Two new IPs on this event The IPs belong to a health org & a building/property owner --	Confirm with Gregg that these IPs are likely for HVAC systems in buildings
20 Jan 2012	Energy (SCADA)	2583	SCADA IPs were posted on Pastebin –		[redacted]	

s.16(2)(c)
s.20(1)(c)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
			Pastebin entry suggests they are vulnerable		Rich mansions in the neighbourhood The posting on Pastebin will draw attention to the log-in panel CCIRC Ops mgr thinks it's a poor practice to expose the log-in screen CCIRC Notified the maintainers that operate these sites: [redacted] and [redacted]	
24 Jan 2012	Govt	2590	Operation SACTA (stop anti-counterfeiting Trade Agreement)	1	Encouraging users to email or attack govt sites Sent info to fed govt CERT	

Noteworthy News from the CCIRC Daily Reports or Ops Meeting during the week of 16 Jan 2012:

s.16(2)(c)
s.20(1)(c)

Tel Aviv Stock exchanged website DDoS'd; not a sophisticated attack (17 Jan 2012) – some info also under Activity 12-3417
Israeli-Palestinian websites were attacked
Bot blackmails Facebook users (Threatwatch 20 Jan 2012)
Some websites going black (on 18 Jan 2012) to protest SOPA
Anonymous downs govt, music industry sites in largest attacks ever – in response to the federal raid on Megaupload (20 Jan 2012) (Note: this includes the US equivalent of getcybersafe.ca)
Click on an Anonymous link, and you could be DDoS'ing the US govt (20 Jan 2012)

Noteworthy News from the CCIRC Daily Reports or Ops Meeting during the week of 23 Jan 2012:

Tax season opens, tax spam follows (Threat Watch from 23 Jan 2012)
CBS is offline and its servers are wiped – by Anonymous (Note: It was actually a DNS poisoning attack; CBS servers were not wiped, but users were directed to another imposter site – CBS managed to regain control)
Cameras may open up the Board Room to Hackers (videoconferencing systems, widely used, if set up outside the firewall of the org can pick up the audio)
Hackers, reportedly associated with Anonymous have been attacking Polish govt websites to protest scheduled signing of ACTA
----Reports suggest Anonymous will attack Facebook on Feb 28
----- Hackers also attacked Irish Govt websites (Op ACTA)
-----European Parliament website taken offline in retaliation of ACTA (website down for almost a day) (27 Jan 2012)
Microsoft researchers find new type of stealth malware that appears to be benign, bypasses AV filters, but morphs into malicious software once it is on a user's computer.
(Note: the point is that you can't keep every malware out – better have a data recovery plan after a cyber attack) (26 Jan 2012)

Symantec warns customers of hacker risk *(advised customers to stop using its pc Anywhere software for accessing remote PCs, saying they're at increased risk of getting hacked. This seems to be the company's most direct acknowledgement to date that a 2006 theft of its source code put customers at risk) (26 Jan 2012: Reuters)*

Products/Alerts Released

- **CCIRC Product:** AV12-003 Oracle Critical Patch Updates – Jan 2012 released to all cyber clients and posted on PS website
- **CCIRC Product:** CF12-001 Hacktivist Group Anonymous – DdoS Activity Related to Coyrights and Intellectual Property – Released to ALL cyber clients (but not posted on departmental website) **ACTION:** *ASK WHY WE DID THIS – THE INTENDED VICTIMS WOULD BE MOSTLY IN GOVT – IS IT BECAUSE CTEC WAS NOT IN A POSITION TO DO THIS?*

- Multiple (7) **ICS-ALERTs** released by the US subsequent to the S4 SCADA conference (researchers sent/gave findings to US CERT)

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
16 Jan 2012	Educational	2573	XSSed Notification – cross-site scripting vulnerability at a university website	one	University website	
	Educational	2574	Malware hosted on university website	one	• CCIRC observed that malware was hosted on a [redacted] website • The file "photographer.exe" is detected by McAfee as Adware (Gabpath). This file will in-turn drop a 2nd binary (postalito.jpg.exe) on victim computers (Trojan Dropper). Mon 16/01/2012 10:40 AM A follow-up check confirmed that the malware was removed from the university website and is no longer being served. Moore, Bruce (1/13/2012 1:07 PM): Fri 13/01/2012 11:49 AM Deactivation request sent to the university (RCMP cc'd). The university was advised that their domain was added to the malc0de blocklist, possibly resulting in decreased legitimate traffic to their website.	s.16(2)(c) s.20(1)(c)
		2575	DNS Changer Malware (Ghostclick) Shadowserver Drone Report	3 provinces, 1 bank, 1 energy co, two health orgs, one transportation	[redacted]gain	Check to see if they're the same ones from previous weeks or if they're new cases
17 Jan 2012	Telecom	2576	Malware hosted on website hosting service server	1	[redacted]n Mtl Sent deactivation request to iweb, cc'd RCMP [redacted]was warned that this domain was added to various block lists, possibly resulting in reduced legitimate traffic to this website.	
	Various, includes	2577	Website compromises – username,	5	[redacted](A forum for	

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
	health and maybe govt		password posted online (pastebin)		public-private sector discussions on how to manage the environmentally in an ethically, scientifically and financially sound way); [redacted] co (sells wholesale vitamins and food supplements); soccer league and 2 AA level hockey leagues CCIRC notified the orgs	
18 Jan 2012	Federal, Provincial, Energy, Finance, Health, Transportation, 12 universities	2580	DNS Changer Malware	24	[redacted] == sent notification	s.16(2)(c) s.20(1)(c)
19 Jan 2012	Financial	2581	Phishing	1	Came in through Phonebusters/anti-fraud centre Hosted in US Report sent to [redacted] Google Phishing Filter Service and APWG	
20 Jan 2012	Energy (SCADA)	2583	SCADA IPs were posted on Pastebin – Pastebin entry suggests they are vulnerable		[redacted] Rich mansions in the neighbourhood The posting on Pastebin will draw attention to the log-in panel CCIRC Ops mgr thinks it's a poor practice to expose the log-in screen CCIRC Notified the maintainers that operate these sites: [redacted]	
	Financial	2584	Phishing	1	[redacted] Hosted in US Different origin and link than in event #2581 Came from phonebusters/anti-fraud centre	
	Financial	2585	Phishing	1	[redacted] Hosted in US	

DATE	SECTOR	INCIDENT/ ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
	Provincial, Energy, Bank, Telecom, Health, Transport, education	2586	DNS Changer malware		The telcos are probably ISPs who have their customers' computer infections showing up on the Shadowserver Drone report	Check for repetition for orgs with other events – maybe ask Luc
	Unsure	2587	Malware hosted on a Cdn IP	Unknown	Files are of the password stealing and backdoor Trojan variety (linked to botnets and stealing banking info) Sent takedown request to network's owner, cc'd LE & CTEC	

Noteworthy News from the CCIRC Daily Reports or Ops Meeting during the week:

Tel Aviv Stock exchanged website DDoS'd; not a sophisticated attack (17 Jan 2012) – some info also under Activity 12-3417
Some websites going black (on 18 Jan 2012) to protest SOPA
Israeli-Palestinian websites were attacked
Bot blackmails Facebook users (Threatwatch 20 Jan 2012)
Anonymous downs govt, music industry sites in largest attacks ever – in response to the federal raid on Megaupload (20 Jan 2012)
Click on an Anonymous link, and you could be DDoS'ing the US govt (20 Jan 2012)

CCIRC Product: AV12-003 Oracle Critical Patch Updates – Jan 2012 released to all cyber clients and posted on PS website

"Anonymous" DDoS Activity

Original release date: January 24, 2012
Last revised: --
Source: US-CERT

Overview

US-CERT has received information from multiple sources about coordinated distributed denial-of-service (DDoS) attacks with targets that included U.S. government agency and entertainment industry websites. The loosely affiliated collective "Anonymous" allegedly promoted the attacks in response to the shutdown of the file hosting site MegaUpload and in protest of proposed U.S. legislation concerning online trafficking in copyrighted intellectual property and counterfeit goods (Stop Online Piracy Act, or SOPA, and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA).

I. Description

US-CERT has evidence of two types of DDoS attacks: One using HTTP GET requests and another using a simple UDP flood.

The Low Orbit Ion Cannon (LOIC) is a denial-of-service attack tool associated with previous Anonymous activity. US-CERT has reviewed at least two implementations of LOIC. One variant is written in JavaScript and is designed to be used from a web browser. An attacker can access this variant of LOIC on a website and select targets, specify an optional message, throttle attack traffic, and monitor attack progress. A binary variant of LOIC includes the ability to join a botnet to allow nodes to be controlled via IRC or RSS command channels (the "HiveMind" feature).

The following is a sample of LOIC traffic recorded in a web server log:

"GET /?id=13270144005 70&msg=We%20Are%20Legion! HTTP/1.1" 200 99406 "hxxp://pastehtml.com/view/blafp1ly1.html" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1"

The following sites have been identified in HTTP referrer headers of suspected LOIC traffic. This list may not be complete. Please do not visit any of the links as they may still host functioning LOIC or other malicious code.

"hxxp://3g.bamatea.com/loic.html"
"hxxp://anonymouse.org/cgi-bin/anon-www.cgi/"
"hxxp://chatimpacto.org/Loic/"
"hxxp://cybercrime.hostzi.com/Ym90bmV0/loic/"

"hxxp://event.seeho.co.kr/loic.html"
"hxxp://pastehtml.com/view/bl3weewxq.html"
"hxxp://pastehtml.com/view/bl7qhhp5c.html"
"hxxp://pastehtml.com/view/blafp1ly1.html"
"hxxp://pastehtml.com/view/blakyjwbi.html"
"hxxp://pastehtml.com/view/blal5t64j.html"
"hxxp://pastehtml.com/view/blaoyp0qs.html"
"hxxp://www.lcnongjipeijian.com/loic.html"
"hxxp://www.rotterproxy.info/browse.php/704521df/ccc21Oi8/
vY3liZXJ/jcmltZS5/ob3N0emk/uY29tL1l/tOTBibVY/wL2xvaWM/v/b5/
fnorefer"
"hxxp://www.tandycollection.co.kr/loic.html"
"hxxp://www.zgon.cn/loic.html"
"hxxp://zgon.cn/loic.html"
"hxxp://www.turbytoy.com.ar/admin/archivos/hive.html"

The following are the A records for the referrer sites as of January, 20, 2012:

3g[.]bamatea[.]com	A	218[.]5[.]113[.]218
cybercrime[.]hostzi[.]com	A	31[.]170[.]161[.]36
event[.]seeho[.]co[.]kr	A	210[.]207[.]87[.]195
chatimpacto[.]org	A	66[.]96[.]160[.]151
anonymouse[.]org	A	193[.]200[.]150[.]125
pastehtml[.]com	A	88[.]90[.]29[.]58
lcnongjipeijian[.]com	A	49[.]247[.]252[.]105
www[.]rotterproxy[.]info	A	208[.]94[.]245[.]131
www[.]tandycollection[.]co[.]kr	A	121[.]254[.]168[.]87
www[.]zgon[.]cn	A	59[.]54[.]54[.]204
www[.]turbytoy[.]com[.]ar	A	190[.]228[.]29[.]84

The HTTP requests contained an "id" value based on UNIX time and user-defined "msg" value, for example:

GET /?id=1327014189930&msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20

Other "msg" examples:

msg=%C2%A1%C2%A1NO%20NOS%20GUSTA%20LA%20
msg=:)
msg=:D
msg=Somos%20Legion!!!
msg=Somos%20legi%C3%B3n!
msg=Stop%20S.O.P.A%20:)%20%E2%99%AB%E2%99%AB HTTP/1.1" 200 99406
"http://pastehtml.com/view/bl7qhhp5c.html"
msg=We%20Are%20Legion!
msg=gh
msg=open%20megaupload
msg=que%20sepan%20los%20nacidos%20y%20los%20que%20van%20a%20nacer
%20que%20nacimos%20para%20vencer%20y%20no%20para%20ser%20vencidos
msg=stop%20SOPA!!
msg=We%20are%20Anonymous.%20We%20are%20Legion.%20We%20do%20not%20

forgive.%20We%20do%20not%20forget.%20Expect%20us!

The "msg" field can be arbitrarily set by the attacker.

As of January 20, 20012, US-CERT has observed another attack that consists of UDP packets on ports 25 and 80. The packets contained a message followed by variable amounts of padding, for example:

66:6c:6f:6f:64:00:00:00:00:00:00:00:00:00 | flood.....

Target selection, timing, and other attack activity is often coordinated through social media sites or online forums.

US-CERT is continuing research efforts and will provide additional data as it becomes available.

II. Solution

There are a number of mitigation strategies available for dealing with DDoS attacks, depending on the type of attack as well as the target network infrastructure. In general, the best practice defense for mitigating DDoS attacks involves advanced preparation.

* Develop a checklist or Standard Operating Procedure (SOP) to follow in the event of a DDoS attack. One critical point in a checklist or SOP is to have contact information for your ISP and hosting providers. Identify who should be contacted during a DDoS, what processes should be followed, what information is needed, and what actions will be taken during the attack with each entity.

* The ISP or hosting provider may provide DDoS mitigation services. Ensure your staff is aware of the provisions of your service level agreement (SLA).

* Maintain contact information for firewall teams, IDS teams, network teams and ensure that it is current and readily available.

* Identify critical services that must be maintained during an attack as well as their priority. Services should be prioritized beforehand to identify what resources can be turned off or blocked as needed to limit the effects of the attack. Also, ensure that critical systems have sufficient capacity to withstand a DDoS attack.

* Have current network diagrams, IT infrastructure details, and asset inventories. This will assist in determining actions and priorities as the attack progresses.

* Understand your current environment and have a baseline of daily network traffic volume, type, and performance. This will allow

staff to better identify the type of attack, the point of attack, and the attack vector used. Also, identify any existing bottlenecks and remediation actions if required.

* Harden the configuration settings of your network, operating systems, and applications by disabling services and applications not required for a system to perform its intended function.

* Implement a bogon block list at the network boundary.

* Employ service screening on edge routers wherever possible in order to decrease the load on stateful security devices such as firewalls.

* Separate or compartmentalize critical services:

  * Separate public and private services
  * Separate intranet, extranet, and internet services
  * Create single purpose servers for each service such as HTTP, FTP, and DNS
  * Review the US-CERT Cyber Security Tip Understanding Denial-of-Service Attacks.

III. References

* Cyber Security Tip ST04-015 - <http://www.us-cert.gov/cas/tips/ST04-015.html>

* Anonymous's response to the seizure of MegaUpload according to CNN - <http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/index.htm>

* The Internet Strikes Back #OpMegaupload - <http://anonops.blogspot.com/2012/01/internet-strikes-back-opmegaupload.html>

* Twitter Post from the author of the JavaScript based LOIC code - <http://www.twitter.com/#!/mendes_rs>

* Anonymous Operations tweets on Twitter - <http://twitter.com/#!/anonops>

* @Megaupload Tweets on Twitter - <http://twitter.com/#!/search?q=%2523Megaupload>

* LOIC DDoS Analysis and Detection - <http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html>

* Impact of Operation Payback according to CNN - <http://money.cnn.com/2010/12/08/news/companies/mastercard_wiki/index.htm>

* OperationPayback messages on YouTube -

<http://www.youtube.com/results?search_query=operationpayback>

* The Bogon Reference - Team Cymru -
<http://www.team-cymru.org/Services/Bogons/>

The most recent version of this document can be found at:

<http://www.us-cert.gov/cas/techalerts/TA12-024A.html>

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@cert.org> with "TA12-024A Feedback INFO#919868" in the subject.

For instructions on subscribing to or unsubscribing from this mailing list, visit <http://www.us-cert.gov/cas/signup.html>.

Produced 2012 by US-CERT, a government organization.

Terms of use:

<http://www.us-cert.gov/legal.html>

Revision History

January 24, 2012: Initial release

* Unknown Key
* 0x5713B18C(L)

*** FIRST restricted and confidential use mailing list. Do not Forward, Cc, Bcc, copy or summarize this email outside of the FIRST community without the express permission of the content owner(s). ***

first-teams mailing list
first-teams@lists.first.org

Williston, Sandra

From: [redacted]
Sent: January-25-12 4:01 PM
To: Beaudoin, Luc
Subject: Activity Log

CCIRC Internal Portal - CDO Watch and Operations

Activity Log - Daily Summary

Modify my alert settings View Activity Log

Title	Modified	Modified by	
Weekly technical report	1/24/2012 4:27 PM	Beaudoin, Luc S	New!

Date/Time	1/24/2012 5:00 PM
Short Description	Weekly technical report
Issue Status	Closed
Detail Description	Vireak put together. Indicator research: Indicators SQL injections attempts initiated from [redacted]

s.16(2)(c)
s.19(1)

s.16(2)(c)

Handler Beaudoin, Luc S

Updates

CI Sector / Client Group 01A Federal; 01B Provincial; 01C Municipal

Context

Projects

N&T 25 Jan 2012 1/25/2012 8:04 AM Williston, Sandra **New!**

Date/Time 1/25/2012 9:00 AM

Short Description N&T 25 Jan 2012

Issue Status Closed

Detail Description N&T 25 Jan 2012

Handler Phlek, Vireak

Updates

CI Sector / Client Group

Context

Projects

Weekly technical report

1/25/2012 8:27 AM | Beaudoin, Luc S | Edite

Detail
Description

s.16(2)(c)

Page 1072

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Updates

PKI public key for CFNOC - Daily...	1/25/2012 9:20 AM	Williston, Sandra	New!

Date/Time 1/25/2012 10:00 AM

Short Description PKI public key for CFNOC - Daily Reports

Issue Status Closed

Detail Description CCIRC produces a daily report which covers the past 24 hours Events, Activities, International reporting, publications released, vulnerability and threat watch reporting, and current Cyber News.

This report is released, to a limited distribution list, using PKI

If CFNOC is able to provide a PKI key, either for the Group account [redacted] (or other group address) or an individual who holds a PKI key. CCIRC would like to add you to our distribution list for this daily product.

Handler Williston, Sandra

Updates

Good Morning MCpl Ennover;

Thank you for your response.

The email address you provided below is an internal DWAN address and will not work on our systems external to DND. However, I assumed you meant to send me the SMTP address, [redacted] which I attempted to test using PKI and was unsuccesstul. No address match found.

Is it possible to EXPORT the public key and send to us? Once received, I would like to do a test.

Please advise. 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: TERRY.ENNOVER@forces.gc.ca [mailto:TERRY.ENNOVER@forces.gc.ca]
Sent: January-25-12 8:12 AM
To: [redacted]
Cc: GRAHAM.BELL@forces.gc.ca
Subject: FW: CCIRC Daily Situation Reports

s.16(2)(c)

Good day Sandra

CFNOC Incident Handling [redacted]

Cheers

CI Sector / Client Group

Context

Projects

Anonymous response to MegaUpload 1/25/2012 9:27 AM Williston, Sandra New!

Date/Time 1/25/2012 10:00 AM

Short Description Anonymous response to MegaUpload

Issue Status Closed

Detail Description Information pertaining to Anonymous response to MegaUpload

Handler Williston, Sandra

Updates

CI Sector / Client Group

Context

Projects

CF12-XXX ["Anonymous" DDoS Activ... 1/25/2012 10:11 AM CYBERDO New!

Date/Time 1/25/2012 11:00 AM

Short Description CF12-XXX ["Anonymous" DDoS Activity]

Issue Status Closed

Detail Description Processing for CF12-XXX

Handler Williston, Sandra

Updates

CI Sector / Client Group

Context

Projects

CF12-XXX ["Anonymous" DDoS Activ... 1/25/2012 10:11 AM CYBERDO Edite

Short Description [redacted] CF12-XXX ["Anonymous" DDoS Activity] - Processing

Updates

Shodan - account CyberDo 1/25/2012 11:06 AM Phlek, Vireak New!

Date/Time 1/25/2012 12:00 PM

Short Description Shodan - account CyberDo

Issue Status Closed

Detail Description Create an account for CyberDo in the shodan search engin.

Handler Phlek, Vireak

Updates

CI Sector / Client Group

Context Account creation

Projects

s.13(1)(a)
s.16(1)(b)
s.19(1)
s.20(1)(c)

Contact - [redacted] 1/25/2012 1:27 PM Williston, Sandra **New!**

Date/Time 1/25/2012 2:00 PM

Short Description Contact - [redacted]

Issue Status Closed

Detail Description GOC got a request for CDO to call [redacted]

Handler Phlek, Vireak

Updates I recommended that they send their question to communications@ps-sp.gc.ca with the attention to NCSD and that they clearly indentify the scope of their definition of smartGrid.

CI Sector / Client Group

Context

Projects

[redacted] 1/25/2012 3:04 PM Beaudoin, Luc S **New!**

Date/Time 1/25/2012 3:00 PM

Short Description [redacted]

Issue Status Closed

Detail Description [redacted]
- Tool fixing DNS setting: AVIRA, exe for windows.
- Talk to identifying the source of the data publically, and raising awareness.
- Proposed a single eye-chart with multi-language.

Updates

CI Sector / Client Group 04 Trusted Security Partners

Context

Shodan - account CyberDo 1/25/2012 3:37 PM Phlek, Vireak Edite

Updates

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-25-12 12:36 PM
To: [redacted]
Subject: CF related
Attachments: [redacted]

Could you have a look to see if additional info here would be relevant to CF ? I am reviewing CF....

s.13(1)(a)
s.16(2)(c)

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: Beaudoin, Luc S
Sent: January-24-12 1:08 PM
To: Beaudoin, Luc S
Subject: JS LOIC

[redacted]

Distribution is GREEN (ie: OK to share with need-to-know partners but not to post publicly)

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

Williston, Sandra

From: CCIRC Internal Portal - CDO Watch and Operations [redacted]
Sent: January-24-12 2:00 PM
To: Beaudoin, Luc
Subject: Cyber Events

s.16(2)(c)

CCIRC Internal Portal - CDO Watch and Operations

Cyber Events - Daily Summary

Modify my alert settings View Cyber Events

Title	Modified	Modified by	
CRA Phishing	1/23/2012 2:02 PM	Murphy, Gregg	Edited

Status Closed

Summary

CCIRC received a [redacted] phishing email.

Email prompts user to click on [redacted] in order to obtain refund.

Updates Link was found to be no longer active. No action required.

[redacted] ~~Deleted~~

s.16(2)(c)
s.20(1)(c)

[redacted]

1/23/2012 Moore, Bruce **Edited** 2:46 PM

CE-Number CE12-2592

Status Closed

Summary [redacted] Drone Report: 2012-01-22
notifications to multiple organizations. Hosts within these organizations were infected with DNS Changer malware.

Updates Mon 23/01/2012 2:07 PM
Notifications sent to IT security or technical contacts in the following organizations:
Provincial: 2 Provinces ([redacted]
Energy: 1 Company [redacted]
Telecom: 15 Companies ([redacted]

Transportation: 1 Company [redacted]
Academia: 10 Universities [redacted]

s.16(2)(c)
s.20(1)(b)

CI Sector Affected	[redacted] 01B Provincial; 02A Telecoms; 02C Energy; 02D Transportation; 05 Academia
Date Closed	1/23/2012 2:45 PM
REF_COL_LOOKUP	[redacted] CE12-2592 [redacted] Notifications - Multiple Organizations]

Targeted Email/Trojan .xls Attac... 1/23/2012 3:28 PM Murphy, Gregg New!

CE-Number	CEYY-nnnn
Status	Active
Title	Targeted Email/Trojan .xls Attachment Report
CCIRC Handler	Murphy, Gregg
Take-down	No
Notification	No
Reporting Organization	Other
Summary	CCIRC received a report that an infected .xls file contained [redacted] File is picked up as: http://www.naked-security.com/malware/Downloader.Sarhus/
Updates	
Incident Type	Cat 3 - MALICIOUS CODE / COMPROMISE
CI Sector Affected	01A Federal
Severity	Normal
Impact	Unknown
Primary Contact	
Related Incidents	
CCIRC/GOC Related Product Number	
Date Closed	
_NOT_USED_Secondary Contact	
_NOT_USED_IATFF Event Category	
_NOT_USED_Primary Event	No
_NOT_USED_Related Event(s)	
_NOT_USED_Assigned To	
_NOT_USED_Priority	(2) Normal
_NOT_USED_Category	(2) Category2
_NOT_USED_Due Date	1/23/2012 4:00 PM
REF_COL_LOOKUP	CEYY-nnnn [Targeted Email/Trojan .xls Attachment Report]

Targeted Email/Trojan .xls Attac... 1/23/2012 3:29 PM Murphy, Gregg Edited

CE-Number	[redacted] CE12-2593
Summary	[redacted]

~~http://www.naked-security.com/malware/Downloader.Sarhus/~~
CCIRC received a report that an infected .xls file contained [redacted]

s.16(1)(b)
s.16(2)(c)
s.20(1)(c)

File is picked up as:
http://www.naked-security.com/malware/Downloader.Sarhus/

Updates Sent encrypted notifications to [redacted]

REF_COL_LOOKUP [redacted] CE12-2593 [Targeted Email/Trojan .xls Attachment Report]

ftp credentials post on the Inte... 1/23/2012 4:51 PM Phlek, Vireak **New!**

CE-Number	CEYY-nnnn
Status	Active
Title	ftp credentials post on the Internet
CCIRC Handler	Phlek, Vireak
Take-down	No
Notification	No
Reporting Organization	
Summary	[redacted]
Updates	
Incident Type	Cat 1 - UNAUTHORIZED ACCESS / CREDENTIAL THEFT
CI Sector Affected	01A Federal; 07 Other Institutions
Severity	Normal
Impact	Unknown
Primary Contact	
Related Incidents	
CCIRC/GOC Related Product Number	
Date Closed	
_NOT_USED_Secondary Contact	
_NOT_USED_IATFF Category	Event
_NOT_USED_Primary Event	No
_NOT_USED_Related Event(s)	
_NOT_USED_Assigned To	
_NOT_USED_Priority	(2) Normal
_NOT_USED_Category	(2) Category2
_NOT_USED_Due Date	1/23/2012 5:00 PM
REF_COL_LOOKUP	CEYY-nnnn [ftp credentials post on the Internet]

ftp credentials post on the Inte... 1/23/2012 4:52 PM Phlek, Vireak Edited

CE-Number [redacted] CE12-2594

Summary

[redacted]

s.16(2)(c)
s.20(1)(c)

Updates

REF_COL_LOOKUP [redacted] CE12-2594 [ftp credentials post on the Internet]

hxxp://4ca.ca/ CLONE site with a... 1/24/2012 12:09 PM Williston, Sandra Edited

Updates

1. CCIRC asked PS lawyer for his opinion.
2. CCIRC asked CIRA to review the Registrant's compliance with our policies, rules and procedures.
3. CCIRC advised CTEC

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-24-12 12:59 PM
To: Boily, Mario **s.16(2)(c)**
Subject: FW: Anonymous anti-ACTA threat

C est ca que j ai envoyé hier matin....

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: Beaudoin, Luc S
Sent: January-23-12 12:42 PM
To: GOC-COG
Cc: Danaitis, Algis; 'Tiago Dejesus' (Tiago.Dejesus@rcmp-grc.gc.ca); Maurizio Rosa (Maurizio.Rosa@rcmp-grc.gc.ca); [redacted] Darren Sabourin (Darren.Sabourin@rcmp-grc.gc.ca); * [redacted]
Subject: Anonymous anti-ACTA threat

Ref: CE12-2590

FY Awareness.

SITUATION:

[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

Williston, Sandra

From:
Sent: January-23-12 1:48 PM
To:
Cc:
Subject: RE: CE12-2590 [Operation SACTA Posted on Pastebin]

s.15(1) - Def
s.16(2)(c)

Hi

It appears that the recent DDoS attacks (OpMegaUploader)

The following links may assist in developing an efficient IDS / IPS signature:

http://blog.spiderlabs.com/2011/01/loic-ddos-analysis-and-detection.html
http://isc.incidents.org/diary/Javascript+DDoS+Tool+Analysis/12442
http://nakedsecurity.sophos.com/2012/01/20/anonymous-opmegaupload-ddos-attack/

Thanks,
Gregg

-----Original Message-----
From: @CSE-CST.GC.CA]
Sent: January-23-12 11:44 AM
To:
Subject: RE: CE12-2590 [Operation SACTA Posted on Pastebin]

Classification: UNCLASSIFIED

Thanks, we will look into it.

ctec@cse-cst.gc.ca

-----Original Message-----
From: @ps-sp.gc.ca]
Sent: January 23, 2012 11:09 AM
To:
Cc:
Subject: CE12-2590 [Operation SACTA Posted on Pastebin]

[redacted]

s.16(2)(c)

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

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-23-12 12:36 PM
To: [redacted] Moore, Bruce; Williston, Sandra; Murphy, Gregg
Cc: Phlek, Vireak
Subject: RE: CE12-2590 [Operation SACTA Posted on Pastebin]

s.15(1) - Def
s.16(1)(b)
s.16(2)(c)

We could also pass to CTEC the links to the use by anonymous [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

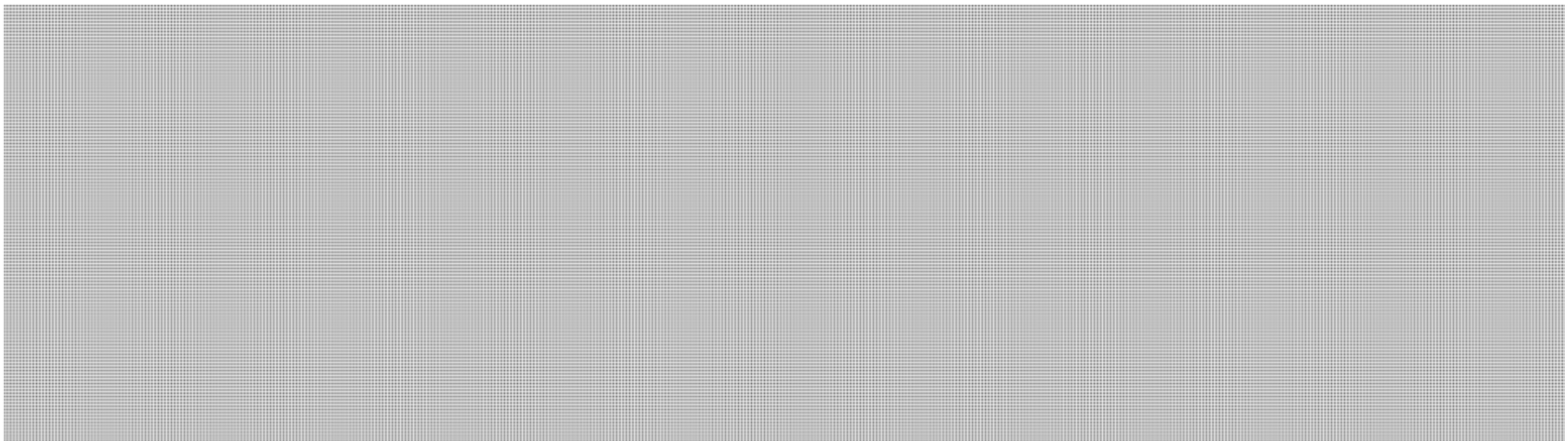
-----Original Message-----
From: [redacted]
Sent: January-23-12 11:10 AM
To: Moore, Bruce; Williston, Sandra; Beaudoin, Luc S
Cc: Phlek, Vireak
Subject: FW: CE12-2590 [Operation SACTA Posted on Pastebin]

FYI, Virak found the following on Pastebin.

-----Original Message-----
From: Gregg.Murphy@ps-sp.gc.ca
Sent: January-23-12 11:09 AM
To: [redacted]CSE-CST.GC.CA> [redacted]CSE-CST.GC.CA)'
Cc: [redacted]
Subject: CE12-2590 [Operation SACTA Posted on Pastebin]

* PGP Signed: 23/01/2012 at 11:08:54 AM

[redacted]



Regards,

s.16(2)(c)

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

* Gregg.Murphy@ps-sp.gc.ca <gregg.murphy@ps-sp.gc.ca>
* 0x0077ACD7

Williston, Sandra

From: Moore, Bruce
Sent: January-20-12 1:25 PM
To: Beaudoin, Luc S; [redacted]
Subject: RE: anonymous and the US

s.16(2)(c)

Done - Jan 20, 2012 1:23:51 PM - via the [redacted]

Bruce

-----Original Message-----
From: Beaudoin, Luc S
Sent: January-20-12 12:38 PM
To: CYBERDO
Cc: Moore, Bruce
Subject: anonymous and the US

Could we please send to US CERT via u5 portal something like that:

/////

CCIRC has been monitoring media and mailist reports about Anonymous actions against US government and private sites. Do not hesitate to contact us to mitigate/coordinate any Canadian nexus of these attacks.

Regards

//////

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 <mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Williston, Sandra

From: Gregg.Murphy@ps-sp.gc.ca
Sent: January-20-12 1:09 PM
To: Klassen, Nathan
Subject: RE: Brief

s.20(1)(c)

Tar sands;

Anonymous also announced "Operation Green Rights/Project Tarmaggedon," [redacted] and others. http://news.cnet.com/8301-27080_3-20078963-245/anonymous-targets-monsanto-oil-firms/

-----Original Message-----
From: Klassen, Nathan
Sent: January-20-12 1:05 PM
To: St-Louis, Danielle
Cc: Murphy, Gregg
Subject: Brief

Hi Danielle,

Today's brief for RD is attached. Ken and Luc are happy with the final product. Could you please read it over for grammar / spacing J / ect? Once done please prepare the official brief and send it over. Cheers,

Nate

Nathan Klassen
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 991-6052
Fax/télécopieur: (613) 996-0995
Email/Courriel: Nathan.Klassen@ps-sp.gc.ca <mailto:Nathan.Klassen@ps-sp.gc.ca>

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-20-12 8:06 AM
To: [redacted]
Cc: Phlek, Vireak; Moore, Bruce; Murphy, Gregg; Williston, Sandra; Melanson, Daryl; Turbide, Frank; Clow, Patrick
Subject: Anonymous and SOPA

$ python twitter.py
Results for search term: [redacted]
URLS

[redacted]

http://t.co/cebkzP9p -> http://www.fbi.gov

[redacted] -> http://www.techdirt.com/articles/20120119/17203417480/mpaa-uses-anon-attacks-to-make-nonsensical-comments-about-free-speech.shtml

[redacted] -> http://anonops.blogspot.com/2012/01/internet-strikes-back-opmegaupload.html?spref=tw

-> [redacted]

TARGETS

HIVE SERVERS

JSLOIC URLS

[redacted]

MOBILELOIC URLS

[redacted]

s.16(1)(b)
s.16(2)(c)

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

Williston, Sandra

From: Bendelier, Kenneth
Sent: January-20-12 6:59 AM
To: Beaudoin, Luc; [redacted]
Subject: Fw: Important: Anonymous downs government, music industry sites in largest attack ever

For the daily?

s.16(2)(c)

----- Original Message -----
From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: Friday, January 20, 2012 03:30 AM
To: Bendelier, Kenneth
Subject: Important: Anonymous downs government, music industry sites in largest attack ever

Generated by your Alert Subscription on Folder:
- Government US
- Anonymous
Source: RT
Complete item: http://rt.com/usa/news/anonymous-doj-universal-sopa-235/

Description:
Hacktivists with the collective Anonymous are waging an attack on the website for the White House after successfully breaking the sites for the FBI, Department of Justice, Universal Music Group, RIAA and Motion Picture Association of America.

In response to todays federal raid on the file sharing service Megaupload, hackers with the online collective Anonymous have broken the websites for the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music Group.

It was in retaliation for Megaupload, as was the concurrent attack on Justice.org, Anonymous operative Barrett Brown tells RT on Thursday afternoon.

E-Secure-IT
https://www.e-secure-it.com

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-20-12 6:45 AM
To: [redacted] s.16(2)(c)
Subject: For daily: Anonymous ddos related to SOPA

Using LOIC and twitter links, anonymous is conducting SOPA related DDOS. We need to research this. This is FYI only from mailing list:
/////
Do *not* click on the pastehtml.com links displayed via this search, else you'll load up LOIC and join the fun:

[redacted]

////

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

Williston, Sandra

From: CYBERDO
Sent: January-18-12 2:34 PM
To: [redacted]
Cc: CTEC
Subject: RE: CE2012-272

s.15(1) - Def
s.16(2)(c)

CTEC;

CCIRC obtained the list from a public website; http://dazzlepod.com/stratfor/ which we used wildcard searches (ie: gc.ca) to find the information we sent you.

Therefore, we confirm that this information is releasable to the requestor.

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: [redacted]@CSE-CST.GC.CA]
Sent: January-18-12 2:13 PM
To: [redacted]
Cc: [redacted]
Subject: CE2012-272

Classification: UNCLASSIFIED

Good Afternoon CyberDO,

CBSA is requesting information for the Stratfor hack and for a list of Canadian Federal Depts. We received the information from you and I would like to verify with you whether or not we can release that information to them. Thanks.

[redacted]
Cyber Threat Evaluation Centre
[redacted]
ctec@cse-cst.gc.ca

From: CBSA/ASFC-IT SECURITY/SECURITE TI [mailto:CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca]
Sent: January 18, 2012 12:14 PM
To: [redacted]

Cc: Samulak, George
Subject: RE: Stratfor hack affects Government of Canada users

Can CTEC provide the following information regarding this hack:

# of Canadian Federal departments affected
List of the # of Canadian Federal departments affected

Regards,

s.15(1) - Def
s.16(2)(c)

George Samulak
Cyber Protection Centre/Centre de Cyber Protection
IT Security Division / Division Sécurité de la TI
Infrastructure Services Directorate / Services d'infrastructure
Information Science & Technology Branch / Direction Générale de l'information, des sciences & de la technologie
Canada Border Services Agency | Agence des services frontaliers du Canada
Government of Canada | Gouvernement du Canada
100 Metcalfe Street (1659), Ottawa, Ontario, K1A 0L8
george.samulak@cbsa-asfc.gc.ca
Telephone | Téléphone 613-952-6717
Facsimile | Télécopieur 613-952-7900
Teletypewriter | Téléimprimeur 1-866-335-3237

From: [redacted]
Sent: December 29, 2011 10:25 AM
To: [redacted]
Cc: [redacted]
Subject: Stratfor hack affects Government of Canada users
Importance: High

Classification: UNCLASSIFIED

Hello,

[redacted]

The hashes for all Stratfor accounts were released allegedly by Anonymous. Some passwords were discovered via a dictionary attack and posted on pastebin [redacted]

[redacted]

It is recommended that users immediately change any passwords on Government of Canada systems if they used the same or similar passwords. Please remind users that this illustrates the importance of using different passwords on different accounts and especially not to reuse passwords that are used on GC systems.

[redacted]

Regards,

[redacted]

s.15(1) - Def

[redacted]

GC-CTEC Cyber Duty Officer

Williston, Sandra

From: [redacted]@CSE-CST.GC.CA>
Sent: January-18-12 2:13 PM
To: CYBERDO
Cc: CTEC
Subject: CE2012-272

s.15(1) - Def

Classification: UNCLASSIFIED

Good Afternoon CyberDO,

CBSA is requesting information for the Stratfor hack and for a list of Canadian Federal Depts. We received the information from you and I would like to verify with you whether or not we can release that information to them. Thanks.

[redacted]
Cyber Threat Evaluation Centre
[redacted]
ctec@cse-cst.gc.ca

From: CBSA/ASFC-IT SECURITY/SECURITE TI [mailto:CBSA/ASFC-IT_SECURITY/SECURITE_TI@cbsa-asfc.gc.ca]
Sent: January 18, 2012 12:14 PM
To: CTEC
Cc: Samulak, George
Subject: RE: Stratfor hack affects Government of Canada users

Can CTEC provide the following information regarding this hack:

# of Canadian Federal departments affected
List of the # of Canadian Federal departments affected

Regards,

George Samulak
Cyber Protection Centre/Centre de Cyber Protection
IT Security Division / Division Sécurité de la TI
Infrastructure Services Directorate / Services d'infrastructure
Information Science & Technology Branch / Direction Générale de l'information, des sciences & de la technologie
Canada Border Services Agency | Agence des services frontaliers du Canada
Government of Canada | Gouvernement du Canada
100 Metcalfe Street (1659), Ottawa, Ontario, K1A 0L8
george.samulak@cbsa-asfc.gc.ca
Telephone | Téléphone 613-952-6717
Facsimile | Télécopieur 613-952-7900
Teletypewriter | Téléimprimeur 1-866-335-3237

Page 1097

is a duplicate

est un duplicata

Williston, Sandra

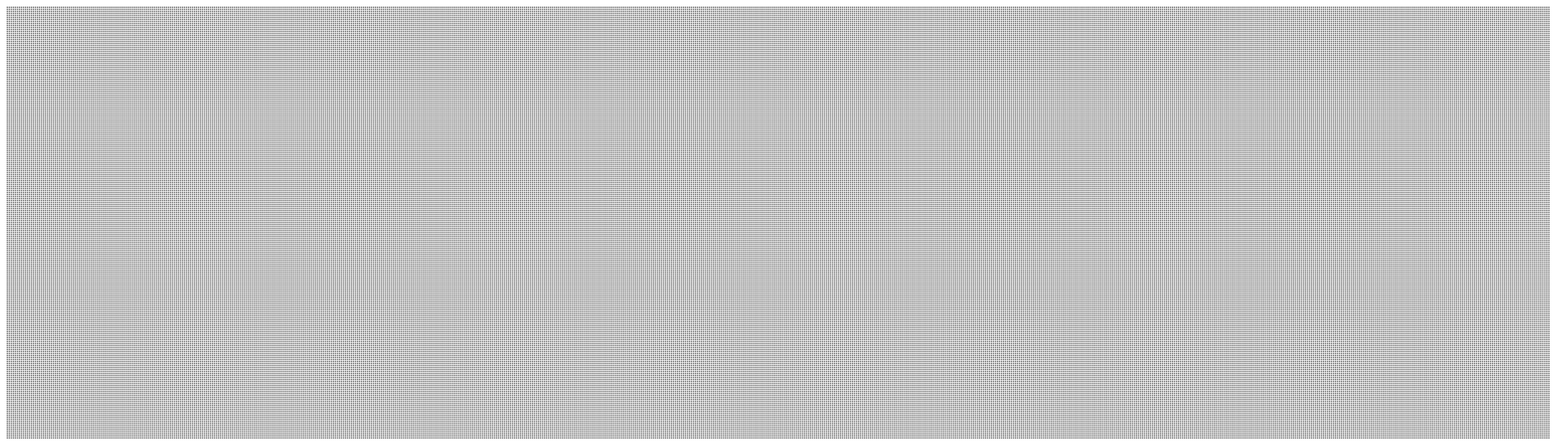
From: Beaudoin, Luc S **s.16(2)(c)**
Sent: January-18-12 9:49 AM
To: Phlek, Vireak
Cc: [redacted]
Subject: Activity 3402

http://www.techspot.com/news/47012-h...da-logins.html (http://www.techspot.com/news/47012-hackers-expose-israeli-government-scada-logins.html)

Hackers expose Israeli government SCADA logins

The drama surrounding Israel continues to unfold as a group of Anonymous hackers expose employee logins to several government websites. Perhaps most disturbingly, this document (http://pastebin.com/ZyEzJnFB) (may be taken down any time) also claims the credentials provided give access to a number of Israel's SCADA (Supervisory Control and Data Acquisition) systems. The document itself includes emails, passwords, hashes and 10 IP addresses that are supposedly Israeli SCADA systems.
At this time of this writing, there were few details regarding the implications. However, such systems are typically used to monitor and regulate processes for industrial control purposes, such as a agricultural complexes, factories or public services and utilities.

[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

Williston, Sandra

From: Beaudoin, Luc S
Sent: January-10-12 1:44 PM
To: [redacted]
Subject: RE: Stratfor Breach

s.19(1)
s.20(1)(c)

[redacted]

Pages 1101 to / à 1102

are withheld pursuant to sections

sont retenues en vertu des articles

20(1)(c), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Page 1103

is withheld pursuant to section

est retenue en vertu de l'article

20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: Timothy O'Neil <tim.oneil@rcmp-grc.gc.ca>
Sent: January-06-12 11:57 AM
To: CYBERDO
Cc: Anderson, Windy; Angus Smith; Anna Gray-Henschel; Darren Sabourin; David Hubley; Debora at Work; Dominic Lafleur; [redacted] Victor Munro
Subject: RE: FW: Stratfor Breach
Attachments: ONeil, Timothy.vcf

Will do and thanks for the follow up.

For my RCMP colleagues please note CCIRC response to the Stratfor breach.

Kindly ensure this message is shared with your RCMP colleagues.

s.13(1)(a)
s.16(2)(c)
s.19(1)

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[redacted]

>>> [redacted] 2012-01-06 11:52 >>>

[redacted]

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"

s.16(1)(a)
s.16(2)(c)

From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-06-12 11:31 AM
To: [redacted]
Cc: Anderson, Windy; Darren Sabourin; [redacted] Victor Munro
Subject: Re: FW: Stratfor Breach

s.16(1)(a)
s.16(2)(c)
s.19(1)

Thanks Sandra

Just so you are aware, my email account was identified on the Stratfor breach and I have not heard anything from anyone on this. So who should I, and for that matter, my RCMP colleagues have heard from within the GoC on this issue?
Thanks.....Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[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. »
>>> [redacted] 2012-01-06 11:24 >>>
Good Day;

[redacted]

Hope this helps.

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

From: Anderson, Windy
Sent: January-06-12 9:17 AM
To: [redacted]

Subject: FW: Stratfor Breach

Can someone get back to Tim about what we are doing on this?
Have a great day,

s.16(2)(c)
s.19(1)

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
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-06-12 9:04 AM
To: Angus Smith; Bruce Rae; Darren Sabourin; [redacted]
Cc: Anderson, Windy; John (CI) SUTHERLAND; tiago.dejesus@rcmp-grc.gc.ca; Victor Munro
Subject: Re: Stratfor Breach

Thank you [redacted] and Angus for sharing.

This type of messaging will probably occur more frequently.

By means of this message I am providing to [redacted] for his assessment.

Darren - do you have the means to check out the noted websites, and provide an assessment for this obviously bogus message.

I am aiming to provide an updated assessment to our stakeholders so they should be aware as to how to handle these types of messages.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[redacted]

>>> [redacted] 2012-01-06 08:40 >>>
[redacted]

s.16(1)(a)
s.19(1)

s.16(2)(c)
s.19(1)

Williston, Sandra

From: [redacted]
Sent: January-06-12 11:52 AM
To: 'Timothy O'Neil'; [redacted]
Cc: Anderson, Windy; Darren Sabourin; [redacted] Victor Munro
Subject: RE: FW: Stratfor Breach

[redacted]

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: January-06-12 11:31 AM
To: [redacted]
Cc: Anderson, Windy; Darren Sabourin; [redacted] Victor Munro
Subject: Re: FW: Stratfor Breach

Thanks Sandra

Just so you are aware, my email account was identified on the Stratfor breach and I have not heard anything from anyone on this. So who should I, and for that matter, my RCMP colleagues have heard from within the GoC on this issue?
Thanks.....Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[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. »
>>> [redacted] 2012-01-06 11:24 >>>
Good Day;

[redacted]

Hope this helps.

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

From: Anderson, Windy
Sent: January-06-12 9:17 AM
To: [redacted]
Subject: FW: Stratfor Breach

Can someone get back to [redacted] about what we are doing on this?
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
From: [redacted]
Sent: January-06-12 9:04 AM
To: [redacted]
Cc: Anderson, Windy; [redacted] tiago.dejesus@rcmp-grc.gc.ca; Victor Munro
Subject: Re: Stratfor Breach

Thank you [redacted] and Angus for sharing.

[redacted]

>>> Dominic Lafleur 2012-01-06 08:40 >>>
Good morning [redacted]

[redacted]

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265

s.19(1)

Williston, Sandra

From: [redacted]
Sent: January-06-12 11:41 AM
To: 'tim.oneil@rcmp-grc.gc.ca'; [redacted] s.16(2)(c)
Cc: Anderson, Windy; CYBERDO
Subject: RE: Stratfor Breach

Good Day Tim;

Thank you for the information below.

We were not aware of this twitter posting, but it sounds like they are preparing for another "wave".

We will stay diligent and keep you informed if we see anything. 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: Anderson, Windy
Sent: January-06-12 10:54 AM
To: [redacted]
Subject: FW: Stratfor Breach

fyi

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

s.15(1) - Subv
s.16(2)(c)
s.19(1)

From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-06-12 10:07 AM
To: bev.richardson@cbsa-asfc.gc.ca; [redacted] Anderson, Windy; Darren Sabourin; Ken Mcphee; [redacted]
Cc: Robert Lafrance; tiago.dejesus@rcmp-grc.gc.ca
Subject: Stratfor Breach

Good Day Darren and Windy

Are either of you two able to provide more information/assessment relating to this?

Specifically: "The Anonymous syndicate behind the recent hacking of Stratfor has published "another exciting [redacted] zine release, and this is a big one."

I believe that we will be getting many more similar requests for assistance regarding this issue.

Tim

Tim O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Intelligence Team
National Security Criminal Investigations
613-949-0265
[redacted]

>>> [redacted] 2012-01-06 07:36 >>>

I found this on twitter via this email not sure what it means or what the implications are.....F.Y.I.

Results for [redacted]

- **Tweets ·**
- Top
  - **Top**
  - **All**
  - **With links**
- Refine results »

»

[redacted]AnonymousIRC
Countdown to Lulz started. Fasten your seatbelts. [redacted]

s.15(1) - Subv
s.16(1)(a)
s.16(2)(c)

13 hours ago
Retweeted 100+ times
»

The Anonymous syndicate behind the recent hacking of Stratfor has published "another exciting zine release, and this is a big one."

CRIIU

From:
Sent: January-05-12 11:45 AM
To: bev.richardson@cbsa-asfc.gc.ca; Ken Mcphee; Terry Pomeroy
Subject: Fwd: Stratfor Breach
For information purposes and dissemination as you see fit to other partners and agencies.;

Pages 1115 to / à 1118

are withheld pursuant to section

sont retenues en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: [redacted]
Sent: January-06-12 11:25 AM
To: Timothy O'Neil (tim.oneil@rcmp-grc.gc.ca)
Cc: [redacted] Anderson, Windy
Subject: FW: Stratfor Breach

Good Day;

[redacted]

I have requested our Technical Analysis Team to perform analysis on the three links in the email received by Dominic Lafleur. We will let you know the results when they are back.

[redacted]

Hope this helps.

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

From: Anderson, Windy
Sent: January-06-12 9:17 AM
To: [redacted]
Subject: FW: Stratfor Breach

Can someone get back to Tim about what we are doing on this?
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
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]

Pages 1120 to / à 1121

are withheld pursuant to section

sont retenues en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From:
Sent: January-06-12 10:32 AM
To:
Subject: FW: Internet facing device. [PGP]
Attachments: PGPexch.htm.pgp; Message2.pgp

s.13(1)(a)
s.16(2)(c)

[redacted]

*** END PGP DECRYPTED/VERIFIED MESSAGE ***

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"

Page 1123

is withheld pursuant to sections

est retenue en vertu des articles

16(2)(c), 13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

-----END PGP MESSAGE-----

Williston, Sandra

From: Darke, Peter
Sent: January-06-12 9:41 AM
To: Mack, Laurie; Clow, Patrick; Bergeron, Dominic
Subject: FW: Symantec Confirms Source Code Leak in Two Enterprise Security Products

fyi

Peter Darke
Senior Advisor | Conseiller
Network & Security | Réseau et Sécurité
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West, Ottawa Ontario K1A 0P8 | 269, avenue Laurier Ouest Ottawa (Ontario) K1A 0P8
Tel | Tél: (613) 991-7750
Fax | Téléc: (613) 996-1085
Email | Courriel: peter.darke@ps-sp.gc.ca
Web: www.publicsafety.gc.ca | www.securitepublique.gc.ca

From: CSO News Watch [mailto:cso_newsletters@cxolyris.cxomedia.com]
Sent: January 6, 2012 9:40 AM
To: Darke, Peter
Subject: Symantec Confirms Source Code Leak in Two Enterprise Security Products

GCHQ Awards Bonuses to Stop IT Security Experts Leaving | WhatsApp to Roll Out Stronger Fixes for Messaging Vulnerability

CSO News Watch

Forward this to a Friend >>>

Symantec Confirms Source Code Leak in Two Enterprise Security Products

Symantec late Thursday confirmed that source code used in two of its older enterprise security products was publicly exposed by hackers this week. **Read More**

In this Issue

- GCHQ Awards Bonuses to Stop IT Security Experts Leaving
- WhatsApp to Roll Out Stronger Fixes for Messaging Vulnerability
- E-Voting Machine Freezes, Misreads Votes, U.S. Agency Says
- Government engineers actively plan for cyberwar
- U.S. State Department Investigating Huawei on Iran Concerns
- Murdoch Wife Fake Twitter Account Highlights Online Identity Risk
- Privacy 2012: I know what you did at 3:30 a.m.
- Ramnit Worm Goes After Facebook Credentials
- Facebook Timeline Scams Prey on Wishful Thinking
- Anatomy of an ATM Skimmer Scam

- Lawmakers Seem Intent on Approving SOPA, PIPA
- Microsoft Plans Big January Patch Tuesday
- Blind spots: How cyber defense is like stopping Tim Tebow
- Two New Security Books Ponder: Just How Vulnerable Are We?
- SpyEye Malware Borrows Zeus Trick to Mask Fraud
- Smart Grid Security Inadequate, Threats Abound
- Murder Retrial Ordered After Court Records Destroyed By Virus
- Japan Testing 'virus' Cyberdefence Weapon, Reports Say
- Anonymous Threatens Sony, Spares PSN Customers
- Windows 8 Can Scrub Data From Disk, but Not Up to Tough Security Specifications
- Microsoft Researcher: Passwords Aren't Dead but They Need Fixing
- Facebook Brings Back the Hack
- Anonymous Targets Neo-Nazis Sites: Anti-Hate Groups Condemn Action

GCHQ Awards Bonuses to Stop IT Security Experts Leaving

Can they compete with IT giants though? **Read More**

WhatsApp to Roll Out Stronger Fixes for Messaging Vulnerability

The problem lets someone change the status message of another person merely by knowing their phone number **Read More**

E-Voting Machine Freezes, Misreads Votes, U.S. Agency Says

DS200 optical scanner from ES&S doesn't meet federal standards, but remains certified, Election Assistance Commission says **Read More**

Government engineers actively plan for cyberwar

Governments are arming themselves to their cyber-teeth with offensive and counter-defense cyber weapons, and there's little enterprises can do to avoid the fray. **Read More**

U.S. State Department Investigating Huawei on Iran Concerns

Six U.S. lawmakers have previously called for the investigation of Huawei's activities in Iran **Read More**

Murdoch Wife Fake Twitter Account Highlights Online Identity Risk

Fake Wendi Deng Murdoch account was initially verified by Twitter as genuine **Read More**

Privacy 2012: I know what you did at 3:30 a.m.

For a peek into what experts expect this year and beyond when it comes to privacy, we turn to the Rebecca Herold (aka the Privacy Professor) for answers. **Read More**

Ramnit Worm Goes After Facebook Credentials

The worm appears to have collected 45,000 logins and passwords already, according to Seculert **Read More**

Facebook Timeline Scams Prey on Wishful Thinking
Read More

Anatomy of an ATM Skimmer Scam
Skimmers could steal your financial information at the ATM—or even at your local supermarket. Here's how to protect yourself.
Read More

Lawmakers Seem Intent on Approving SOPA, PIPA
So far, strong opposition to the copyright bills hasn't changed many minds **Read More**

Microsoft Plans Big January Patch Tuesday
Mystery of the month, say experts, is what Microsoft means by 'security feature bypass' update **Read More**

Blind spots: How cyber defense is like stopping Tim Tebow
Michigan's CTO on the extremes of marketing hype and defeatist mentality in security **Read More**

Two New Security Books Ponder: Just How Vulnerable Are We?
Read More

WEBCAST: CA Technologies

A Step-by-Step Guide to Building Virtualization Maturity
This webinar will explain the key phases of virtualization maturity, outline the critical maturity challenges, and provide you with a step-by-step guide to building your virtualization maturity and maximizing your virtualization outcomes. **View Now**

SpyEye Malware Borrows Zeus Trick to Mask Fraud
One of the most powerful banking trojans has an additional tricky feature, according to Trusteer **Read More**

Smart Grid Security Inadequate, Threats Abound
Read More

Murder Retrial Ordered After Court Records Destroyed By Virus
Stenographer blamed after backup records nixed **Read More**

Japan Testing 'virus' Cyberdefence Weapon, Reports Say
Capable of tracing and disabling attackers **Read More**

Anonymous Threatens Sony, Spares PSN Customers
The hacker collective threatens to expose private information of Sony executives, promising to spare customers and the PlayStation Network **Read More**

Windows 8 Can Scrub Data From Disk, but Not Up to Tough Security Specifications
Read More

Microsoft Researcher: Passwords Aren't Dead but They Need Fixing
Read More

Facebook Brings Back the Hack
In its third annual Hacker Cup, Facebook is inviting programmers to rapidly solve programming challenges **Read More**

Anonymous Targets Neo-Nazis Sites: Anti-Hate Groups Condemn Action
Anonymous hacktivists name names at Nazi-leaks.net in latest round of attacks against controversial targets **Read More**

Editor's Picks: All-time classics, part 3

1. What is a Chief Security Officer?
2. A few good information security metrics
3. 10 tough security interview questions and how to answer them
4. Red gold rush: The copper theft epidemic
5. 19 ways to build physical security into a data center

Get more CSO peer perspective online
LinkedIn | Facebook | Twitter

Williston, Sandra

From: [redacted]
Sent: January-05-12 2:01 PM
To: Beaudoin, Luc
Subject: Cyber Events

s.16(2)(c)
s.20(1)(b)

CCIRC Internal Portal - CDO Watch and Operations

Cyber Events - Daily Summary

Modify my alert settings View Cyber Events

Title	Modified	Modified by	
[redacted] **Drone Notifications...**	1/4/2012 2:21 PM	Moore, Bruce	Edited

CE-Number [redacted] CE12-2559

Status [redacted] Closed

Summary [redacted] Canada Drone Report: 2012-01-03 notifications to multiple organizations. Hosts within these organizations were communicating with a [redacted] sinkhole server. Infection types included (DNS Changer, Mebroot, or Torpig).

Updates

Wed 04/01/2012 12:27 PM
Notifications sent to IT security or technical contacts in the following organizations:
Federal: [redacted]
Provincial: [redacted]
Financial: [redacted]

CI Sector [redacted] Federal; Provincial; CI - Bank / Finance

Date Closed 1/4/2012 1:55 PM

REF_COL_LOOKUP [redacted] CE12-2559 [redacted] Drone Notifications - Multiple Organizations]

Possible compromised .ca TLDs	1/5/2012 8:09 AM	Pitcher Robert	Edited

Status [redacted] Closed

Updates [redacted]

CCIRC processing these notifications through our regular channels.

Closing event.

Possible compromised website ser... 1/5/2012 9:15 AM Moore, Bruce **New!**

CE-Number	CE12-nnnn
Status	Active
Title	Possible compromised website serving malware [redacted]
CCIRC Handler	Moore, Bruce
Take-down	Yes
Notification	No
Reporting Organization	SpyEye Tracker
Summary	
Updates	
Incident Type	Cat 3 - MALICIOUS CODE / COMPROMISE
CI Sector	Other industries
Severity	Normal
Impact	Degradation / disruption
Primary Contact	
Related Incidents	
_NOT_USED_Secondary Contact	
_NOT_USED_IATFF Category	Event
_NOT_USED_Primary Event	No
_NOT_USED_Assigned To	
_NOT_USED_Priority	(2) Normal
_NOT_USED_Category	(2) Category2
_NOT_USED_Due Date	1/5/2012 10:00 AM
REF_COL_LOOKUP	CE12-nnnn [Possible compromised website serving malware [redacted]

s.16(2)(c)

Stratfor Hack affected Canadians 1/5/2012 10:42 AM Williston, Sandra Edited

Updates

[redacted]

Pages 1131 to / à 1133

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: [redacted]@CSE-CST.GC.CA>
Sent: January-05-12 12:10 PM
To: CYBERDO
Cc: CTEC
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

s.15(1) - Def
s.16(2)(c)

Classification: UNCLASSIFIED

Thanks Sandra... I think!

[redacted]
Cyber Threat Evaluation Centre
[redacted]
ctec@cse-cst.gc.ca

From: [redacted]@ps-sp.gc.ca]
Sent: January 5, 2012 11:08 AM
To: CTEC; CYBERDO
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Good Day;

Further to our email from 27 December.

[redacted]

Pages 1135 to / à 1136

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

s.15(1) - Def

s.16(2)(c)

"Patience isn't a skill — it's a decision"

From: [redacted]@CSE-CST.GC.CA]
Sent: January-04-12 1:31 PM
To: CYBERDO
Cc: CTEC
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Hi,

thanks for the email. We did use the file with all email addresses when contacting departments last week, not just the cracked ones and have verified that departments were contacted with regards to all the email addresses in your spreadsheet.

cheers,

[redacted]

GC-CTEC Cyber Duty Officer

From: [redacted]@ps-sp.gc.ca]
Sent: January 4, 2012 1:08 PM
To: CYBERDO; CTEC
Subject: RE: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Good Afternoon CTEC;

For clarification and possible action.

[redacted]

s.15(1) - Def

s.16(2)(c)

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: [redacted]
Sent: December-27-11 1:14 PM
To: 'CTEC <[redacted]CSE-CST.GC.CA> [redacted]CSE-CST.GC.CA)'
Cc: CYBERDO
Subject: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Greetings GTEC,

We have received a report from a partner that did a research on Stratfor hack mentioned in different news outlet (http://www.cbc.ca/news/world/story/2011/12/25/anonymous-hackers.html). Include are link to pastebin of the post and a compress file(.piz) of a different Anonymous release on Stratfor.

[redacted]

Please acknowledge.

Thanks

Vireak Phlek
Cyber Duty Officer
Public Safety Canada

s.15(1) - Subv
s.16(1)(a)
s.16(2)(c)

Williston, Sandra

From: [redacted]
Sent: January-04-12 3:31 PM
To: 'Darren Sabourin'; [redacted]
Cc: [redacted]
Subject: RE: Fw: Release of Canadian Government and Corporate usernames and passwords

Darren;

Thank you for the explanation and the links.

CCIRC is responsible for receiving the information for notification purposes. We are not limited to ps-sp.gc.ca users.

Once we receive any data, we parse it and split up the "gc.ca" user and provide them to CTEC (Federal Government CERT) for notification. Public Safety is included in this list for CTEC to notify. CCIRC will not notify Public Safety users directly.

However, with the remainder of the Canadian users, CCIRC would like to parse through and locate any Critical Infrastructure we are responsible to notify.

As for who will notify the "Joe Public" user, at this point, CCIRC does not have the resources to do such a large notification. However, Stratfor should be doing this themselves, for all their clients anyway.

Again, thank you for the links. We will grab the FULL list and start CI notifications.

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: Darren Sabourin [mailto:Darren.Sabourin@rcmp-grc.gc.ca]
Sent: January-04-12 2:06 PM
To: [redacted]
Cc:
Subject: Fwd: Fw: Release of Canadian Government and Corporate usernames and passwords

The size of the initial email dump has changed significantly.

There are two lists that I am now referring to.

[redacted]

Pages 1140 to / à 1141

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 16(1)(a), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

Thank you for any info you can provided.

s.16(2)(c)

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"

s.16(1)(a)

Williston, Sandra

From: Darren Sabourin <Darren.Sabourin@rcmp-grc.gc.ca>
Sent: January-04-12 2:06 PM
To:
Cc:
Subject: Fwd: Fw: Release of Canadian Government and Corporate usernames and passwords
Attachments:

Page 1144

is withheld pursuant to sections

est retenue en vertu des articles

16(1)(a), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

From: [redacted]
Date: Wed, 4 Jan 2012 18:15:56 +0000
To: 'Darren Sabourin'
Cc: [redacted]
Subject: RE: Release of Canadian Government and Corporate usernames and passwords

Hello Darren;

The information you provided below, [redacted] has been processed.

[redacted]

Thank you for any info you can provided.

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"

Williston, Sandra

From: [redacted]
Sent: January-04-12 1:16 PM
To: 'Darren Sabourin'
Cc: [redacted]
Subject: RE: Release of Canadian Government and Corporate usernames and passwords

Hello Darren;

The information you provided below, [redacted] has been processed.

[redacted]

Thank you for any info you can provided.

s.15(1) - Subv
s.16(1)(a)
s.16(2)(c)
s.19(1)

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: Darren Sabourin [mailto:d[redacted]
Sent: December-26-11 10:47 PM
To: [redacted]
Cc: dave.bachynski@rcmp-grc.gc.ca; [redacted] Tim O'Neil; Tiago Alves de Jesus
Subject: Re: Release of Canadian Government and Corporate usernames and passwords

[redacted]

Page 1147

is withheld pursuant to section

est retenue en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: Alain.Labossiere@ic.gc.ca
Sent: January-04-12 11:38 AM
Subject: U2 - N3 - Stratfor Breach

U2 - N3 - Subject: Stratfor Breach

"...
On December 25, 2011, the Anonymous group hacked into a private intelligence agency, Strategic Forecasting Inc. or STRATFOR, based in Austin, Texas. The attack began with the release of STRATFOR's client list announced at https://twitter.com/#!/AnonymousIRC/status/150679351589998593 followed by release of accounts in batches believed to belong to STRATFOR's customers. The release announced in another Twitter post at https://twitter.com/#!/AnonymousIRC/status/150985258999885824 includes emails, passwords (hashed with MD5), home/office addresses and credit card information (full 16-digit number, expiry date and CVV number). The table below is the list of of the leaked accounts with the passwords removed.

STRATFOR has brought down their site following the attack but kept their members posted on the status of the attack via their Facebook page.

For ease of reference try: http://dazzlepod.com/stratfor/

..."

According to this website:

"...

UPDATE (January 2, 2012): We have processed all 860,000 STRATFOR's registered users and added them into the table below. These users do not have their credit card information leaked. The earlier accounts with credit card information leaked are now tagged with "cc" in the table below.

This disclosure was mentioned in PCWorld, Forbes, CNN and TheBlaze.

UPDATE (December 30, 2011): The Anonymous group has just released the remaining accounts making the total of leaked STRATFOR's accounts with credit card information to a total of approx. 75,000. The table below has been updated to include these accounts. Additionally, login information for approx. 860,000 STRATFOR's registered users have been leaked as well but they don't include credit card information; we may update the table below to include these users later.
..."

Williston, Sandra

From: Moore, Bruce
Sent: January-04-12 9:10 AM
To: [redacted]
Subject: FW: Stratfor Breach
Attachments: ONeil, Timothy.vcf

s.16(1)(a)
s.16(2)(c)

-----Original Message-----
From: Timothy O'Neil [mailto:tim.oneil@rcmp-grc.gc.ca]
Sent: January-03-12 3:52 PM
To: tim.oneil@rcmp-grc.gc.ca
Subject: Stratfor Breach

YOU ARE BLIND COPIED

[redacted]

Page 1150

is withheld pursuant to section

est retenue en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: Clow, Patrick
Sent: January-04-12 7:42 AM
To: Turbide, Frank; Anderson, Windy
Subject: FW: UPDATE - Stratfor breach

s.16(1)(a)

Some information related to the Stratfor breach. Not sure if this is of any value to us?

From: Scott Foster [mailto:Scott.Foster@rcmp-grc.gc.ca]
Sent: January-03-12 4:13 PM
To: Scott Foster
Subject: UPDATE - Stratfor breach

Good day,

Page 1152

is withheld pursuant to section

est retenue en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

s.16(1)(a)
s.16(1)(b)
s.16(2)(c)

Williston, Sandra

From: Moore, Bruce
Sent: January-03-12 1:09 PM
To: 'Scott.Foster@rcmp-grc.gc.ca'
Cc: Bendelier, Kenneth; [redacted]
Subject: RE: CIIT Update - STRATFOR Breach [CCIRC CE11-2549]

Good Afternoon Scott & Happy New Year;

[redacted]

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From: Bendelier, Kenneth
Sent: January-03-12 11:05 AM
To: Moore, Bruce
Subject: Fw: CIIT Update - STRATFOR Breach

Hi Bruce,

If you're in, you might want to update Scott on what we've done.

Thanks

From: Scott Foster [mailto:Scott.Foster@rcmp-grc.gc.ca]
Sent: Tuesday, January 03, 2012 11:03 AM
To: Scott Foster <Scott.Foster@rcmp-grc.gc.ca>
Subject: CIIT Update - STRATFOR Breach

Good day,

[redacted]

Pages 1154 to / à 1155

are withheld pursuant to section

sont retenues en vertu de l'article

16(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Centre des opérations du gouvernement

Rapport quotidien — 1er novembre 2011

SOMMAIRE

ÉVÈNEMENTS, INCIDENTS ET POINTS D'INTÉRÊT

ADDENDA CLASSIFIÉ AU RAPPORT QUOTIDIEN : Il n'y a pas d'addenda classifié aujourd'hui.

INCIDENTS EN COURS

Rien d'important à signaler.

À VENIR

1. Les 3 et 4 novembre 2011 : Sommet du G20 à Cannes, en France : La France accueillera le 6e Sommet du G20 les 3 et 4 novembre 2011. Le très honorable Stephen Harper, premier ministre du Canada, sera à la tête de la délégation canadienne. Le CIET estime que la menace est FAIBLE pour la délégation canadienne qui assistera au Sommet du G20 en France.

2. Le 5 novembre 2011 : appel du groupe « Anonymous » à commettre des actes de nuisance à l'occasion de la Journée Guy Fawkes : Le groupe international de cyber-pirates « Anonymous » a diffusé en ligne un message incitant ses sympathisants à participer à diverses activités de nuisance ciblant des sites Web du gouvernement et des médias le 5 novembre, pour commémorer la Journée Guy Fawkes. L'initiative, baptisée « Operation Injustice Awareness », incite les sympathisants du groupe à défigurer des sites Web et à rediriger les visiteurs de ces sites vers des messages qu'il a diffusés sur Twitter, selon sa façon de faire habituelle. Le groupe incite également ses sympathisants à descendre dans la rue, à porter des masques à l'effigie de Guy Fawkes et à défigurer leur ville en y faisant des graffitis, à affronter quiconque les interpelle et à capter des images de leurs actes pour ensuite les télécharger sur les médias sociaux. L'ACTI ignore si l'opération annoncée visera des systèmes informatiques ou des installations physiques du gouvernement du Canada ou des médias canadiens.

Page 1157

is withheld pursuant to section

est retenue en vertu de l'article

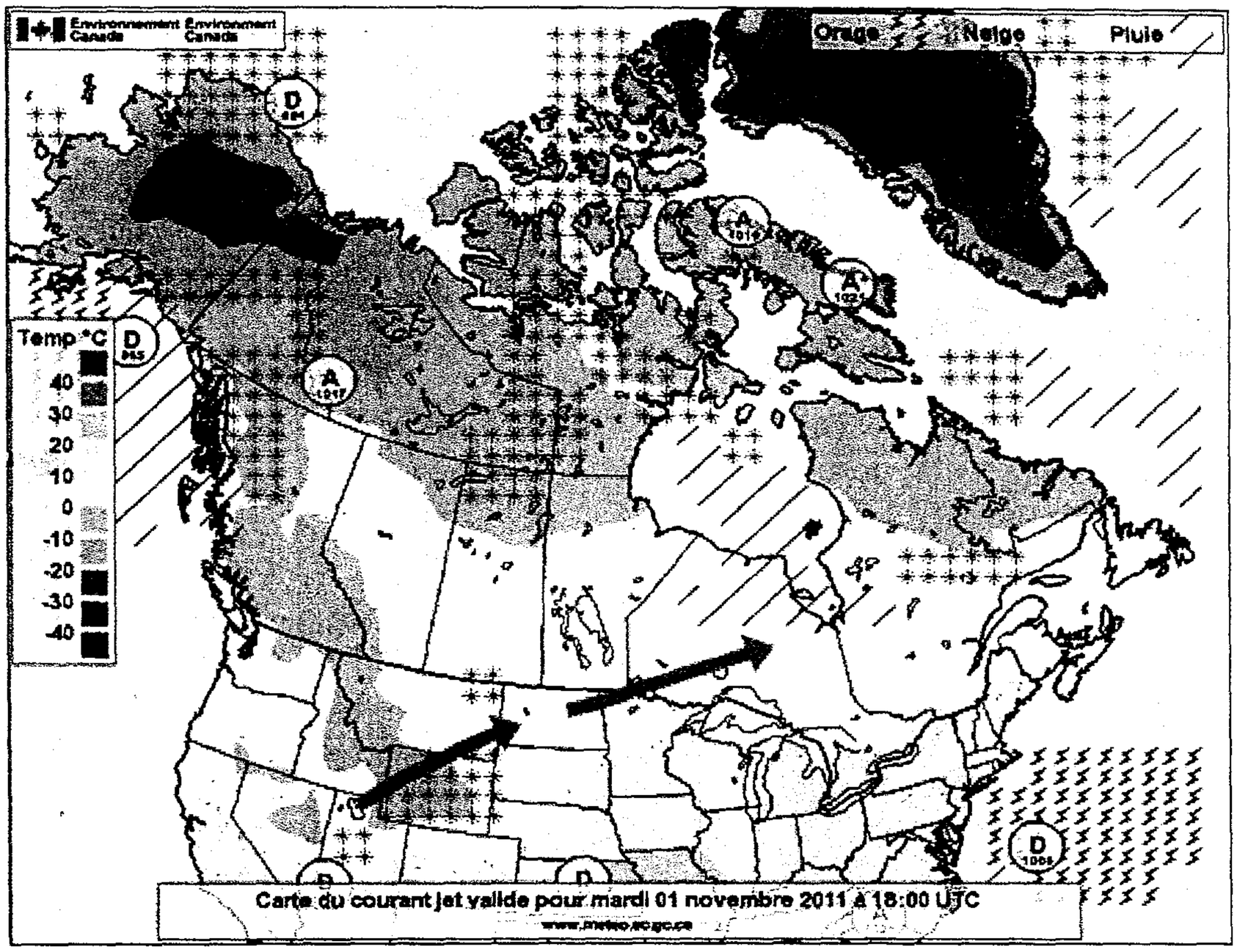
15(1) - Subv

of the Access to Information

de la Loi sur l'accès à l'information

CENTRE MÉTÉOROLOGIQUE CANADIEN

Météo au Canada



Légende:

A 1019 **Anticyclone** hPa-hectopascal

D 1007 **Dépression** hPa-hectopascal

Courant-jet

Situation météorologique importante

Aperçu

Une dépression qui se forme dans l'Est du Pacifique se déplacera au-dessus du Yukon au cours de la nuit et provoquera de la neige abondante dans le Nord de la Colombie-Britannique et le Sud du Yukon, le long de la route Haines. De 15 à 25 cm de neige sont attendus. De la pluie et des vents violents toucheront aussi la côte de la Colombie-Britannique plus tard aujourd'hui.

Avertissements

Colombie-Britannique/Yukon : Neige dans le Nord de la Colombie-Britannique et le Sud du Yukon.

Source : Centre météorologique canadien – Environnement Canada

Anderson, Windy

From: Bendelier, Kenneth
Sent: January-25-12 9:01 AM
To: Dick, Robert
Cc: Hatfield, Adam; Cameron, Bud; Beaudoin, Luc S; Anderson, Windy
Subject: Deck For CCIRC <-> DHS Brief
Attachments: *CCIRC Overview Presented to DHS.ppt*

Importance: High

Good morning,

Please find attached the proposed CCIRC – DHS Brief for tomorrow. It is, essentially, relevant plagiarism of the Brief to the DM, Adam's Brief to the DND IA Symposium with additional input from CCIRC's Operations Section.

For your review.

Thanks

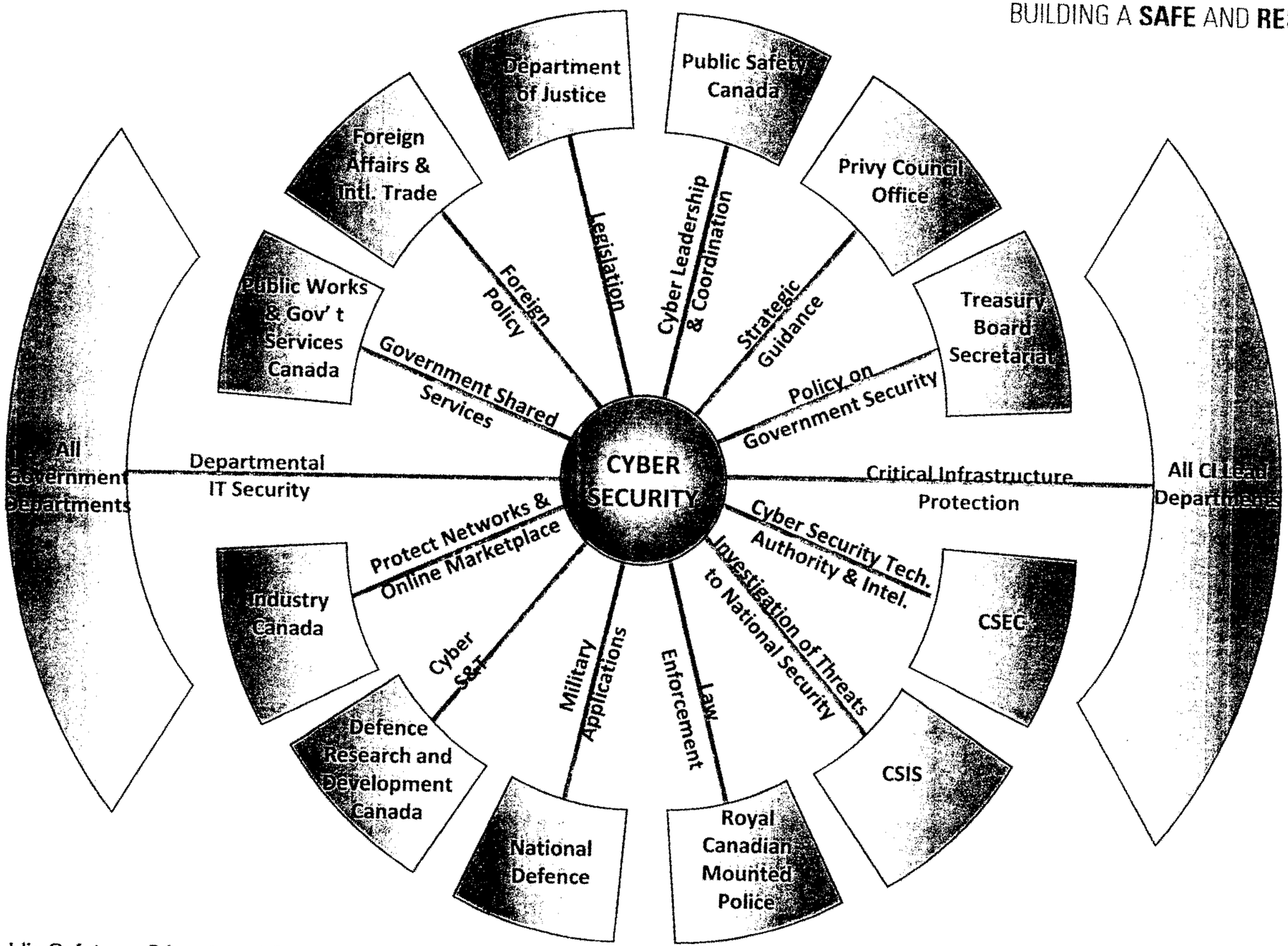
Ken Bendelier, CD, MSc
Cyber Support Officer | Agent de soutien cybernétique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West | 269 rue Laurier ouest
Ottawa, Ontario
Canada K1A 0P8
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

UNCLASSIFIED

...curity Roles and Responsibilities ...m the Government of Canada

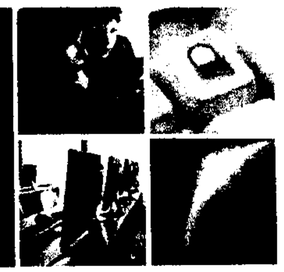
BUILDING A **SAFE** AND **RESILIENT CANADA**



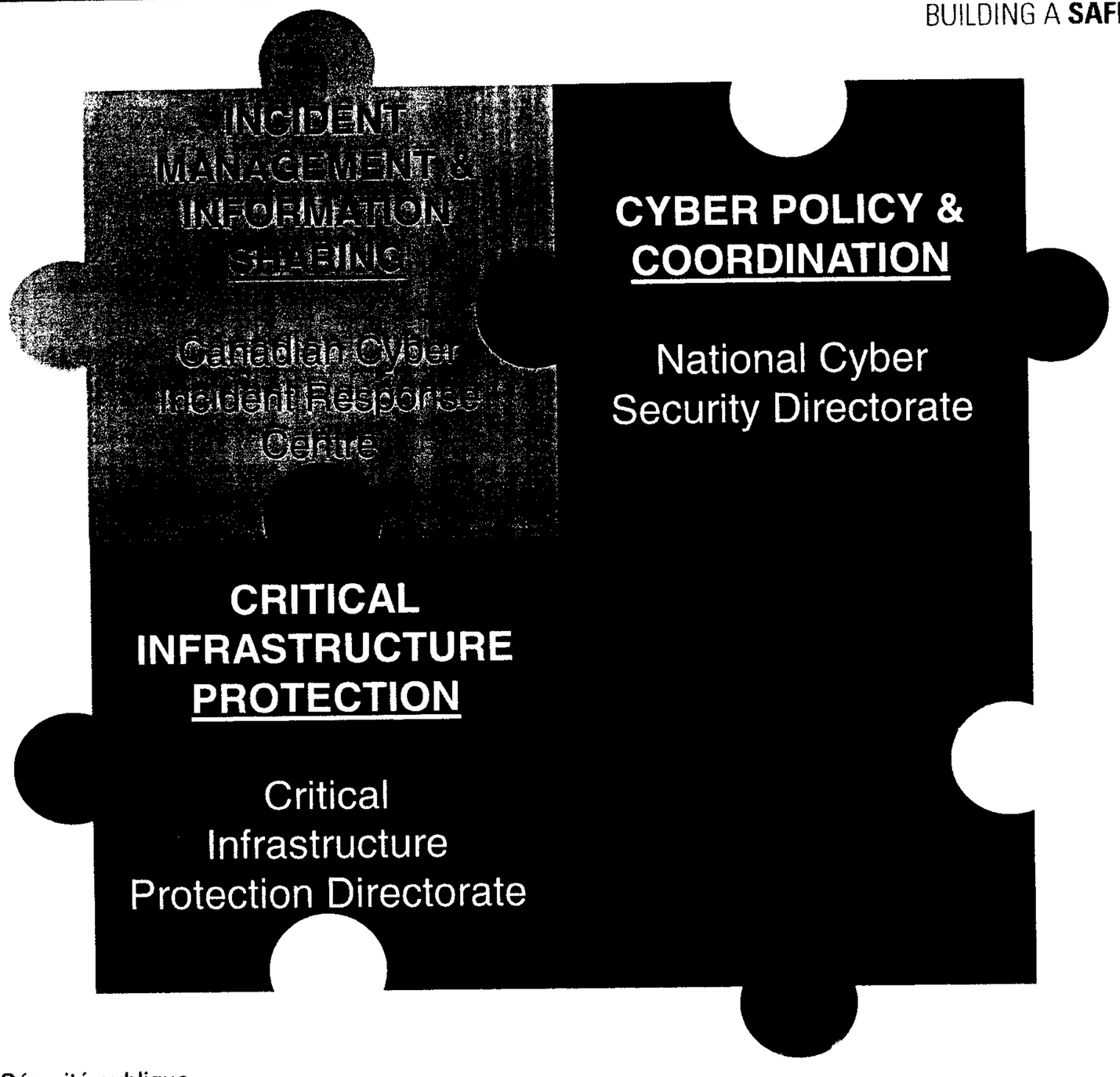
Public Safety Canada | Sécurité publique Canada

01160

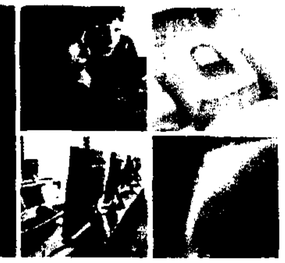
Cyber Security Roles and Responsibilities within Public Safety Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**



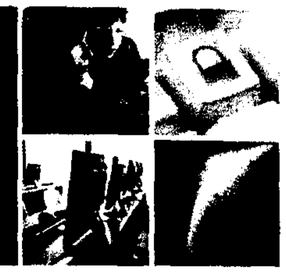
Division of Cyber Security Roles in Canada



BUILDING A **SAFE** AND **RESILIENT CANADA**

- On June 20, 2011, the responsibilities between Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) and Communications Security Establishment Canada (CSEC) were modified in terms of cyber incident management:
  - CSEC has created the Cyber Threat Evaluation Centre, which is the computer emergency response team for federal departments and agencies.
  - CCIRC is now the national computer emergency response team for provinces, territories and critical infrastructure sectors.

Proposed Mandate



BUILDING A **SAFE** AND **RESILIENT CANADA**

-FOR DISCUSSION ONLY

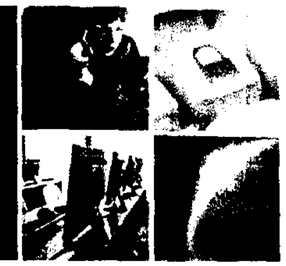
Proposed mandate

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

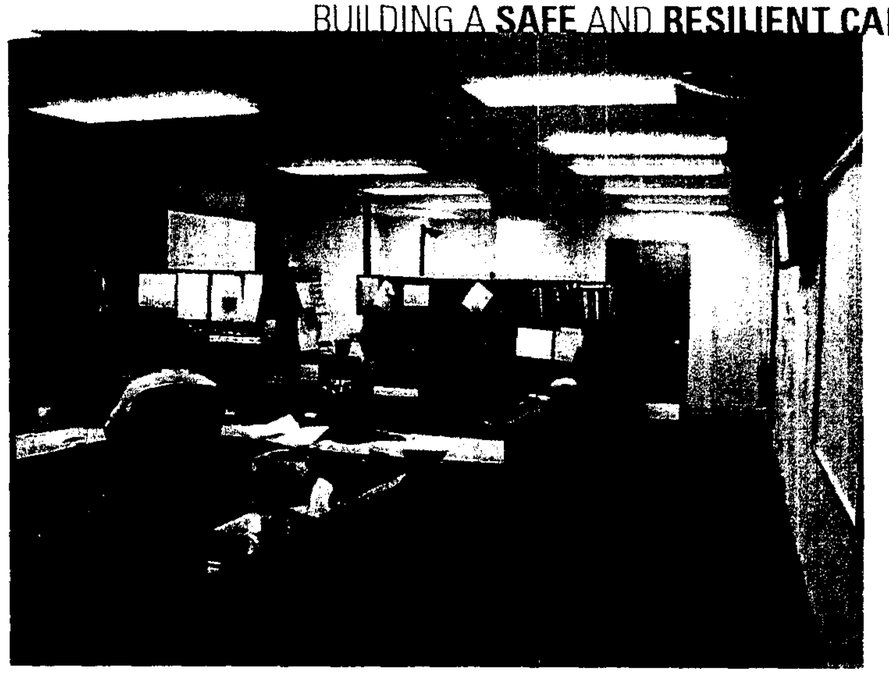
As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention, mitigation, and response to cyber events.

CCIRC provides authoritative advice to, and coordinates information sharing and event response among, all levels of government, international counterparts, critical infrastructure operators and information technology vendors.

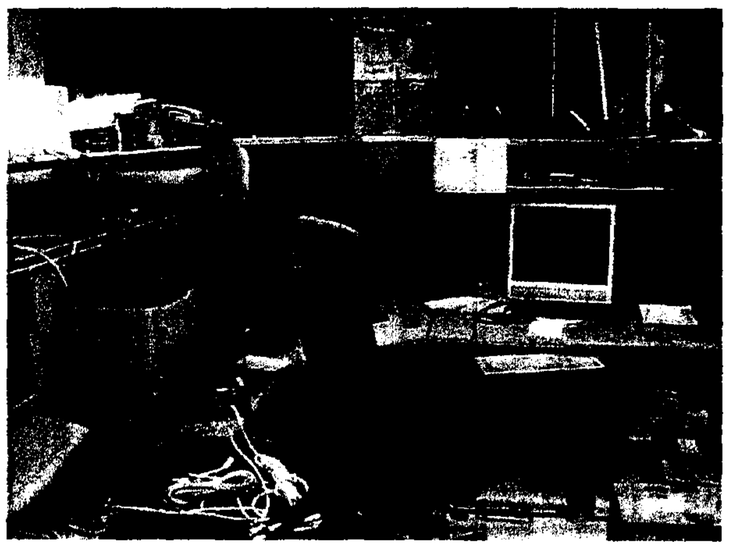
CCIRC – what it is



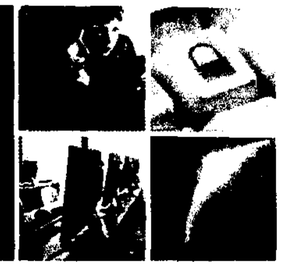
- Incident response centre
  - primary contact point into Government for domestic and international partners
  - CCIRC subject matter experts respond 9-5, 5 days a week
  - after hours coverage by Government Operations Centre



- Computer lab
  - isolated from corporate network for analyzing malicious software and testing solutions
  - industrial control system equipment for security testing and analysis in support of CI sectors

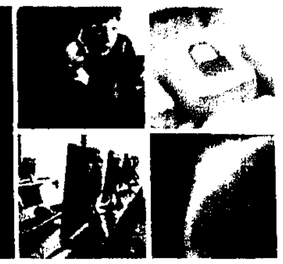


CCIRC – who it is



- 22 FTEs, 14 staffed
  - mainly highly specialized computer specialists (CS) with knowledge of IT security, computer forensics, and incident handling
  - 4 positions to be staffed for analysis of multi-source intelligence and technical data and writing strategic assessments
- Organized into three functions:
  - Incident Handling – assists partners in identifying, mitigating, and managing incidents
  - Technical Support – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis
  - Strategic Initiatives and Situational Awareness – builds and maintains operational relationships with partners, and produces strategic analysis products for decision makers

CCIRC – what it does



-These partners…

-Government S&I community

-Critical Infrastructure

-Provinces and territories

-Five Eyes and International CERTs

-Trusted vendors

-Academia

-Cyber security -expert community

-Open source

provide information to…

-CCIRC-

which provides these services:

~~Incident Handling and National Event~~ Coordination and Assistance

-- Direct technical assistance to partners and coordination of Government response to cyber events of national significance

-- Audience: technical staff in partner organizations responding to cyber incidents

-- Metric: 749 incidents responded to in 2011; 197 notifications to partners of compromised systems, 9 requests issued to shut down ~~malicious systems in Nov/Dec 2011~~

-Provision of Mitigation Advice

-- Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice

-- Audience: technical staff in partner organizations

-- Metric: 27 Cyber Flashes, 6 Alerts, 49 Advisories, and 13 Technical Notes in 2011

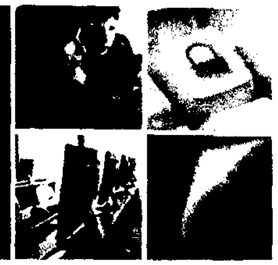
~~-Reporting and Analysis~~

-- Daily, weekly, monthly and annual reports providing summary, trend, and strategic analysis

-- Audience: technical staff, decision makers (under ~~development~~)

UNCLASSIFIED

CCAP: CCIRC Cyber Awareness Products



BUILDING A **SAFE** AND **RESILIENT CANADA**

-Currently Produced

-In Development

Product	CyberFlash	Daily Report	Weekly Technical Report	Information Notes	Technical Report	Advisory	Monthly Statistical Report	Weekly SA Report	Monthly SA Rollup	Issue of the Month	Annual Report	Ad hoc
Description	Time sensitive reports for immediate security issues ➢ Security fix unavailable	Daily situation report	Summary of daily reports, CCIRC products / events / activities / indicators / and cyber reporting	Report on significant cyber events ➢for general awareness	Detailed report WRT a cyber security issue ➢Ad hoc	Cyber security advisory on threat and vulnerability ➢ Security fix available	All CCAP products + (1) incidents handled ; (2) take down requests; and (3) victim notifications	Notable cyber events / CCIRC products / open source reports	Summary of weekly SA reports for ADM	Single strategic cyber issue analysis	Yearly status report WRT Canadian cyber security	Strategic cyber issue 1 pagers
Clients	P/T/CI operational contacts	CCIRC / trusted GoC partners	P/T/CI/GoC operational contacts	P/T/CI/GoC ➢Posted on website	P/T/CI operational contacts	P/T/CI operational contacts ➢Posted on website	Public Safety /other Federal departments	GoC managers / executives P/T/CI partners	Public Safety / Senior GoC executives	P/T/CI partners	Public	Public Safety

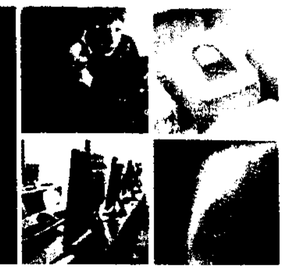
-Operational / Technical

-Strategic

Public Safety Canada | Sécurité publique Canada

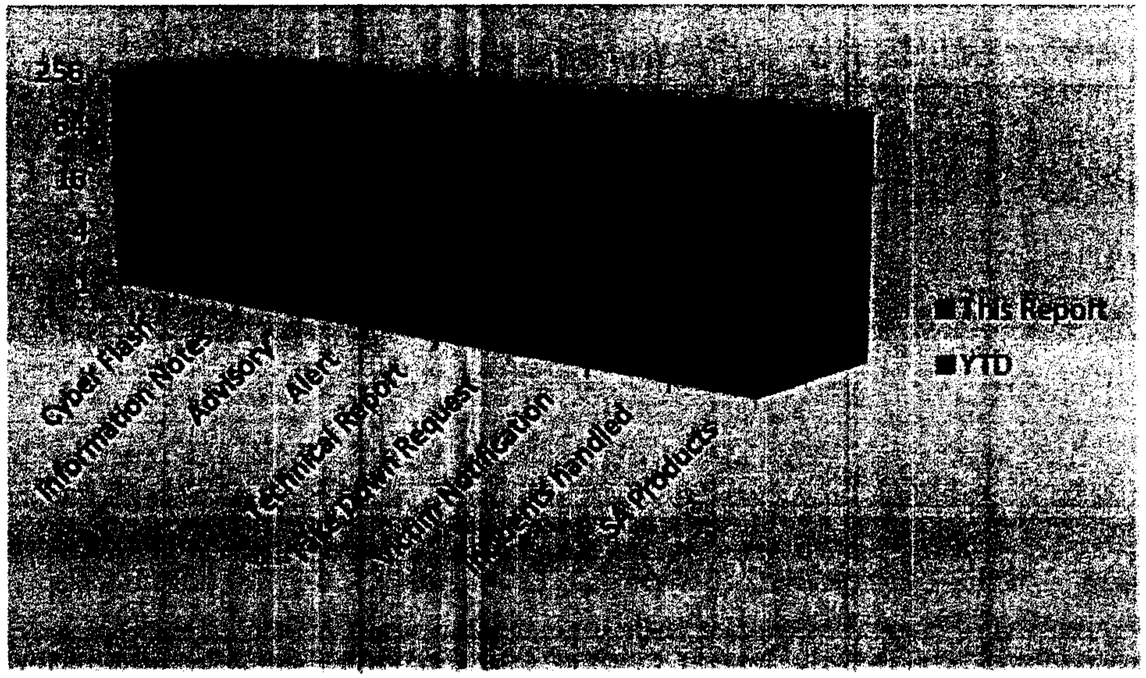
01167

CCIRC Activity Summary

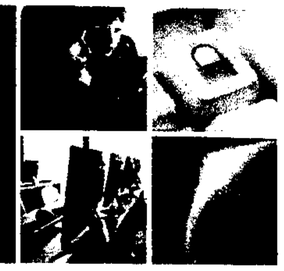


BUILDING A **SAFE** AND **RESILIENT CANADA**

CCIRC Activities -- January 16 - 22									
	Cyber Flash	Information Notes	Advisory	Alert	Technical Report	Take Down Request	Victim Notification	Incidents handled	SA Products
This Report	0	0	1	0	0	3	110	20	4
YTD	0	0	3	0	0	5	176	60	9

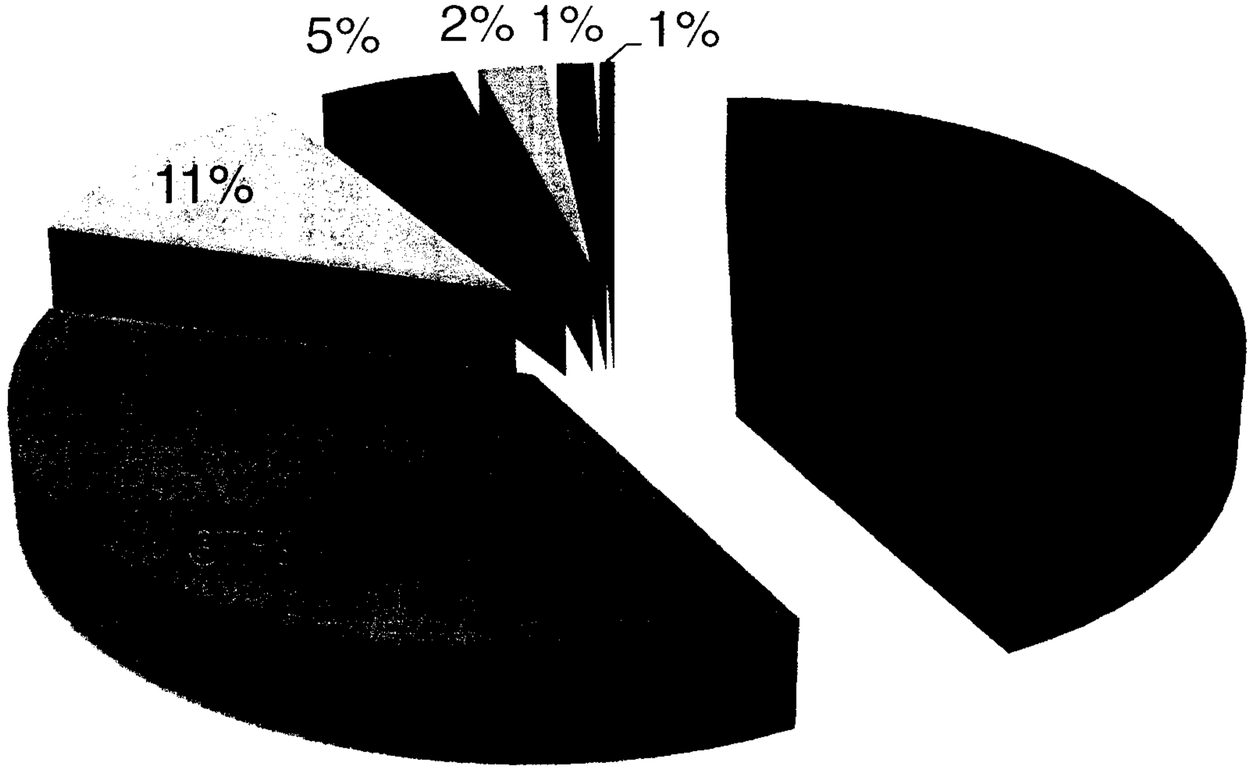


Stats



BUILDING A **SAFE** AND **RESILIENT CANADA**

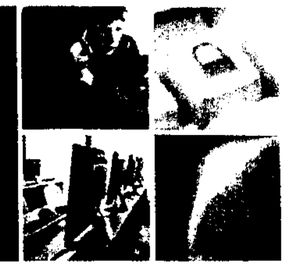
Events



- Cat 3 - MALICIOUS CODE / COMPROMISE
- Cat 7 - PHISHING / TARGETED EMAILS
- Cat 6 - INVESTIGATION / RESEARCH
- Cat 4 - IMPROPER USAGE / MISCONFIG
- Cat 1 - UNAUTHORIZED ACCESS / CREDENTIAL THEFT
- Cat 5 - SCANS/PROBES/ATTEMPTED ACCESS
- GridEx

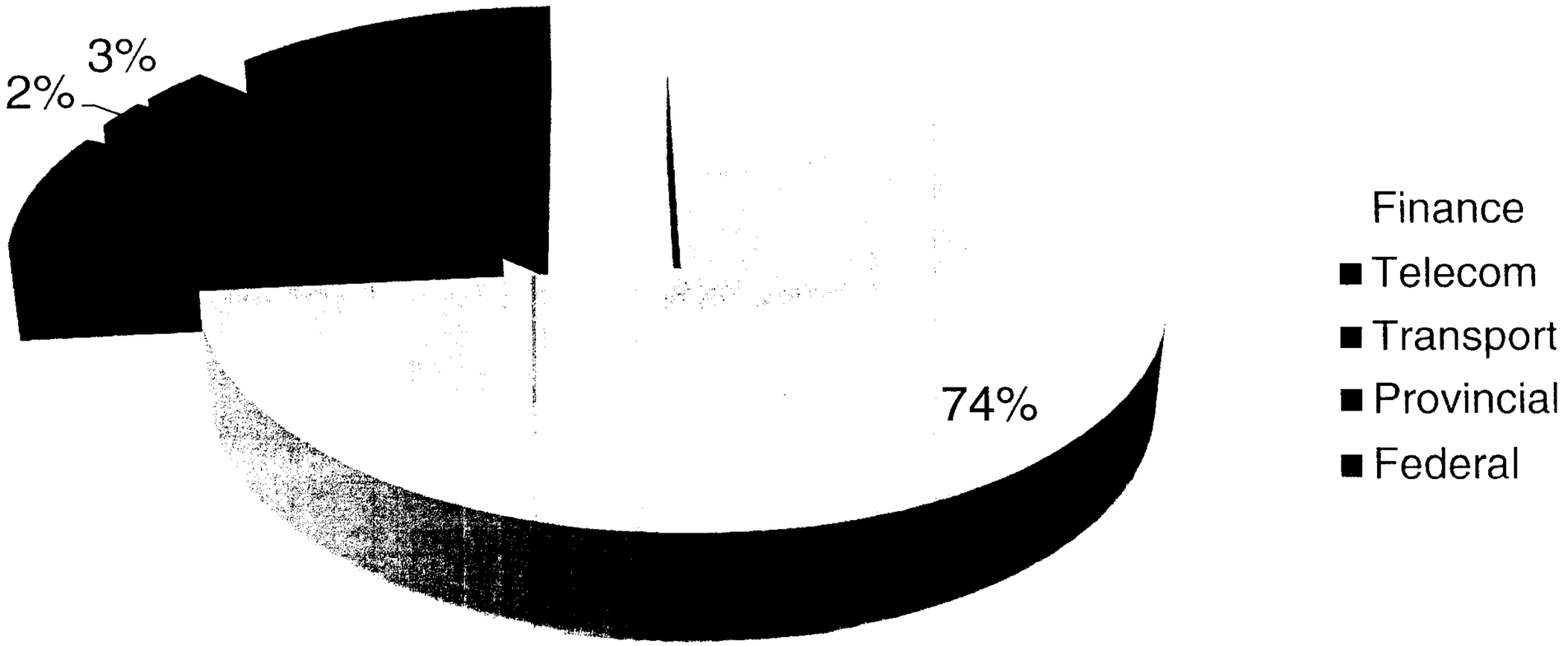
Public Safety Canada | Sécurité publique Canada

Phishing Reports



BUILDING A **SAFE** AND **RESILIENT CANADA**

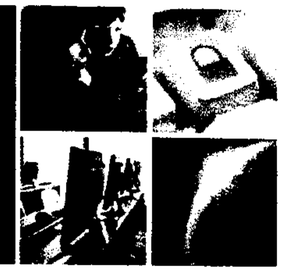
Phishing Reports to CCIRC
Jul 2011 - Jan 2012



Public Safety Canada | Sécurité publique Canada

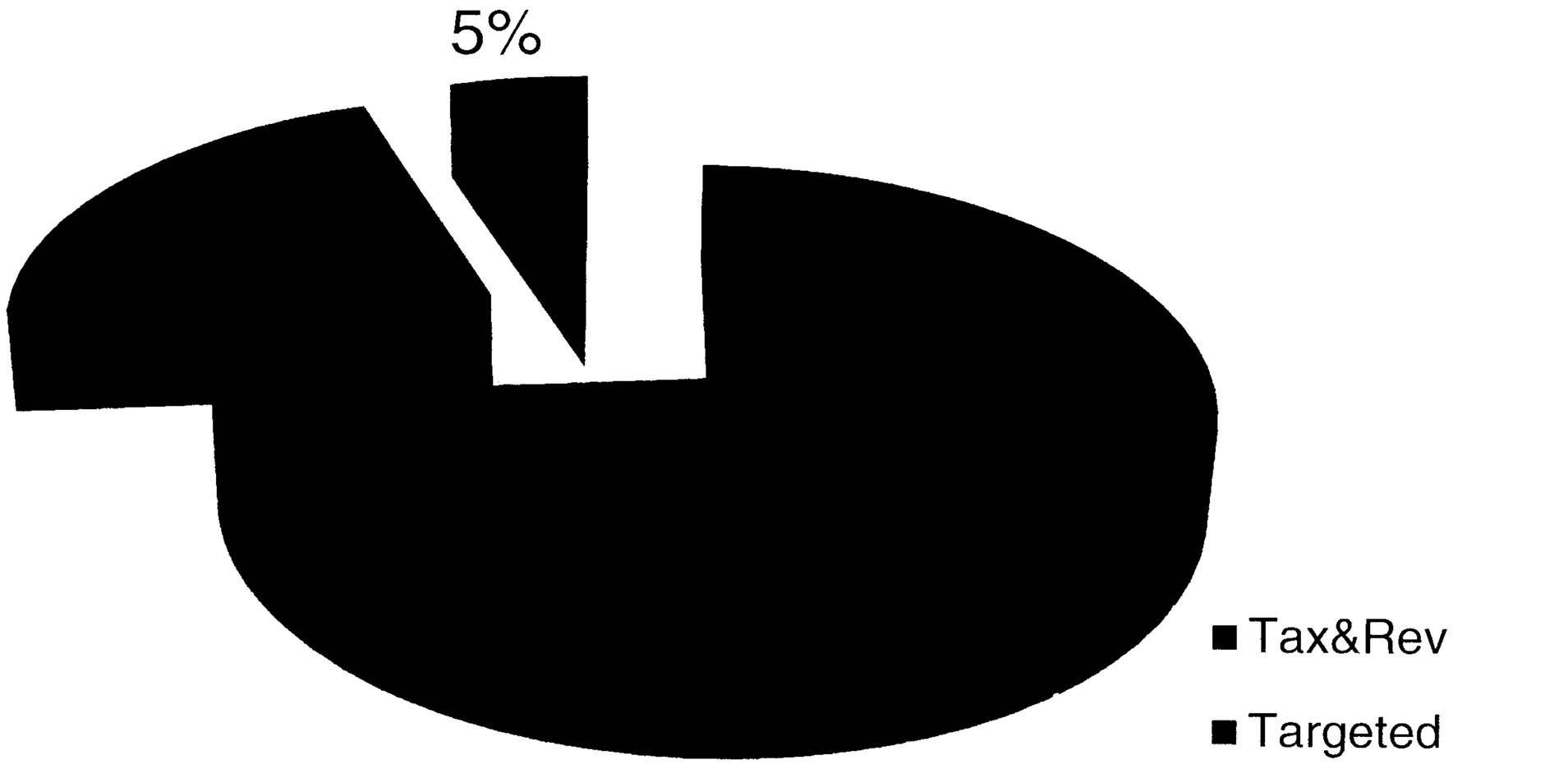
01170

Phishing Reports



BUILDING A **SAFE** AND **RESILIENT CANADA**

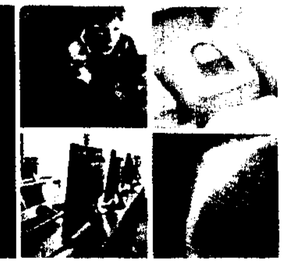
Federal



Public Safety Canada | Sécurité publique Canada

01171

Where CCIRC fits in *Canada's Cyber Security Strategy*



BUILDING A **SAFE** AND **RESILIENT CANADA**

-Securing Federal Government Systems

-Key actors:

- CSEC
- Shared Services
- TBS CIOB
- CF

-Partnering to Secure Vital Systems Outside the Federal Government

-Key actors:

- PS CCIRC, NCSD, CISCD
- CI Sector lead departments

-Existing effort:

- PT, select CI (telecom, energy, finance)
- U5 CERTs

-Future effort:

- trusted vendors
- international CERTs
- remaining CI sectors
- economic interests
- academia

-Helping Canadians to be Secure Online

-Key actors:

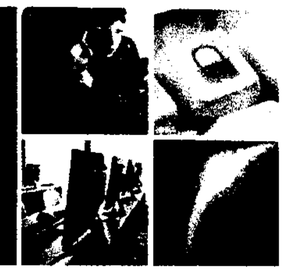
- PS Communications
- law enforcement
- Industry Canada
- CRTC
- Privacy Commissioner
- Competition Bureau

-Audiences:

- Home users
- Academia
- Small business

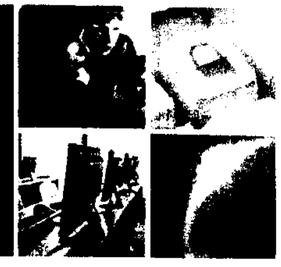
-State-sponsored cyber espionage ← ***-Risk*** → **-Crime**

Partnership Focal Areas



- Federal Government Partners
  - Security and Intelligence Leads
  - Industry Canada / Competition Bureau / Privacy Commissioner
- Provinces and Territories
- Critical Infrastructure
  - Canadian Electrical Association
  - Canadian Association of Petroleum Producers
  - Finance Sector
  - Telecommunications Sector
- International Partners
  - U5
  - International Watch and Warning Network (IWWN)
  - Forum for Incident Response and Security Teams (FIRST)

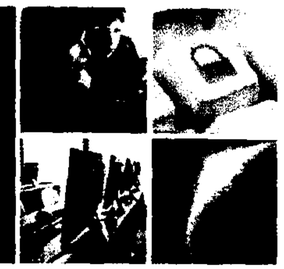
Current Initiatives



- [redacted] tools being reviewed
- [redacted] implementation in the next quarter
- Notification tool for email and CI sector IP range, domain and ASN matching implemented operationally
- SCADA/ICS simulation and VA tools being deployed
- Significant overhaul of lab infrastructure
- Partner Portal

s.16(2)(c)

CCIRC – US-CERT Cooperation



- **Assistance with malicious site Take-down in the US:**
  - Canada Revenue Agency Phishing
  - Targeted Email and associated infrastructure (hop host, etc)

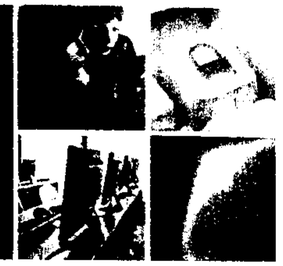
- **Sharing of threats and vulnerabilities:**

s.13(1)(a)
s.16(2)(c)

  -
  -
  - APT related indicators (ex: IP, URL, phishing email samples)
  - Hacktivist (ex: Anonymous during Tarmageddon)
  - Crimeware (ZeuS, BlackHole)
  - Pastebin information related to CAN/US : vulnerable systems, SCADA, accounts…

- **Industrial Control Systems**
  - Web exposed ICS devices notifications
  - Vulnerability coordination with SCADA Canadian companies

Contacting CCIRC



BUILDING A **SAFE** AND **RESILIENT CANADA**

Government Operations Centre

s.16(2)(c)

[redacted]

(request CYBERDO)

PGP: http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx

www.publicsafety.gc.ca/cyber

www.publicsafety.gc.ca/ci

Public Safety Canada | Sécurité publique Canada

Canada

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-008

For the Week of

3 Dec – 9 Dec 2011

Issued: 16 Dec 2011

HIGHLIGHTS:

Threat Warnings: Nothing significant to report.

CCIRC Products: CCIRC sent the following Cyber Flashes to stakeholders.

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
- CF11-026: Widespread SQL injection campaign
- CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

Incidents to report:

- Malicious e-mails from threat actors impersonating a Canadian federal agency, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems in the provincial government, financial, health, telecommunications and education sectors
- SQL injection attacks infected thousands of legitimate websites around the world, resulting in re-direction of internet users to a malicious websites. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

Noteworthy Open Source Reports:

- A draft US Bill in cyber security gets support from privacy proponents
- White House announces cloud security "rules of the road" for US federal agencies and contractors
- Hacker groups successfully attack websites of the Portuguese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

CCIRC PRODUCTS RELEASED THIS WEEK:

CCIRC sent three Cyber Flashes to key stakeholders – mainly IT professionals and managers in government, critical infrastructure and related sectors.

CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator. CCIRC has been receiving reports of various spear phishing campaigns that may be associated with Advanced Persistent Threat (APT) activity. This Cyber Flash highlighted the technical details of such recent attacks so stakeholders can check if they have been victimized. CCIRC also offered references for additional background information and mitigation advice.

CF11-026: Widespread SQL injection campaign. CCIRC received reports of a recent and broadly distributed SQL injection campaign. This world-wide attack campaign resulted in compromised websites redirecting unsuspecting site visitors to a malicious website, reportedly hosted in Moldova. It is estimated the campaign affected over 160,000 websites in the world, including Canadian ones. SQL injection attacks are a common and effective way to compromise legitimate but vulnerable websites in order to perpetrate malicious acts.

CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products. The purpose of this cyber flash is to raise awareness and offer mitigation for a number of unpatched vulnerabilities affecting versions of Adobe Reader, Adobe Acrobat and Adobe Flash products. CCIRC believes one of these vulnerabilities may have been leveraged in targeted attacks against the defence industrial sector.

NOTABLE INCIDENTS– 3 DECEMBER THROUGH 9 DECEMBER 2011:

Canadian Critical Infrastructure:

Federal Government. E-mails from threat actors impersonating a federal agency tried to entice internet users to a malicious website located in China. CCIRC notified its Chinese equivalent organization (China CERT) and recommended deactivation of the malicious website (still pending). CCIRC also reported the incident to Google as well as the Anti-Phishing Working Group (APWG).

Threat actors impersonating the same federal agency tried to entice internet users to a malicious website and tried to persuade them to reveal personal information (ex: name, social insurance and credit card numbers). The request was traced to a Romanian website hosted in the U.S. CCIRC

notified the internet service provider and informed US CERT (American equivalent of CCIRC). The malicious content had been removed from the website later that week.

- **Analysis:** CCIRC cooperates with computer incident or emergency response centres around the world, including US and China CERT. This type of incident for this agency occurs on a weekly basis. CCIRC works with the organization as well as the Canadian Antifraud Centre to have these malicious websites deactivated as quickly as possible.

Provincial Government. A provincial health organization was one of the victims of the wide-spread, world-wide, SQL injection attack described above for Cyber Flash CF11-026. The impact on the organization and the number of web-site visitors victimized is unknown. CCIRC notified the provincial government contacts and gave mitigation advice.

CCIRC also received infection reports for another provincial government's computer systems. Possible impacts can range from data theft to taking control of those computers to send SPAM. CCIRC notified the provincial contacts and gave mitigation advice. Impact on the organization is unknown.

- **Analysis:** These types of infections, commonly seen by CCIRC, could potentially lead to a compromise of that government's computer system. There is no information to suggest these were targeted attacks on that system.

Financial Sector. CCIRC received infection reports for a Canadian financial institution, which indicates potential computer compromises on the organization's network facing the internet. The impact on the organization and its clients is unknown. CCIRC notified the organization and offered mitigation advice.

- **Analysis:** The infections reported for this institution are commonly found on the internet, probably passed on from an on-line bank client who does not practice good cyber security. In CCIRC's experience, financial institutions pay keen attention to cyber security, because they are aware they are attractive targets to cyber criminals. Cyber security is understood to be a risk mitigation measure that will minimize a bank's financial losses and protect its reputation.

Telecommunications Sector. CCIRC received infection reports for two Canadian internet service providers and notified the organizations. These reports indicate there were likely compromises of computers belonging to internet users subscribing to those providers.

A large telecommunications service provider was one of the victims of the wide-spread, world-wide, SQL injection attack described earlier. This attack resulted in compromised websites redirecting unsuspecting site visitors to malicious websites. It is unknown how many client computers were compromised as a result of this malicious activity. CCIRC notified the service providers and gave mitigation advice. A Cyber Flash was also issued because of the estimated wide-spread impact.

Health. CCIRC received reports on potential compromises for a municipal Canadian health service provider and notified the organization. CCIRC does not have any information to indicate these compromises relate to a targeted attack.

Other Sectors:

CCIRC received reports on potential compromises for a Canadian university and notified the organization. A local real estate board was also the victim of the SQL injection attack described earlier in the report.

Noteworthy Open Source Reports:

A draft US Cyber security bill gets nod from privacy proponents. The House Homeland Security Subcommittee on Cyber security, Infrastructure Protection and Security Technologies held hearings on a draft cyber security bill. This bill proposes cyber-threat information sharing between the public and private sectors via a not-for-profit National Information Sharing Organization. This organization, would be led by DHS and consist of privacy advocates, representatives from critical infrastructure industry sectors, state and local government. The Center for Democracy and Technology, a US civil liberties group, publicly favours this draft bill over the other draft bill (H.R. 3523) because of its "superior information sharing stipulations".

Analysis: The House Intelligence Panel has already approved a competing draft cyber security bill that expands the pilot cyber threat information sharing program between the Defence Department and defence contractors. Privacy groups are concerned would this bill would allow Internet service providers to share private communications with the government. Of particular concern would be any customer data disclosure to the National Security Agency (NSA), who ran the pilot information sharing program.

US agencies and contractors get rules of the road for cloud security approvals. The White House announced that cloud providers to US federal agencies will have to comply with new uniform security requirements, by June 2012. US officials said agencies have shifted 40 IT services, such as email and collaboration software, to the cloud, in the past year. Seventy-nine more services have been identified for transfer to the cloud by June 2012. The newly announced Federal Risk and Authorization Management Program (FedRAMP), is expected to allow for more rapid and cost-effective deployment of cloud services for multiple US government agencies. Reports suggest an estimated $5 billion savings could result.

- **Analysis:** Cloud computing and securing data in a cloud is also a current topic of discussion in Canada. Though there are no specific official guidelines for cloud computing in the Canadian federal government, there are Treasury Board guidelines for outsourcing IT infrastructure and services.

- Cloud computing allows one to store and process one's data in an off-site computer system owned by a third party. This data can be accessible from almost any location. This feature, coupled with the proliferation of smart mobile devices, has brought cloud computing heightened attention. A recent survey by CSC, a US technology company, suggests that allowing employees mobile access to data, rather than saving money, was the reason for moving data to the cloud for many organizations.

Hacker groups successfully attack websites for the Portuguese Government, Columbian Army, Mexican Government and the PR firm for Monsanto. Open sources reported that Lulzsec Portugal, a self-proclaimed activist group, disabled the websites of **Portuguese government**, National Police, House of Parliament and several political parties. Reasons given for the attack were the Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest.

Anonymous, the famous international hacker group, successfully attacked the **Columbian Army**'s website. The motive given was to avenge a recently televised shooting of a seemingly harmless dog by soldiers. Anonymous also took down websites of numerous Mexican transportation and government websites, protesting the "dangerous travelling conditions present in Mexico".

Anonymous also executed a successful attack on a public relations firm working with Monsanto, as part of "Operation End Monsanto". The public relations firm, Bivings, reportedly had its website defaced and data stolen. Shortly after the incident, the firm liquidated their assets, and employees started a new public relations company. Monsanto is a large international producer of genetically engineered seeds and pesticides. It is the target of a number of activist groups and was named "Worst Company of 2011" by an environmental activist group.

- **Analysis:** Even though LulzSec was declared defunct in June 2011, affiliated hacker groups are still operating successfully around the world. Anonymous continues to target and successfully execute attacks around the world against vulnerable targets for activist purposes. Anonymous threatened to attack the Toronto Stock Exchange in support of the "Occupy" movement earlier this year. CCIRC is unaware of any incidents resulting from this threat.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

UNCLASSIFIED
DRAFT

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

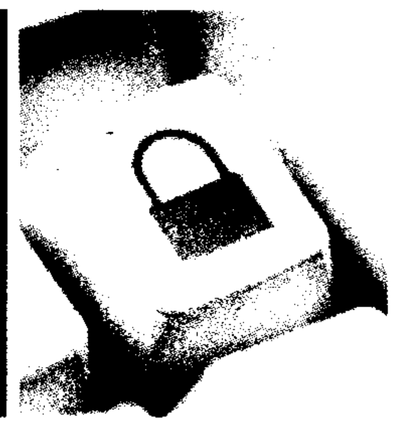
Public Safety Canada | Sécurité publique Canada

Canada

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-008



For the Week of

3 Dec – 9 Dec 2011

Issued: 16 Dec 2011

HIGHLIGHTS:

Threat Warnings: Nothing significant to report.

CCIRC Products: CCIRC sent the following Cyber Flashes to stakeholders.

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
- CF11-026: Widespread SQL injection campaign
- CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

Incidents to report:

- Malicious e-mails from threat actors impersonating a Canadian federal agency, enticing internet users to visit malicious websites and reveal personal information
- Potential compromises in computer systems in the provincial government, financial, health, telecommunications and education sectors
- SQL injection attacks infected thousands of legitimate websites around the world, resulting in re-direction of internet users to a malicious websites. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

Noteworthy Open Source Reports:

- A draft US Bill in cyber security gets support from privacy proponents
- White House announces cloud security "rules of the road" for US federal agencies and contractors
- Hacker groups successfully attack websites of the Portuguese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

CCIRC PRODUCTS RELEASED THIS WEEK:

CCIRC sent three Cyber Flashes to key stakeholders – mainly IT professionals and managers in government, critical infrastructure and related sectors.

CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator. CCIRC has been receiving reports of various spear phishing campaigns that may be associated with Advanced Persistent Threat (APT) activity. This Cyber Flash highlighted the technical details of such recent attacks so stakeholders can check if they have been victimized. CCIRC also offered references for additional background information and mitigation advice.

CF11-026: Widespread SQL injection campaign. CCIRC received reports of a recent and broadly distributed SQL injection campaign. This world-wide attack campaign resulted in compromised websites redirecting unsuspecting site visitors to a malicious website, reportedly hosted in Moldova. It is estimated the campaign affected over 160,000 websites in the world, including Canadian ones. SQL injection attacks are a common and effective way to compromise legitimate but vulnerable websites in order to perpetrate malicious acts.

CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products. The purpose of this cyber flash is to raise awareness and offer mitigation for a number of unpatched vulnerabilities affecting versions of Adobe Reader, Adobe Acrobat and Adobe Flash products. CCIRC believes one of these vulnerabilities may have been leveraged in targeted attacks against the defence industrial sector.

NOTABLE INCIDENTS– 3 DECEMBER THROUGH 9 DECEMBER 2011:

Canadian Critical Infrastructure:

Federal Government. E-mails from threat actors impersonating a federal agency tried to entice internet users to a malicious website located in China. CCIRC notified its Chinese equivalent organization (China CERT) and recommended deactivation of the malicious website (still pending). CCIRC also reported the incident to Google as well as the Anti-Phishing Working Group (APWG).

Threat actors impersonating the same federal agency tried to entice internet users to a malicious website and tried to persuade them to reveal personal information (ex: name, social insurance and credit card numbers). The request was traced to a Romanian website hosted in the U.S. CCIRC

notified the internet service provider and informed US CERT (American equivalent of CCIRC). The malicious content had been removed from the website later that week.

- **Analysis:** CCIRC cooperates with computer incident or emergency response centres around the world, including US and China CERT. This type of incident for this agency occurs on a weekly basis. CCIRC works with the organization as well as the Canadian Antifraud Centre to have these malicious websites deactivated as quickly as possible.

Provincial Government. A provincial health organization was one of the victims of the wide-spread, world-wide, SQL injection attack described above for Cyber Flash CF11-026. The impact on the organization and the number of web-site visitors victimized is unknown. CCIRC notified the provincial government contacts and gave mitigation advice.

CCIRC also received infection reports for another provincial government's computer systems. Possible impacts can range from data theft to taking control of those computers to send SPAM. CCIRC notified the provincial contacts and gave mitigation advice. Impact on the organization is unknown.

- **Analysis:** These types of infections, commonly seen by CCIRC, could potentially lead to a compromise of that government's computer system. There is no information to suggest these were targeted attacks on that system.

Financial Sector. CCIRC received infection reports for a Canadian financial institution, which indicates potential computer compromises on the organization's network facing the internet. The impact on the organization and its clients is unknown. CCIRC notified the organization and offered mitigation advice.

- **Analysis:** The infections reported for this institution are commonly found on the internet, probably passed on from an on-line bank client who does not practice good cyber security. In CCIRC's experience, financial institutions pay keen attention to cyber security, because they are aware they are attractive targets to cyber criminals. Cyber security is understood to be a risk mitigation measure that will minimize a bank's financial losses and protect its reputation.

Telecommunications Sector. CCIRC received infection reports for two Canadian internet service providers and notified the organizations. These reports indicate there were likely compromises of computers belonging to internet users subscribing to those providers.

A large telecommunications service provider was one of the victims of the wide-spread, world-wide, SQL injection attack described earlier. This attack resulted in compromised websites redirecting unsuspecting site visitors to malicious websites. It is unknown how many client computers were compromised as a result of this malicious activity. CCIRC notified the service providers and gave mitigation advice. A Cyber Flash was also issued because of the estimated wide-spread impact.

Health. CCIRC received reports on potential compromises for a municipal Canadian health service provider and notified the organization. CCIRC does not have any information to indicate these compromises relate to a targeted attack.

Other Sectors:

CCIRC received reports on potential compromises for a Canadian university and notified the organization. A local real estate board was also the victim of the SQL injection attack described earlier in the report.

Noteworthy Open Source Reports:

A draft US Cyber security bill gets nod from privacy proponents. The House Homeland Security Subcommittee on Cyber security, Infrastructure Protection and Security Technologies held hearings on a draft cyber security bill. This bill proposes cyber-threat information sharing between the public and private sectors via a not-for-profit National Information Sharing Organization. This organization, would be led by DHS and consist of privacy advocates, representatives from critical infrastructure industry sectors, state and local government. The Center for Democracy and Technology, a US civil liberties group, publicly favours this draft bill over the other draft bill (H.R. 3523) because of its "superior information sharing stipulations".

Analysis: The House Intelligence Panel has already approved a competing draft cyber security bill that expands the pilot cyber threat information sharing program between the Defence Department and defence contractors. Privacy groups are concerned would this bill would allow Internet service providers to share private communications with the government. Of particular concern would be any customer data disclosure to the National Security Agency (NSA), who ran the pilot information sharing program.

US agencies and contractors get rules of the road for cloud security approvals. The White House announced that cloud providers to US federal agencies will have to comply with new uniform security requirements, by June 2012. US officials said agencies have shifted 40 IT services, such as email and collaboration software, to the cloud, in the past year. Seventy-nine more services have been identified for transfer to the cloud by June 2012. The newly announced Federal Risk and Authorization Management Program (FedRAMP), is expected to allow for more rapid and cost-effective deployment of cloud services for multiple US government agencies. Reports suggest an estimated $5 billion savings could result.

- **Analysis:** Cloud computing and securing data in a cloud is also a current topic of discussion in Canada. Though there are no specific official guidelines for cloud computing in the Canadian federal government, there are Treasury Board guidelines for outsourcing IT infrastructure and services.

- Cloud computing allows one to store and process one's data in an off-site computer system owned by a third party. This data can be accessible from almost any location. This feature, coupled with the proliferation of smart mobile devices, has brought cloud computing heightened attention. A recent survey by CSC, a US technology company, suggests that allowing employees mobile access to data, rather than saving money, was the reason for moving data to the cloud for many organizations.

Hacker groups successfully attack websites for the Portuguese Government, Columbian Army, Mexican Government and the PR firm for Monsanto. Open sources reported that Lulzsec Portugal, a self-proclaimed activist group, disabled the websites of **Portuguese government**, National Police, House of Parliament and several political parties. Reasons given for the attack were the Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest.

Anonymous, the famous international hacker group, successfully attacked the **Columbian Army**'s website. The motive given was to avenge a recently televised shooting of a seemingly harmless dog by soldiers. Anonymous also took down websites of numerous Mexican transportation and government websites, protesting the "dangerous travelling conditions present in Mexico".

Anonymous also executed a successful attack on a public relations firm working with Monsanto, as part of "Operation End Monsanto". The public relations firm, Bivings, reportedly had its website defaced and data stolen. Shortly after the incident, the firm liquidated their assets, and employees started a new public relations company. Monsanto is a large international producer of genetically engineered seeds and pesticides. It is the target of a number of activist groups and was named "Worst Company of 2011" by an environmental activist group.

- **Analysis:** Even though LulzSec was declared defunct in June 2011, affiliated hacker groups are still operating successfully around the world. Anonymous continues to target and successfully execute attacks around the world against vulnerable targets for activist purposes. Anonymous threatened to attack the Toronto Stock Exchange in support of the "Occupy" movement earlier this year. CCIRC is unaware of any incidents resulting from this threat.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

UNCLASSIFIED
DRAFT

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Public Safety Canada | Sécurité publique Canada

Canada

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-008

For the Week of

3 Dec – 9 Dec 2011

Issued: 16 Dec 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released:** CCIRC sent the following Cyber Flashes to stakeholders.
  - CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator
  - CF11-026: Widespread SQL injection campaign
  - CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products

- **Incidents to report:**
  - Threat actors impersonating a Canadian federal agency enticing internet users to a malicious website and to reveal personal information
  - Potential **infections** in computer systems in the provincial government, financial, health, telecommunications and education sectors
  - SQL injection attacks, resulting in compromised websites re-directing site visitors to a malicious website. Website compromises seen include a Canadian provincial health organization, a large Canadian telecommunications service provider and a local real estate board.

- **Noteworthy Open Source Reports:**
  - A draft US Bill in Cyber security gets nod from privacy proponents
  - US agencies and contractors get rules of the road for cloud security approvals
  - Hacker groups' successful attacks against websites of the Portugese Government, the Columbian Army, the Mexican Government and the Monsanto PR firm Bivings Group.

Comment [DR1]: Or is it better to say "Infection reports" instead of "Potential infections"?

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

CCIRC PRODUCTS RELASED THIS WEEK:

CCIRC sent three Cyber Flashes to key stakeholders – mainly IT professionals and managers in government, critical infrastructure and related sectors.

CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT Indicator. CCIRC has been receiving reports of various spear phishing campaigns that may be associated with Advanced Persistent Threat (APT) activity. This Cyber Flash highlighted the technical details of such recent attacks so stakeholders can check if they have been victimized. CCIRC also offered references for additional background information and mitigation advice.

CF11-026: Widespread SQL injection campaign. CCIRC received reports of a recent and broadly distributed SQL injection campaign. This world-wide attack campaign resulted in compromised websites redirecting unsuspecting site visitors to a malicious website, reportedly hosted in Moldova. It is estimated the campaign affected over 160,000 websites in the world, including Canadian ones. SQL injection attacks are a common and effective way to compromise legitimate but vulnerable websites to perpetrate malicious acts.

CF11-027: Zero-Day Vulnerabilities in Adobe Reader, Adobe Acrobat and Adobe Flash Products. The purpose of this cyber flash is to raise awareness and offer mitigation for a number of unpatched vulnerabilities affecting versions of Adobe Reader, Adobe Acrobat and Adobe Flash products. CCIRC believes one of these vulnerabilities may have been leveraged in targeted attacks against the defence industrial sector.

NOTABLE INCIDENTS– 3 DECEMBER THROUGH 9 DECEMBER 2011:

Canadian Critical Infrastructure:

Federal Government. Threat actors impersonating a federal agency tried to entice internet users to a malicious website hosted in China. CCIRC notified its Chinese equivalent organization (China CERT) and recommended deactivation of the malicious website. CCIRC also reported the incident to Google as well as the Anti-Phishing Working Group (APWG).

- **Analysis:** CCIRC cooperates with computer incident or emergency response centres around the world, including China CERT. Cyber crime is also a concern in China, where internet

users are targeted quite heavily by criminals. A recently publicized incident was the defrauding of customers of a popular Chinese shopping website.

Threat actors impersonating the same federal agency tried to entice internet users to a malicious website and tried to persuade them to reveal personal information (ex: name, social insurance and credit card numbers). The request was traced to a Romanian website hosted in the U.S. CCIRC notified the internet service provider and informed US CERT (American equivalent of CCIRC). The malicious content had been removed from the website later that week.

Provincial Government. A provincial health organization was one of the victims of the wide-spread, world-wide, SQL injection attack described above. The impact on the organization and the number of web-site visitors victimized is unknown. CCIRC notified the provincial government contacts and gave mitigation advice. A Cyber Flash was also issued given the wide-spread compromise.

CCIRC also received infection reports for another provincial government's computer systems. CCIRC notified the provincial contacts and gave mitigation advice. Impact is unknown.

- **Analysis:** These types of infections, commonly seen by CCIRC, could potentially lead to a compromise of that government's computer system. There is no information to suggest these were targeted attacks on that system.

Financial Sector. CCIRC received infection reports for a Canadian financial institution and notified the organization.

Telecommunications Sector. CCIRC received infection reports for two Canadian internet service providers and notified the organizations.

A large telecommunications service provider was one of the victims of the wide-spread, world-wide, SQL injection attack described earlier. This attack resulted in compromised websites redirecting unsuspecting site visitors to malicious websites. It is unknown how many internet users' computers were compromised as a result of this malicious activity. CCIRC notified the service providers and gave mitigation advice. A Cyber Flash was also issued because of the estimated wide-spread impact.

Health. CCIRC received infection reports for a municipal Canadian health service provider and notified the organization.

Other Sectors:

CCIRC received infection reports for a Canadian university and notified the organization. A local real estate board was also the victim of the SQL injection attack described earlier in the report.

Noteworthy Open Source Reports:

A draft US Cyber security bill gets nod from privacy proponents. The House Homeland Security Subcommittee on Cyber security, Infrastructure Protection and Security Technologies held hearings on a draft cyber security bill. This bill proposes cyber-threat information sharing between the public and private sectors via a not-for-profit National Information Sharing Organization. This organization, it is suggested, would be led by DHS and consist of two privacy advocates, 10 representatives from critical infrastructure industry sectors, four federal officials as well as state and local government representatives. The Center for Democracy and Technology, a US civil liberties group, publicly favours this draft bill over the other draft bill (H.R. 3523) because of its "superior information sharing stipulations".

Analysis: The House Intelligence Panel has already approved a competing draft cyber security bill that expands the pilot cyber threat information sharing program between the Defence Department and defence contractors. Privacy groups are concerned would this bill would allow Internet service providers to share private communications with the government. Of particular concern would be any customer data disclosure to the National Security Agency (NSA), which is responsible for monitoring foreign communications and protecting U.S. information systems. NSA, a Defence Department Agency, ran the pilot information sharing program.

US agencies and contractors get rules of the road for cloud security approvals. The White House announced that cloud providers to US federal agencies will have to comply with new uniform security requirements, by June 2012. US officials said agencies have shifted 40 IT services, such as email and collaboration software, to the cloud, in the past year. Seventy-nine more services have been identified for transfer to the cloud by June 2012.

A new framework, to be administered by the new Federal Risk and Authorization Management Program (FedRAMP), establishes Federal policy for the protection of Federal information in cloud services, as well as operational roles and responsibilities for agencies. According to the announcement, this framework will allow for more rapid and cost-effective deployment of cloud services for multiple US government agencies. Reports suggest an estimated $5 billion savings could result.

- **Analysis:** Cloud computing and securing data in a cloud is also a current topic of discussion in Canada. Though there are no specific official guidelines for cloud computing in the Canadian federal government, there are Treasury Board guidelines for outsourcing IT infrastructure and services.

- Cloud computing allows one to store and process their data in an off-site computer system owned by a third party. This data can be accessible from almost any location. This feature, coupled with the proliferation of smart mobile devices, has brought cloud computing heightened attention. A recent survey by CSC, a US technology company, suggests that allowing employees mobile access to data, rather than saving money, was the reason for

moving data to the cloud for many organizations. More than half of the organizations surveyed said they saved little or no money after transitioning to cloud computing.

Hacker groups successfully attack websites for the Portuguese Government, Columbian Army, Mexican Government and the PR firm for Monsanto. Open sources reported that Lulzsec Portugal, a self-proclaimed activist group, disabled the websites of Portuguese government, National Police, House of Parliament and several political parties. Reasons given for the attack were the Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest.

Anonymous, the famous international hacker group, successfully attacked the Columbian Army's website. The motive given was to avenge a recently televised shooting of a seemingly harmless dog by soldiers. Anonymous also took down websites of numerous Mexican transportation and government websites, protesting the "dangerous travelling conditions present in Mexico".

Anonymous also executed a successful attack on a public relations firm working with Monsanto, as part of "Operation End Monsanto". The public relations firm, Bivings, reportedly had its website defaced and data stolen. Shortly after the incident, the firm liquidated their assets, and employees started a new public relations company. Monsanto is a large international producer of genetically engineered seeds and pesticides. It is the target of a number of activist groups and was named "Worst Company of 2011" by an environmental activist group.

- **Analysis:** Even though LulzSec was declared defunct in June 2011, affiliated hacker groups are still operating successfully around the world. Anonymous continues to target and successfully execute attacks around the world against vulnerable targets for activist purposes. Anonymous threatened to attack the Toronto Stock Exchange in support of the "Occupy" movement earlier this year. CCIRC is unaware of any incidents resulting from this threat.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

POTENTIAL HEADLINES FOR CCIRC WEEKLY SUMMARY – WEEK OF NOV 28 2011

The Potash related Cyber-hacking stories:

1. Item Description: **Foreign hackers targeted Canadian firms.** "A leading cyber-crime expert says foreign hackers who launched a massive attack on Canadian government computers last fall also broke into the data systems of prominent Bay Street law firms and other companies to get insider information on an attempted $38-billion corporate takeover. Daniel Tobok, whose international cyber-sleuthing company was called in by a number of the firms hit by the attacks, **says the hacking spree from computers in China were all connected to last year's ultimately unsuccessful takeover bid for Potash Corporation of Saskatchewan**. "All those different attacks on companies, law firms and government were all interconnected — they weren't isolated incidents," he said in an interview with CBC News. Tobok said hackers penetrated the computer systems of at least seven of Canada's leading law firms in what experts believe was an attempt to mask the real target of the attacks — the few firms directly involved in the aborted Potash deal. The foreign hack-attack on Canadian law firms was "very sophisticated and highly targeted," he said. The hackers appeared to have been hunting exclusively for information on the Potash deal, and there was no evidence they had penetrated the confidential files of other clients of the firms affected."
Reference: http://www.cbc.ca/news/canada/story/2011/11/29/pol-weston-hacking-firms.html

Saskatchewan also targeted by hackers during Potash bid
Hackers targeted Saskatchewan government computers during the multibillion-dollar takeover bid of Potash Corp. of Saskatchewan, says the head of information technology for the province. The provincial Information Technology Office said Thursday that an unsuccessful attack was made on government computers during BHP Billiton's takeover bid of Potash Corp. last year. Calgary Herald, D7

*** Chinese cyber spies sought Potash deal secrets**
Hackers linked to computers in China engaged in cyber attacks on major Bay Street law firms, financial institutions and public-relations agencies in an apparent effort to seek inside information on last year's abortive takeover of Potash Corp. of Saskatchewan, a security consultant says. Globe and Mail, B3; StarPhoenix

---

4. Item Description: **Targeted attacks steal credit cards from hospitality and educational institutions.** "A little more than a week ago SophosLabs became aware of a resurgence of an attack against the education and hospitality industries. In at least one case the malware has shown up at a financial services company. One thing important to note is that it has only been seen at moderate to small size organizations. These criminals aren't targeting Walmart. They are after organizations with less investment in defensive counter-measures. The goal of this Trojan is to target credit card processing and point of sale (PoS) equipment and make off with all of the card details. It installs itself as a service in Windows and the filename is typically rdasrv.exe, while the service is called rdasrv. More recent samples have changed their name to be A########.exe, where the # is a random number."
Reference: http://nakedsecurity.sophos.com/2011/11/30/targeted-attacks-steal-credit-cards-from-hospitality-and-educational-institutions/

Spoof Health Canada Email Offers Shovelling Credit
Some journalists were left scratching their heads Monday after a fake government press release promising snow shovelling tax credits for seniors hit their inboxes. The spoof release was quickly revealed as a fake by a phone call to the office of Health Minister Leona Aglukkaq. The phony

emailed news release said the government would provide fitness tax credits for seniors shovelling snow if they submitted photos as evidence. The email appeared to come from Health Canada's media relations email address, but instead came from a variation on the address. Huffington Post

(MAYBE FOR AN ISSUE PAPER RE CERTIFICATE AUTHORITIES?) 1. Item Description **Google researchers propose fix for ailing SSL system.** "Security researchers from Google proposed an overhaul to improve the security of the Secure Sockets Layer encryption protocol that millions of Web sites use to protect communications against eavesdropping and counterfeiting. The changes are designed to fix a structural flaw that allows any one of the more than 600 bodies authorized to issue valid digital certificates to generate a Web site credential without the permission of the underlying domain name holder. The consequences of fraudulently issued certificates was underscored in late August when hackers pierced the defenses of Netherlands-based DigiNotar and minted bogus certificates for Google and other high-profile Web sites. One of the fraudulent credentials, for Google mail, was used to snoop on as many as 300,000 users, most of them from Iran. Under changes proposed November 29 by Google security researchers, all certificate authorities would be required to publish the cryptographic details of every Web site certificate to a publicly accessible log that has been cryptographically signed to guarantee its accuracy. The overhaul, they said, is designed to make it impossible –- or at least much more difficult –- for certificates to be issued without the knowledge of the domain name holder."
Reference: http://www.theregister.co.uk/2011/11/29/google_proposes_ssl_fix/

NOTE: THERE WAS ALREADY AN EMAIL EXCHANGE IN OUR DEPT AMONG SENIOR MANAGERS ON THIS ONE –
3. Item Description: **Carrier IQ snoops on US cell users - Spyware or service monitoring tool?.** "Last week a very scary piece of research was published by Trevor Eckhart about spyware that is being included on cellular phones in the United States. The commercial software application is called Carrier IQ and is reportedly being used by Verizon, Sprint and potentially other carriers. Carrier IQ was unhappy with Eckhart publishing public copies of their training materials and proceeded to send a cease and desist letter to Mr. Eckhart. Fortunately Eckhart worked with the EFF to explain things to Carrier IQ and their CEO responded with an apology promising to work with the EFF and Eckhart. Eckhart analyzed the software that was running on his Android-based HTC phone (Carrier IQ also supports Blackberry, Nokia and others) and discovered it was doing some rather sneaky things. It was installed in such a manner as to be largely invisible, it was logging his location even when he had location services disabled and keeping track of every key press and URL he visited (including HTTPS urls). The software ignored the "Force stop" button and was nearly impossible to remove from the device for non-Android hackers."
Reference: http://nakedsecurity.sophos.com/2011/12/01/carrier-iq-snoops-on-us-cell-users-spyware-or-service-monitoring-tool/

ok, not redacted

After consultation with IC and other intelligence partners, CCIRC has advised the following:

- CarrierIQ is essentially a tool that provides mobile service providers the ability of monitor and troubleshoot wireless network issues. It is installed at the smartphone operating system level with a high level of privilege.
- The carrier who purchases CarrierIQ will determine what information is collected and where to send it, and must do so within the legislative and regulatory framework of the jurisdiction(s) in which it is operating. In Canada, this would include privacy regulation falling under Industry Canada.
- CTEC has confirmed CarrierIQ is installed on some iPhones, and on Android phones by carrier request. However, Rogers and Telus announced they do not have it on their

phones, RIM and Nokia do not install it, and we confirmed via IC that neither does Bell. Based on the response from Canadian wireless suppliers the impact Canadians appears to be low.

- In the US, AT&T and Sprint use it but Verizon does not. In the UK, Vodaphone, Orange and O2 stated they do not have it installed.
- We have no information to indicated this software is vulnerable to tampering by hackers.
- The general consensus is that this is not a technology issue. However, it may have an impact from the point of view of consumer protection and privacy.

While at the strategic level, and through public awareness and education activities underway, PS collaborates with the Office of the Privacy Commissioner to align messages and show how attaining cyber security objectives aligns with achieving greater individual control over personal information, the operational focus of CCIRC is directed at "securing vital systems outside the Government of Canada", and with our limited resources, at key systems within a few critical infrastructure sectors. As such, areas such as this are ones that Industry Canada would normally address should it decide to do so as the regulator of telecoms.

Anonymous launches new operation targeting big banks (OpRobinHood: teaming up with Team Poison)

2. Item Description: **Anonymous launches new operation targeting big banks.**
"Hacktivist collective Anonymous and hacking group Teamp0ison have announced that they will be joining their forces once again and starting another operation against banks. They call it OpRobinHood, and apparently it will consist of stealing credit card details from big banks in order to use it to make donations to charities and others. "In regards to the recent demonstrations and protests across the globe, we are going to turn the tables on the banks," they state. "Operation Robin Hood is going to return the money to those who have been cheated by our system and most importantly to those hurt by our banks. Operation Robin Hood will take credit cards and donate to the 99% as well as various charities around the globe. The banks will be forced to reimburse the people there money back." The operation is meant to damage the banks' financial standing as well as their reputation, and as such it should continue the work initiated by the Operation Cash Back, with which bank users were urged to close their accounts and transfer the money to accounts opened with credit unions. "Operation Robin Hood urges YOU, to now move your accounts into secure credit unions, before it's too late while we hit them from the inside," they say, but don't reveal whether the stolen information will be used by them or made public for the "99%" to use. Allegedly, Chase, Bank of America, and CitiBank have already been hit with big breaches, and credit cards issued by them have been used to make donations."
Reference: http://www.net-security.org/secworld.php?id=12024
http://www.itworld.com/security/229141/team-poison-anonymous-campaigners-claim-first-victims-oprobinhood

5. Item Description: **First National Bank of Long Island, Operation Robin Hood Victim**.
"In order to prove me wrong and to show theyre still able to pull off a hacking operation, the hacktivists behind Operation Robin Hood revealed the vulnerabilities present in the website of the First National Bank of Long Island. I wanna say, that, we TeaMp0isoN pulled off any project we started, sooner or later of course. As i am not defacer or fame hunting kid/skid, Ill just prove that banks are secure and can(WILL) be hacked, wrote the hackers in response to my article. By making use of an SQL injection flaw, members of the newly formed alliance, p0isAnon, injected a piece of arbitrary code into the website. To prove the attack concept, they posted a link that clearly shows the vulnerability really exists."

Reference: http://news.softpedia.com/news/First-National-Bank-of-Long-Island-Operation-Robin-Hood-Victim-237131.shtml?utm_source=twitter?utm_source=twitter&utm_medium=twitter&utm_campaign=twitter_web

---

Complete item: http://ffiec.bankinfosecurity.com/articles.php?art_id=4295&pg=1

Description:
The Federal Bureau of Investigation has issued a warning about a new Zeus malware attack targeting commercial bank accounts, ultimately leading to incidents of corporate account takeover. The Zeus variant used: a malware called Gameover, which the FBI says is able to defeat several forms of dual-factor authentication.

To protect themselves, the FBI suggests consumers and businesses pay attention to suspicious e-mails. In the case of the Gameover attacks, e-mails purporting to come from NACHA-The Electronic Payments Association contained malicious links. NACHA does not traditionally send e-mails directly to businesses or consumers. Receipt of a direct e-mail from an organization such as NACHA should raise a red flag.

But according to the FBI's Denver Cyber Squad, it's not just phishy e-emails and dual-factor get-arounds that have made the Gameover attacks forces to be reckoned with. As it turns out, the fraudsters behind this scheme combined a number of tactics, including the use of money mules and denial of service attacks, to con businesses and banks out of funds.

"After the accounts are compromised, the perpetrators conduct a distributed denial of service (DDos) attack on the financial institution," the FBI states. "The belief is the DDoS is used to deflect attention from the wire transfers, as well to make them unable to reverse the transactions."

Over the past two weeks, since the Gameover scheme was discovered, the FBI has tracked fraudulent wire transfers routed to high-end jewelry stores. And here is where the scheme takes its twist. Money mules, which've been hired to visit these stores, where funds have been fraudulently transferred, go to pick up jewels worth the amount of the fake wire.

"A money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as pending and releases the merchandise to the mule," the FBI states. "Later on, the transaction is reversed or cancelled ... and the jeweler is out whatever jewels the money mule was able to obtain."

Connecting the Dots
Fraudsters' ingenuity in the Gameover scheme is concerning.

"We've gotten fairly good at the Red Flag rules and detecting money mules, so the attackers are now figuring out they need to stall for time to get the cash," says Mike Smith, an online security expert with Akamai Technologies.

To do that, fraudsters are launching DDoS attacks against the banking institutions, just to distract them long enough to get the money and run.

"These attacks kill the interface that the customers are used to seeing, as well as the interface the banks use, like the APIs they use to do their transfers between each other," Smith says.

Cybercriminals have figured out how to connect the dots. They are committing cross-channel fraud.

The scam relies on traditional phishing and spear-phishing tactics to get in the door. Spear-phishing e-mails are sent to executives, who oftentimes are identified via social networking channels like LinkedIn and corporate databases. Additionally, the fraudsters send massive phishing e-mails to every employee in an organization, just waiting for one with access to the corporate online banking account to click a link.

Once the malware is launched, the fraudsters can monitor keystrokes and the online bank sites those infected PCs visit.

But it's the DDoS and money mule additions that bring the fraud full circle.

"You usually see one of three things in a DDoS attack," Smith says:

A protection racket scam, which involves an attack against an ecommerce site that blackmails the site into paying a few to stop the attack;

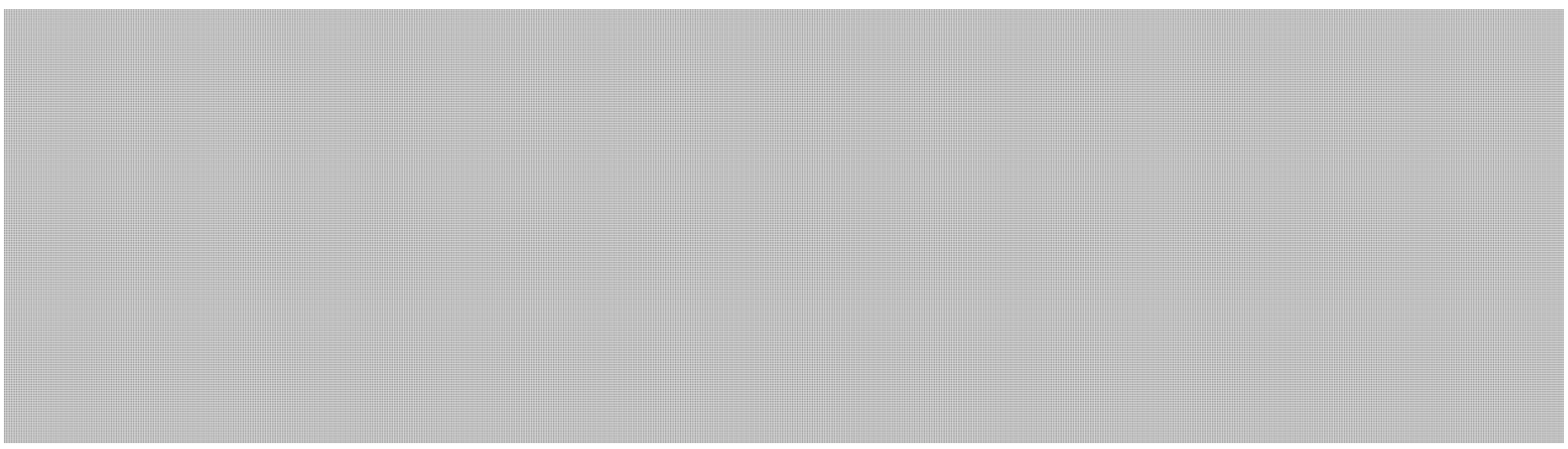
An activist threat, like the ones the industry has seen waged by groups such as Anonymous against entities for social reasons;

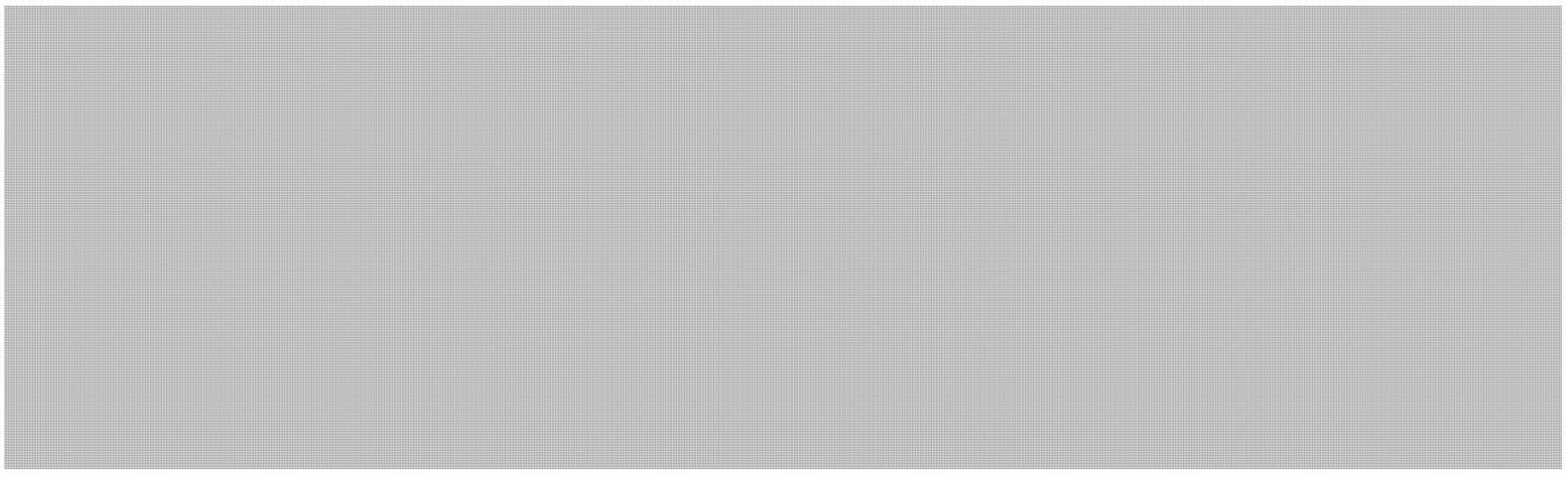
A political threat, which could be waged against a corporation or country by a nation state.

"This is an entirely different scenario," Smith says. "What you're seeing is that the attack is designed to slow down the businesses being defrauded and slow down the bank's response."

Dave Jevans of the Anti-Phishing Working Group says financial institutions have two theories about the reasoning behind the attacks: to shut down access and distract bank security and IT. For large institutions, the attacks likely only serve as distractions.

E-Secure-IT
https://www.e-secure-it.com





Update: Ill. pump failure wasn't cyberattack from Russia

Mystery solved. A reported cyberattack on a water district in central Illinois turned out to be a false alarm set off when an American contractor logged onto the system remotely while vacationing in Russia.

Lessons from the 'water plant hack' that never happened
Two weeks ago, the Internet was abuzz with news of a network intrusion into a utility's operation and control system that caused months of glitches and the eventual failure of a water pump. Details of the alleged intrusion came from a leaked alert issued earlier in November by Illinois's fusion center, the Illinois Statewide Terrorism and Intelligence Center that is supported by the U.S. Department of Homeland Security. The alert suggested that an intrusion from a Russian Internet address was to blame. InfoWorld

---

Obama Fortifies Efforts To Protect Critical Infrastructure (USE IN THE ANALYSIS FOR STORY ABOVE)
Deeming December "Critical Infrastructure Protection Month", President Obama has called on the feds to "reflect on" their responsibility to keep U.S. electricity, financial networks, and other critical control facilities safe from cyber threats. Information Week

Cybersecurity bill approved by U.S. House panel
A bill to let U.S. spy agencies share intelligence on cyber threats with private companies was backed by a House of Representatives intelligence panel on Thursday. In a 17-1 vote, the Permanent Select Committee on Intelligence approved the legislation that would expand a pilot Pentagon program for sharing classified and sensitive threat information with defense contractors and their Internet service providers. Reuters

The bill is narrower than Senate proposals, which favor more sweeping cybersecurity regulations. House Republicans have largely steered away from significant government regulations or mandates on industry, instead favoring cybersecurity incentives for private firms to boost their own security and share information……..The bill already has support from industry. IBM's vice president of government relations, Christopher Padilla, said that the legislation "provides a solid framework and useful legal protections to permit the timely flow of actionable threat information in order for organizations to better protect themselves and customers."
http://www.nextgov.com/nextgov/ng_20111130_2019.php?oref=rss?zone=NGtoday

---

New Android malware targets Canadians (NOTE: Not sure if this affects CCIRC stakeholders, but it would affect Android users in Canada – should it be in or out?)
Hackers are targeting Canadian smartphones running Google Inc.'s Android platform to send costly text messages to paid services against their will. Discovered by security software firm Kaspersky Lab late last week and first reported by ITbusiness.ca early Tuesday morning, the new trojan — which refers to malicious software (malware) disguised as a harmless update — forces Android phones to send text messages (read: SMS messages) to expensive pay-per-message services. The attackers are then able to collect the fees generated by those messaging services. Financial Post

Report Says Android Market Is Number One Source of Mobile Malware
Android should be proud of its dominate market share, which climbed up to 33% after only four years in the business. With that much success, it's no surprise that the popular operating system has become the number one target of malware, according to a report from McAfee senior architect Igor Muttik. TIME

Hackers 'jailbreak' RIM's PlayBook
Software developers say they have hacked into Research In Motion's PlayBook tablet computer, controlling the device's file system and allowing the PlayBook to run unauthorized applications. The PlayBook, which in July became the first tablet to win U.S. government security clearance, is viewed as less vulnerable to hacking than devices running on open-source software platforms, notably Google's Android OS. The Record, C8; Globe and Mail; Montreal Gazette

'Jailbreak' of PlayBook no emergency
An opinion piece states, "A group of U.S.-based computer hackers claim to have found a vulnerability within Research In Motion Ltd.'s BlackBerry PlayBook that allows the tablet computer to be "jail-broken," giving users the ability to access and alter core features of the device. The announcement set off alarm bells in the technology world, prompting some observers to fret that the jailbreak had dealt a damaging blow to RIM's reputation for iron clad mobile security…"
National Post, FP14

For the UN Website Hacking Event #2490 - use in the analysis:

TeaMp0isoN's list also included some user accounts at the World Food Program, UNESCO -- U.N. Educational, Scientific and Cultural Organization, UNICEF, U.N. Population Fund, and World Health Organization.

A few individuals with email addresses at the World Bank, which is not part of the U.N., were targeted as well.

http://www.nextgov.com/nextgov/ng_20111129_4678.php?oref=rss?zone=NGpopular

Hackers break into old UN server
The United Nations on Wednesday said that hackers broke in to an old server and swiped outdated account and password information. Windsor Star, C2

Obama Uses Cold-War Powers to Unmask Spyware
The U.S. is invoking Cold War-era national-security powers to force telecommunication companies including AT&T Inc. and Verizon Communications Inc. (VZ) to divulge confidential information about their networks in a hunt for Chinese cyber-spying. Bloomberg

U.S. Cyber Command Practices Defense In Mock Attack
The military command in charge of U.S. cyber-warfare activities has successfully completed its first major exercise in its mission to protect the Department of Defense (DOD) from cyber attacks. The U.S. Cyber Command performed the exercise, called Cyber Flag, over a week's time at the Air Force Red Flag Facility at Nellis Air Force Base in Nevada, and through a virtual environment pulled in participants from other locations, according to a press statement. InformationWeek

Lawmakers pad FBI cyber schooling funds

Congress will pay the FBI an additional $18.6 million to better investigate computer hacking cases, following a federal study that found a third of bureau agents probing breaches significant to national security lacked the necessary networking and counterintelligence skills. http://www.nextgov.com/nextgov/ng_20111122_7398.php?oref=rss?zone=NGtoday

CYBER SECURITY / CYBERSÉCURITÉ

1. Canadian businesses unprepared for hackers

Canadian businesses are increasingly being victimized by hackers but are also less prepared for such Internet threats, new reports have found. Breaches of Canadian publicly traded companies jumped an "alarming" 50% in 2011, says a **joint study released Tuesday by Telus Corp. and the University of Toronto's Rotman School of Management**. The annual study said public companies in Canada were hacked an average of 18 times this year, compared with an average of 12 attacks suffered in 2010. Overall, the study says, attacks on businesses and government offices were down nearly 50% from last year, to an average of 7.6 breaches in 2011 from 14.6 in 2010. Insider breaches, in which hackers turned out to be employees, were extremely prevalent in government - the "most startling" result of the survey, researchers said - accounting for 42% of every government computer hacked in 2011. National Post, FP4 (Times Colonist, The Province, Calgary Herald, Montreal Gazette)

Here's a link to an article that appeared today at Globe and Mail online, titled "Hackers target Canada, 'insider' data theft spikes in public
sector: report":
http://www.theglobeandmail.com/news/technology/tech-news/hackers-target-canada-insider-data-theft-spikes-in-public-sector-report/article2236729/

2. U.S. probes cyber attack on water system

Federal investigators are looking into a report that hackers managed to remotely shut down a utility's water pump in central Illinois last week, in what could be the first known foreign cyber attack on a U.S. industrial system. Kingston Whig-Standard, 44 (Ottawa Citizen, Montreal Gazette, Windsor Star, Calgary Herald, Calgary Sun)

Water utility hackers destroy pump, expert says. "Hackers destroyed a pump used by a US water utility after gaining unauthorized access to the industrial control system it used to operate its machinery, a computer security expert said. Joe Weiss, a managing partner for Applied Control Solutions, said the breach was most likely performed after the attackers hacked into the maker of the supervisory control and data acquisition software used by the utility and stole user names and passwords belonging to the manufacturer's customers. The unknown attackers used IP addresses that originated in Russia. Weiss cited an official government report from the state where the regional water district was located. It was dated November 10, two days after the hack was discovered. The document indicates that the utility had been experiencing unexplained problems with its computerized system in the weeks leading up to the breach."
Reference: http://www.theregister.co.uk/2011/11/17/water_utility_hacked/
http://community.controlglobal.com/content/water-system-hack-%E2%80%93-system-broken

Hackers Attacked U.S. Water Utility; Destroyed Pump
Hackers gained remote access into the control system of the city water utility in Springfield, Illinois, last week and destroyed a pump, according to a report released by a state fusion center and obtained by a security expert. The hackers were discovered on Nov. 8 when a water district employee noticed problems in the city's Supervisory Control and Data Acquisition System (SCADA). The system kept turning on and off, resulting in the burnout of a water pump. Wired

3. City on high alert for hackers after threat

In response to a hacking threat, City of Toronto employees are being urged to closely watch web pages for unusual activity and also report any weird phone calls, emails or other "odd occurrences." Toronto Star, GT2

Website snafu strictly 'routine'
"Routine maintenance" -- not Anonymous -- knocked Mayor Rob Ford briefly off the Internet Wednesday. But the Sun has learned Toronto Police are investigating a threat that Anonymous, a group of hacker activists, allegedly made against Ford and the city. Toronto Sun, 5; Toronto Star

4. Defence and energy sites hacked in Norway
The biggest wave of hacking and espionage attacks in Norway's history has hit key defence and energy companies among its targets, the National Security Agency said Friday. Windsor Star, A15

Item Description: **Phishers net Norwegian secrets**. "Oil, gas and defense data has been boosted from computers in Norway, in what the country fears is its largest-ever data espionage case. Details are still slim, but according to *AP*, phishing e-mails were sent with viruses designed to "sweep entire hard drives for data". Norway's National Security Authority, NSM, which coordinates the country's CERT activities, says attackers have sent industrial secrets from the targeted companies out of the country. It's not the first time Norway has suffered serious breaches of security. In March, shortly after its F-16s were involved in air strikes on Libya, a data-stealing trojan was e-mailed to military employees."
Reference: http://www.theregister.co.uk/2011/11/17/noway_data_theft_attack/

Norway Cyberattack: Country Hit By Major Data Theft
Data from Norway's oil and defense industries may have been stolen in what is feared to be one of the most extensive data espionage cases in the country's history, security officials said Thursday. Industrial secrets from companies were stolen and "sent out digitally from the country," the Norwegian National Security Authority said, though it did not name any companies or institutions that were targeted. Huffington Post

5. Une firme informatique montréalaise critiquée
Une firme d'informatique de Montréal dont la Caisse de dépôt et placement est l'un des principaux actionnaires est sur la sellette pour son hébergement de sites internet liés au gouvernement de la Syrie et à sa répression des manifestants politiques. La Presse, A9

RCMP called in to investigate report Canadian servers hosting
The Department of Foreign Affairs and International Trade has called in the RCMP to investigate revelations that Syrian government websites are being hosted on Canadian servers. Globe and Mail, A14; Times-Colonist; La Presse

6. Report Says Utility Smart-Grid Cybersecurity in Chaos
A new report released by Pike Research, "Utility Cyber Security: Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond," puts it bluntly: "Utility cyber security is in a state of near chaos. After years of…utilities investing in compliance minimums rather than full security and attackers having free rein, the attackers clearly have the upper hand." Security Management

7. Senate to Take Up Cybersecurity Bill in 2012
Debate in the Senate over cybersecurity legislation will begin in early 2012, Senate Majority Leader Harry Reid (D-Nev.) said late Wednesday. ExecutiveGov

8. Malicious virus armies target Android devices
The arsenal of malicious code aimed at Android- powered gadgets has grown exponentially, with criminals hiding viruses in applications people download to devices, according to Juniper Networks. The Province, A23

9. **Employees' Droids among biggest government cyber menaces.** "In 2012, agencies should worry about hackers attacking the growing number of federal employees toting their own iPhones and Droids to work, according to a forecast of **2012's greatest cyber dangers compiled by M86 Security Labs**. On November 15, the network security firm released its annual predictions of the top computer threats to business and government organizations. At federal agencies, the biggest targets are likely to be employee-owned devices, a department's own public Web site, and cloud services. Agencies without policies to manage security on an employee's smartphone or tablet may have no way of protecting government data from online viruses, according to the research. Even devices that are centrally managed could be vulnerable to intrusions in 2012 because mobile antivirus software has not yet matured, the report said."

Reference: http://www.nextgov.com/nextgov/ng_20111115_9168.php

10. **Cyber-security of power grid in 'near chaos,' report says.** "The cybersecurity of the North American power grid is "in a state of near chaos," according to **report by Pike Research, a consulting group monitoring the industry's transition to wireless digital technologies**, the Ottawa Citizen reported November 15. The group's white paper revealed a $60 smart phone application can bypass security measures and allow direct communications between the phone and some industrial control systems (ICS) that regulate breakers, relays, feeders, and the flow of electricity. As the industry evolves from largely isolated systems to a grid built around interoperable, digital technologies, security jitters are rising. Many ICS have lifespans of 30 years, and mitigation and compensation measures to help them mesh with the newer technologies are creating additional weak links and vulnerabilities. The installation of "smart meters" to improve electricity distribution efficiency is also a potential gateway for attacks. In a rush to install a patchwork of fixes to address potential cybersecurity gaps and with some utilities investing in compliance minimums rather than full security, "the attackers clearly have the upper hand," said the report."

Reference:

11. **US general: 'We're cleared to cyber-bomb enemy hackers'**. "The US military is now legally in the clear to launch offensive operations in cyberspace, the commander of the US Strategic Command has said. "I do not believe that we need new explicit authorities to conduct offensive operations of any kind," Air Force General Robert Kehler told Reuters. But he added that the military was still figuring out the rules of engagement for cyber-warfare outside the "area of hostilities", which are the places they've already been approved to do battle in. US Strategic Command is in charge of a number of areas for the US military, including space operations (like military satellites), cyberspace concerns, 'strategic deterrence' (translation: nuclear weapons) and combating WMDs. In May 2010, it set up a subdivision called US Cyber Command to specifically deal with what the military refers to as the newest potential battle 'domain'. The US Department of Defense released a report on Tuesday that echoes what America and the UK have previously said, that they reserve the right to respond to cyber threats as they would to any other sort of threat."

Reference: http://www.theregister.co.uk/2011/11/17/us_military_cyberspace/

12. **Make it easy for biz to report cyber robberies, say MPs.** "Ten British MPS are calling on the UK.gov to make it easier for companies to report cybercrime to the relevant authorities. Members from a whole bunch of parties – two MPs from the Labour, Conservative and Lib Dem parties and one each from the DUP, SDLP, Plaid Cymru and one Independent – are backing the early day motion that hopes to get Parliament to debate the current lack of an efficient method for businesses to let the right people know when they have been the victim of a cybercrime. According to the motion, 40 per cent of cybercrimes committed against firms currently go unreported, but 85 per cent of businesses in Scotland and England say they would report the incidents if "they felt that there was a sufficient and dedicated mechanism to do so". The MPs also said that

although the Met in London has a dedicated e-crime unit, there was no direct access for assistance or reporting by companies and "standard methods of reporting are proving ineffective"."

Reference: http://www.theregister.co.uk/2011/11/17/mp_call_for_easier_cybercrime_reportage/

13. Duqu Gang Working on Trojan for Years: Kaspersky

Security researchers find that some Duqu Trojan components date back to 2007 and Iran may have seen an early variant months ago, but didn't share the information with the global security research community. The team behind the Duqu Trojan may have been working on the Trojan for at least four years, according to the latest analysis of the sophisticated malware. Kaspersky Lab researchers have identified the overall methods used by the authors of the Duqu Trojan and an approximate timeline of the attack, Alexander Gostev, chief security expert at Kaspersky Lab, wrote on the Securelist blog. The analysis was based on samples provided by the Computer Emergency Response Team - Sudan that were used in at least three attacks against unidentified targets in the country. eWeek

14. Bitdefender finds Anonymous threat to attack Facebook

Bitdefender, an award-winning provider of innovative Internet security solutions, has found a recent video post by the hacktivist group, Anonymous Central, saying it intends to attack Facebook accounts with a 'highly sophisticated' piece of malware, codenamed Fawkes Virus. Allegedly, the malware – which was 'fully written' by Anonymous' programmers – has already been tested. According to the message, the Fawkes Virus consists of "a highly sophisticated worm, with advanced network self-replication and remote abilities. It sends out malicious links and gains access of your account." PR Wire

15. Stolen Malaysian key used to sign malicious software

A malicious program that uses a signing key has been detected. According to F-Secure, a malicious program has been using a digital certificate that was stolen from the Malaysian government. This certificate has been used to legitimise software when users download it from the web, helping it to remain undetected. Mikko Hypponen, chief research officer at F-Secure, claimed it is not that common to find a signed copy of malware, but it is even rarer that it is signed with an official government key. F-Secure detected that the 'mardi.gov.uk' signing key was found to belong to the Malaysian Agricultural Research and Development Institute, and its investigations suggest that it was stolen quite some time ago. SC Magazine U.K.

16. **Ambulance System Disabled by Malware**

A malware infection recently disabled the communications network for New Zealand's St. John Ambulance service, forcing dispatchers to use manual backup systems. eSecurity Planet

17. **Ambulance service disrupted by computer virus infection:** "The St John Ambulance service in New Zealand fell victim to a computer virus infection last week, according to media reports, which disabled its automated response systems across the country.The service, which provides 90% of the emergency and non-emergency ambulance cover for the New Zealand population, was struck by a malware attack on Wednesday forcing staff to allocate ambulances manually according to Alan Goudge"

Reference: http://nakedsecurity.sophos.com/2011/11/14/ambulance-service-disrupted-by-computer-virus-infection/

18. Iran Claims To Have Contained 'Duqu' Computer Virus

Iran claimed Monday that it has contained the so-called espionage malware Duqu that had infected some computer systems linked to the Islamic Republic's controversial nuclear program. RTT News

19. sn3Ak3r hacks social network and leaks 57,000 credentials.

http://news.softpedia.com/news/sn3Ak3r-Hacks-Social-Network-and-Leaks-57-000-Credentials-234240.shtml

FindFriendz.com social network website is the one that leaked the massive quantities of information as a result of an SQL injection attack which took advantage of a common vulnerability.

The hacker published only a small part of his loot, but he claims that he will make the rest available for anyone that requests it.

20. UK Cyber Security Strategy themes revealed

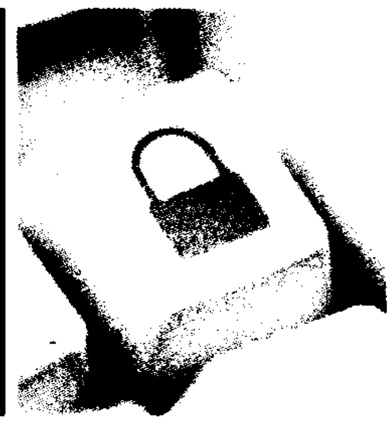
The UK government will urge businesses to form 'uncomfortable partnerships' with competitors as part of the upcoming UK Cyber Security Strategy, ZDNet UK has learned. Businesses must look to forming close working relationships with competitors to share sensitive cybersecurity information, they will be told when the document is published. The UK Cyber Security Strategy is due on 25 November, a Cabinet Office spokesman confirmed on Thursday. ZDNet

Public Safety Canada | Sécurité publique Canada

Canada

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-002



For the Week of

22 - 28 Oct 2011

Issued: 4 Nov 2011

HIGHLIGHTS:

- **Threat Warnings:**
  - Hacker group Anonymous urged sympathizers to participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5 - ITAC assesses the risk to be low.
- **Reported Incidents:**
  - Federal agency spammed with a suspicious e-mails referencing Gaddafi;
  - Targeted attacks on a Canadian Internet Service Provider's core infrastructure;
  - On-line recruitment of Canadian money launderers;
  - On-line posting of Canadian police personnel computer user information;
  - Computers in provincial governments, energy companies, universities and a hospital's networks compromised; and
  - Computer users lured to malicious web sites by threat actors impersonating reputable Canadian bank and airline organizations.
- **International News:** Chinese military suspected of hacking US satellites; Japanese missions around the world experienced targeted cyber attacks; Finland wants to build offensive cyber capability.

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered or reported to the Canadian Cyber Incident Response Centre (CCIRC), any notable international news and any CIRC information products issued during the week.

NOTABLE INCIDENTS– 22 THROUGH 28 OCTOBER 2011:

Government Systems.

Federal Government. CCIRC received a report of employees in a federal agency receiving e-mails, with the subject line referencing Mohammed Gaddafi and Allah. CCIRC forwarded information on this incident to the Cyber Threat Evaluation Centre (CTEC), the cyber incident handler for the federal government.

Analysis: CCIRC has no information to indicate whether this federal departmental was targeted specifically by these e-mails. However, referencing popular news items and events is a common tactic used to lure internet users into opening e-mails with malicious content.

Provincial Government. CCIRC received reports on potential compromises of computers on three provincial government systems.

Analysis: CCIRC has no information to indicate that these were targeted attacks on the provinces. Reports indicated that the computers in question were infected with malicious software commonly used by cyber criminals.

Police. CCIRC discovered that user account information for a number of Canadian police organizations was posted on a hacker website. CCIRC sent information to the RCMP for evaluation and notification of the affected police agencies.

Analysis: CCIRC has no information whether police computer networks were compromised as a result of this activity. A similar incident for a Canadian provincial police force and a number of American police organizations occurred earlier in 2011.

Canadian Critical Infrastructure:

Financial Sector.

Phishing. CCIRC received nine phishing reports and actioned the one that continued to pose a threat. In this incident, a threat actor, impersonating a well-known Canadian bank, was luring computer users via e-mail, to a website hosted in Australia. CCIRC notified the bank, Google phishing, the Anti-Phishing Working Group and Microsoft, so internet users may be alerted if they encounter these websites.

Threats by Anonymous. Anonymous, the famed hacker group, urged sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on November 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on November 5. As of the date of this writing, CCIRC learned the operation to hack the TMX computers on November 7 has been cancelled.

Analysis: Anonymous is a loosely organized hacker group that has the capacity to organize and launch a Distributed Denial of Service (DDOS) attack that could potentially bring down a website. However, the Integrated Threat Assessment Centre (ITAC) does not believe there is a high risk of a cyber attack on November 5.

When Anonymous called for a November 7 attack on the TMX computers, CCIRC contacted major Canadian financial institutions. They confirmed their awareness of the potential threat from Anonymous, and that their internet service providers were prepared to mitigate any DDOS attack. As of the date of this writing, the cyber attack on TMX has been called off.

On-line recruitment for money laundering. CCIRC learned of an on-line recruitment campaign in Canada for money laundering, originating from abroad. CCIRC sent summary and technical details sent to the RCMP Anti-fraud centre as well as the RCMP High-Tech Crime Branch for possible further investigation.

Telecommunications Sector.

Intrusion attempt – Internet Service Provider Core Infrastructure: A Canadian internet service provider informed CCIRC and other Canadian telecommunication companies about recent brute force hacking attempts against their routers, at the rate of 60-100 attempts each day. The attacks appear to be coming from internet service providers in China and Romania, but the attacker cannot be identified conclusively with the available information. The reporting internet service provider has taken mitigation measures.

Analysis: Routers of an internet service provider are used to route internet traffic of its subscribers, and possibly other internet users. Having control of a router on the Canadian telecommunication network would enable a hacker to intercept Canadians' communications and information going through that router, and use that information for a variety of malicious purposes.

Energy Sector. CCIRC received infection reports on computers of three energy sector organizations. These organizations are: A large of oil & gas producer, a service & equipment provider to the oil and gas sector, and a provincial electricity producer. CCIRC notified all three organizations of the potential infections.

Health. CCIRC received a computer infection report for a Canadian hospital and notified the organization's IT department.

Transportation. CCIRC received a report of phishing attempts in the aviation sector. Threat actors were seeking on-line customer credentials for an airline.

UNCLASSIFIED
DRAFT

CCIRC Product: CCIRC released Alert AL11-501 to IT professionals and managers in its stakeholder community. This Alert informs stakeholders about the work-around solution and update released by Entrust, created when it was discovered that a Java software updated interfered with the functionality of some Entrust products.

International News

Chinese military suspected of hacking US satellites. According to a publicized portion of the draft US-China Economic and Security Review Commission annual report, computer hackers, possibly from the Chinese military, interfered with two US government satellites four times in 2007 and 2008. There is currently no public information about the nature of the hackers' interference with these satellites, which are used for earth climate and terrain observations. The report, which is to be released next month, states the interferences occurred through a ground station in Norway.

Japanese missions around the world experienced targeted cyber attacks. Open sources report that at least dozens of computers used at Japanese missions in nine countries, including Canada, have been compromised since this past summer. Many of the compromises were found to allow a remote hacker to gain access and steal confidential information. The Japanese Foreign Ministry is investigating this incident and assessing its impact.

Finland wants cyber war weapons. Open sources report Finland has joined Sweden in planning to include counter-offensive capability for cyber attacks as part of its defence strategy. The new strategy would be presented to parliament and formalized in 2013.

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

NOTES

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 Flashed marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Public Safety Canada | Sécurité publique Canada

Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 28-FEBRUARY 11, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-003

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations. This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents. CCIRC handled 48 incidents during the reporting period. MS Office documents were stolen from over 600 computers in 19 identifiable organizations and 84 telecommunications service providers, which include internet service providers for the Canadian public and corporate sector. Malicious acts include coordinating cyber attacks on the financial sector of another country. A botnet that affected the Canadian energy utility sector in late 2011 was still active. Cyber criminals impersonated banks and the federal government to obtain financial and personal information from computer users (phishing). There were website defacements for health, education, municipal and provincial government sector organizations.

Highlights

- Microsoft Office documents stolen from over 600 computers.
- Is your computer one of the thousands in Canada affected by Ghostclick? Check CCIRC approved site www.dns-ok.ca
- Ghostclick in Canada – Some Statistics
- In the news: Anonymous hacks websites of U.S., French Government & UN

CCIRC Products Released:

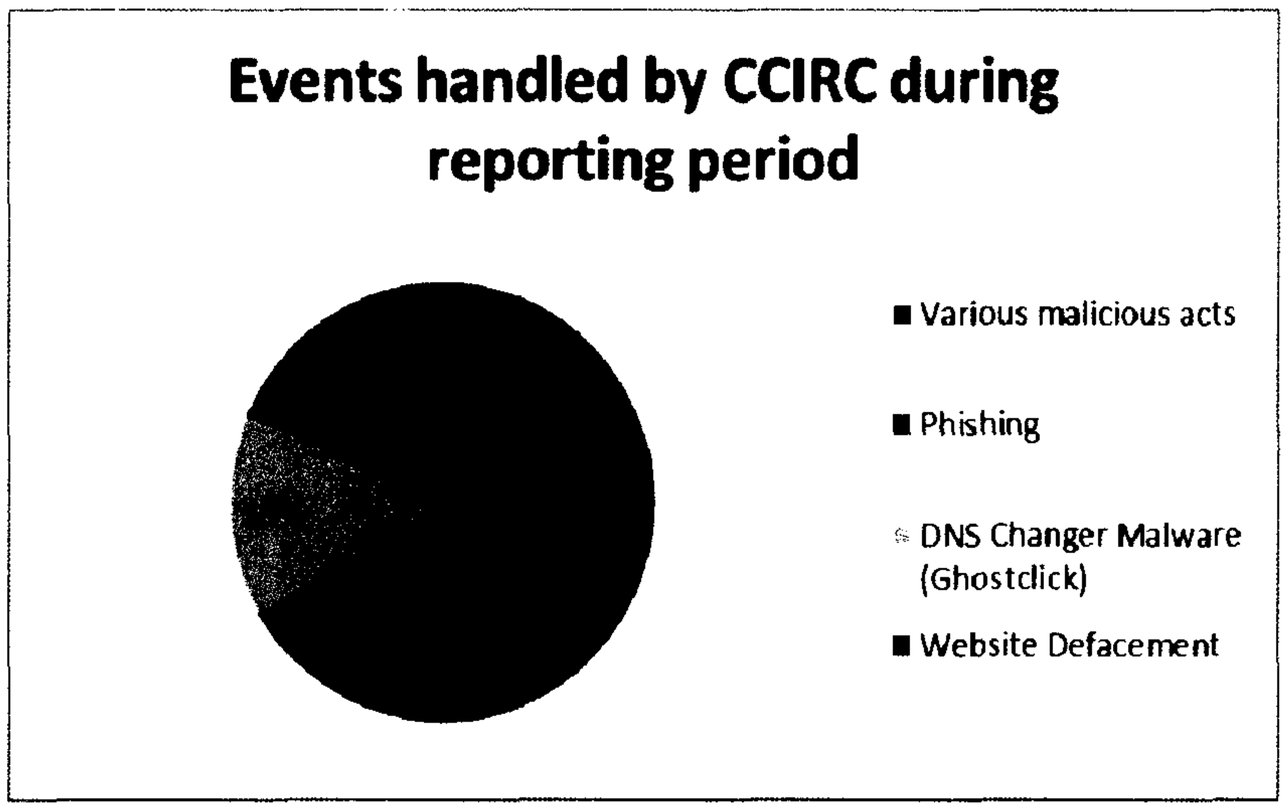
- Cyber Flash CF12-002: Malware uses Sendspace.com file-hosting site to store stolen documents.

Noteworthy News in the Media:

- Hackers attack websites of the French Government, US Department of Homeland Security and UN; Anonymous releases FBI conference call recording
- Hackers in Europe release names of persons involved in hate movements – includes 74 Canadians

NEW EVENTS REPORTED

Non-Federal Government Critical Infrastructure Sector



Microsoft Office Documents stolen from over 600 Canadian entities. A trusted partner alerted CCIRC that MS Excel and Word documents originating from over 600 Canadian computers were stolen and posted to a file-sharing website. Computers in question were compromised via a malicious executable file attachment to an e-mail. It was noted the malicious software attempts to contact a website in Russia. The impact of this incident is unknown to CCIRC.

CCIRC notified the identified entities, which included provincial health and municipal government entities, a financial institution, a utility, an auto parts manufacturer, post-secondary institutions. Telecommunications service providers were also notified so they could to notify their clients, whose data would have been stolen. CCIRC also sent Cyber Flash CF12-002 to all CCIRC stakeholders.

part of document - not a redaction

> ***Comment:*** *The impact of this incident is unknown at this time. It is likely that the threat actors intended to upload the stolen documents from this file-sharing website to obscure their identity and location.*
>
> *Malicious e-mails are a very common but still very effective method of compromising computer systems. Security researchers see this trend continuing in 2012 and CCIRC would agree. In fact, CCIRC sees that cyber criminals are becoming more effective by sending more tailored e-mails to individuals in organizations. Organizations need to implement a wide range of organizational measures that range from technical solutions to employee education.*

Canadian domain being used in cyber attacks. CCIRC learned that a Canadian domain was used to coordinate a Distributed Denial of Service cyber attack on websites of an allied country's financial sector. This domain was registered in Canada by an individual in Moscow, Russia, but the cyber attacks were traced to a computer in Latvia.

CCIRC assisted the ally country by contacting the Canadian domain name registrar and requesting it rectify the situation. CCIRC also notified the Canadian Internet Registration Authority (CIRA) and Canadian law enforcement. The malicious site is no longer active as of the writing of this report.

> ***Comment:*** *Many computer users/operators can and do block internet access from computers and websites known to reside in untrusted countries. Therefore, cyber criminals take advantage of the trusted on-line reputation of countries like Canada by registering an Internet domain name in Canada and appearing to be a Canadian website.*

Web related services such as domain name registration have an international client base and no rigorous identity verification process. International law enforcement is discussing this issue with the international domain name registrar community at the International Corporation for Assigned Names and Numbers (ICANN) meetings. ICANN is an international, non-profit group that plays a coordinating role for the Internet's naming system.

Botnet that affected the Canadian energy utility sector in late 2011 is still active. An energy utility partner reported that the Raumoni Perl Botnet that affected that organization three months ago was still active elsewhere and provided information about the controller to CCIRC. CCIRC's technical team is currently analyzing the associated data so Canadian victims can be identified and notified.

Canadian credit card information posted online. Credit card information of six Canadians was found to be posted online. This item is of interest because it appears to be a continuation of the STRATFOR website hacking in December 2011. In that incident, approximately 75,000 credit card numbers and 860,000 login credentials were posted online. In Canada, 880 federal government workers and 109 provincial government users in nine provinces were affected.

not a redaction

Comment: *There is little doubt we will continue TO see repercussions of the STRATFOR website hacking. The client information posted online includes government officials who are interested in STRATFOR's intelligence reports. As of the time of this writing, there were news reports of STRATFOR clients being targeted with malicious e-mails. These e-mails, purportedly originating from the STRATFOR CEO, asked clients to click on a link and fill out a form.*

Canadian computer part of an international malicious network (botnet). CCIRC learned a Canadian computer was part of a FastFlux botnet that appears to be controlled by a Russian website. A Fast Flux botnet is a malicious network of computers that can hide phishing and malware delivery sites behind an ever-changing network of compromised computers.

The Internet services for the Canadian entity are provided by a hosting provider in British Columbia. CCIRC contacted the parent company of the hosting provider and informed law enforcement.

Comment: *Zeus is a common trojan virus used by cyber criminals to gain access to computers and recruit them for botnets. It has evolved over time and proven to be very resilient. The international community keeps a reasonably up to date map of computers infected with this virus, called the "Zeus Tracker". Organizations are encouraged to check this map periodically to see if they are inadvertently hosting the Zeus virus.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonated Canadian financial institutions and tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in Russia, France, Vietnam, Germany and the U.S. Almost half of the phishing attempts originated from the U.S. The entity linked to the German website spoofed two different well known Canadian banks.

CCIRC notified the Phishing Intake Centres of the impersonated financial institutions. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website defacements. CCIRC discovered a provincial department of health's website was defaced. This was also observed by the local IT staff and mitigated before any loss of personal data or content occurred. Similarly, the websites of a first nation's health organization, an educational institution and student/community organization, were defaced.

CCIRC notified all the relevant technical contacts in each situation and offered mitigation advice where required.

> ***Comment:*** *Many websites have built-in technical vulnerabilities from the design stage. Website vulnerabilities such as cross-site scripting are well known to hackers. CCIRC is seeing instances where websites are scanned for well-known vulnerabilities with automated tools and lists of the vulnerable websites posted online.*
>
> *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

Federal Government Sector

Fraudulent Government of Canada website is malicious. A malicious website, spoofing a federal government department, solicited sensitive private information from computer users. It is unknown whether any information was given by users. This website was hosted in the U.S.

CCIRC contacted the Internet Service Provider hosting the website and requested remedial action. CCIRC also requested CIRA help deactivate this fraudulent domain and informed US CERT. While the malicious content from this website has now been removed, the website itself is still accessible by Internet users. CCIRC continues to work on this case.

Government of Canada Agency logo used in on-line extortion case. Cyber criminals, impersonating a Government of Canada agency, caused extortion messages to appear on some users' computers. The messages informed users that they were "caught" looking at child porn and that their internet access would be shut down immediately unless a ransom was paid. CCIRC has passed this case to Law Enforcement for investigation.

> ***Comment:*** *Trusted entities are frequently impersonated by cyber criminals for fraud purposes. At the time of this writing, the same scheme was being perpetrated outside Canada where cyber criminals impersonated Scotland Yard.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

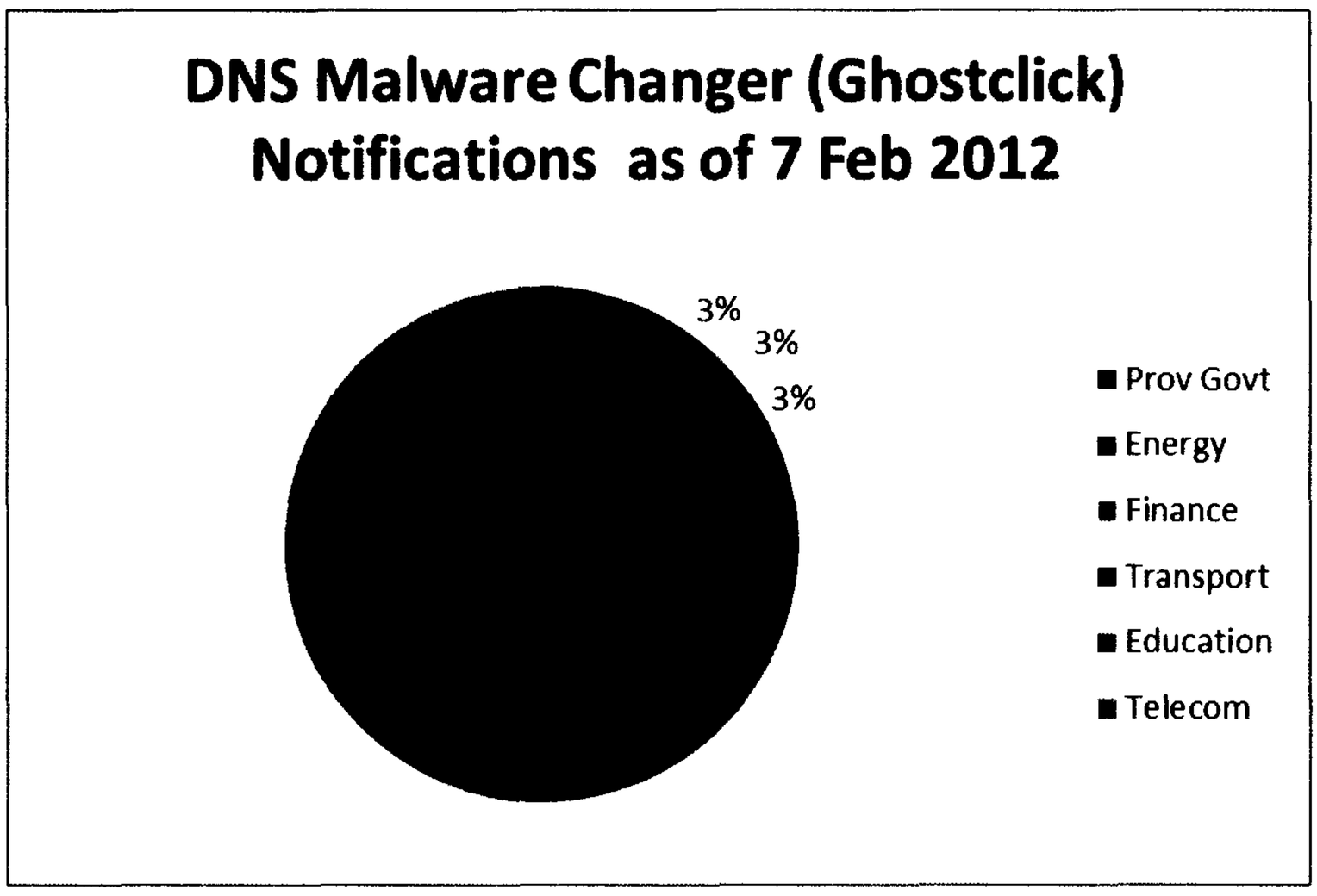
Ghostclick Fraud – DNS Changer malicious software. There were new and continued reports of infected computers in the provincial government, energy, finance, health, transportation, educational and telecommunication sectors.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012 {March 8 or 31st??) There are reports that the deadline may be extended to July 2012.

Canadians may now check to see if their computers have been affected by clicking on www.dns-ok.ca. This website, the result of a CCIRC-CIRA cooperation, is hosted by CIRA. Canada is now one of the four countries in the world that offer such a website to their citizens and the world.

Operation Ghostclick in Canada – as seen by CCIRC

- Initial count: 20,481
- Current count: 16,671
- 11th in 54 countries with more than 1000 IPs
- Most improved: Universities



While 65% of the remaining infections seen by CCIRC in Canada are traced to the telecommunications companies, it is more than likely that it is the companies' customers' computers that remain infected. These telecommunications companies provide Internet service to corporate and individual clients.

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in.

NOTEWORTHY NEWS IN THE MEDIA:

Hacker Group Anonymous releases FBI conference call recording and hacks DHS website. As what is widely presumed to be a resumption of Anonymous's Operation against law enforcement, the hacker group eavesdropped on an internal conference call at the FBI. The recording of that call was then released publicly. FBI has confirmed the recording was authentic. The hacker group was able to accomplish this by obtaining the conference call information e-mail sent to invited participants.

Anonymous also took credit for hacking of US Department of Homeland Security's website. Though this happened on the same Friday as the event above, the exact reason is unknown. The DHS website was back online within minutes of the incident.

The French Government website is hacked by Anonymous. The reason given for this hacking was opposition to ACTA, the controversial Anti-Counterfeiting Trade Agreement (ACTA). The same week, hundreds of people across 36 cities in France demonstrated against ACTA. The European Parliament has not yet ratified this agreement but 22 members of the EU, including France, have signed on. Canada has also signed ACTA.

Hackers in Europe release names of persons involved with hate movements, including 74 Canadians. The identities were revealed on a website called Nazi Leaks, which is now offline.

The UN website is hacked. TeamPoison, a hacker group loosely associated with Anonymous, hacked the UN's website. Though the group cited they were for "freedom on the internet" (sic), the exact reason was unclear.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

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

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Public Safety Canada | Sécurité publique Canada

Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 28-FEBRUARY 11, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-001

Purpose

This product is intended to provide Chief Information Officers (CIO) in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations. This product also provides contextual background information on the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents. CCIRC handled 48 incidents during this reporting period. MS Office documents were stolen from over 600 computers in 19 identifiable organizations and 84 telecommunications service providers, which include internet service providers for the Canadian public and corporate sector. Malicious acts include coordinating cyber attacks on the financial sector of another country. A botnet that affected the Canadian energy utility sector in late 2011 was still active. Cyber criminals impersonated banks and the federal government to obtain financial and personal information from computer users (phishing). There were website defacements for health, education, municipal and provincial government sector organizations.

Highlights

- Microsoft Office documents stolen from over 600 computers.
- Is your computer one of the thousands in Canada affected by Ghostclick? Check CCIRC approved site www.dns-ok.ca
- Ghostclick in Canada – Some Statistics
- In the news: Anonymous hacks websites of U.S., French Government & UN

CCIRC Products Released:

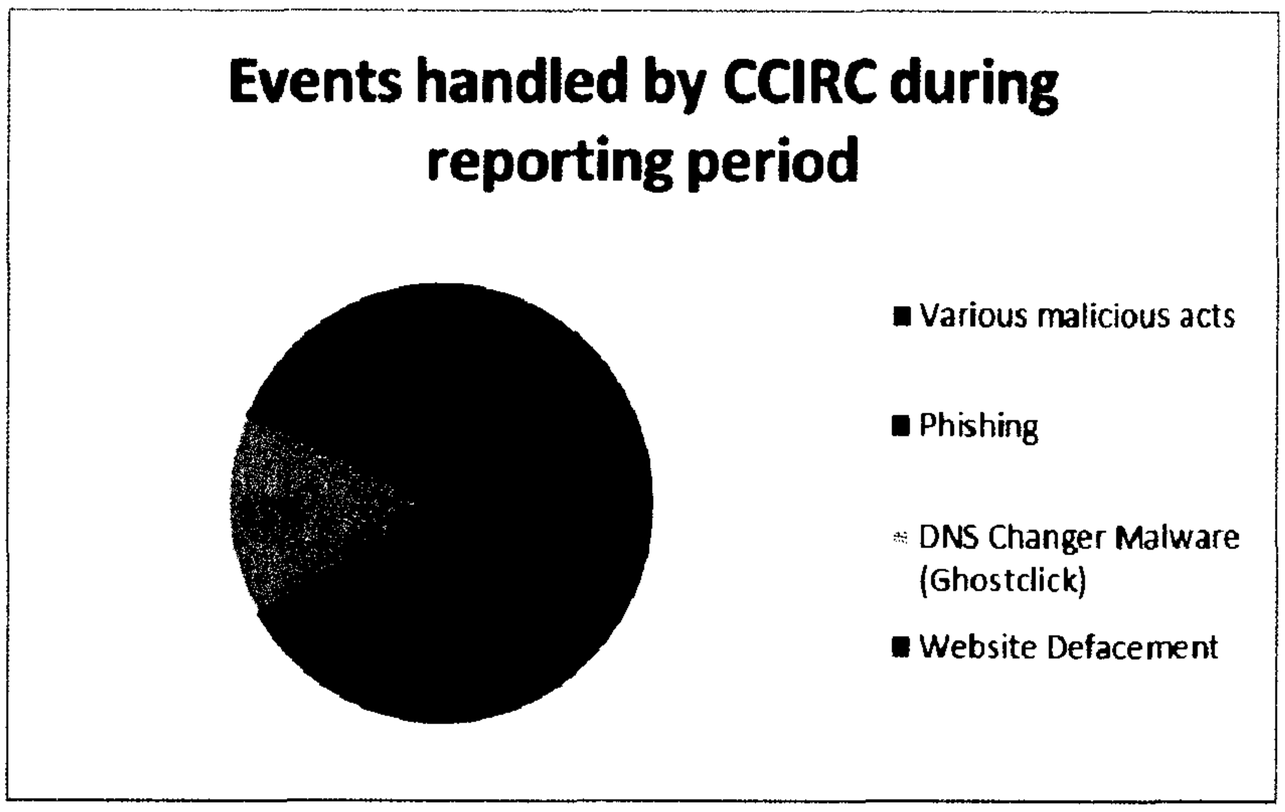
- Cyber Flash CF12-002: Malware uses Sendspace.com file-hosting site to store stolen documents.

Noteworthy News in the Media:

- Hackers attack websites of the French Government, U.S. Department of Homeland Security and UN; Anonymous releases FBI conference call recording
- Hackers in Europe release names of persons involved in hate movements – includes 74 Canadians

NEW EVENTS REPORTED

Non-Federal Government Critical Infrastructure Sector



Microsoft Office Documents stolen from over 600 Canadian entities. A trusted partner alerted CCIRC that MS Excel and Word documents originating from over 600 Canadian computers were stolen and posted to a file-sharing website. Computers in question were compromised via a malicious executable file attachment to an e-mail. It was noted the malicious software attempts to contact a website in Russia. The impact of this incident is unknown to CCIRC.

CCIRC notified the identified entities, which included provincial health and municipal government entities, a financial institution, a utility, an auto parts manufacturer, post-secondary institutions. Telecommunications service providers were also notified so they could notify their clients, whose data would have been stolen. CCIRC also sent Cyber Flash CF12-002 to all CCIRC stakeholders.

> ***Comment:*** *The impact of this incident is unknown at this time. It is likely that the threat actors intended to upload the stolen documents from this file-sharing website to obscure their identity and location.*
>
> *Malicious e-mails are a very common but still very effective method of compromising computer systems. Security researchers see this trend continuing in 2012 and CCIRC would agree. In fact, CCIRC sees that cyber criminals are becoming more effective by sending more tailored e-mails to individuals in organizations. Organizations need to implement a wide range of organizational measures that range from technical solutions to employee education.*

Canadian domain being used in cyber attacks. CCIRC learned that a Canadian domain was used to coordinate a Distributed Denial of Service cyber attack on websites of an allied country's financial sector. This domain was registered in Canada by an individual in Moscow, Russia, but the cyber attacks were traced to a computer in Latvia.

CCIRC assisted the ally country by contacting the Canadian domain name registrar and requesting it rectify the situation. CCIRC also notified the Canadian Internet Registration Authority (CIRA) and Canadian law enforcement. The malicious site is no longer active as of the writing of this report.

> ***Comment:*** *Many computer users/operators can and do block internet access from computers and websites known to reside in untrusted countries. Therefore, cyber criminals take advantage of the trusted on-line reputation of countries like Canada by registering an Internet domain name in Canada and appearing to be a Canadian website.*

Web related services such as domain name registration have an international client base and no rigorous identity verification process. International law enforcement is discussing this issue with the international domain name registrar community at the International Corporation for Assigned Names and Numbers (ICANN) meetings. ICANN is an international, non-profit group that plays a coordinating role for the Internet's naming system.

Botnet that affected the Canadian energy utility sector in late 2011 is still active. An energy utility partner reported that the Raumoni Perl Botnet that affected that organization three months ago was still active elsewhere and provided information about the controller to CCIRC. CCIRC's technical team is currently analyzing the associated data so Canadian victims can be identified and notified.

Canadian credit card information posted online. Credit card information of six Canadians was found to be posted online. This item is of interest because it appears to be a continuation of the STRATFOR website hacking in December 2011. In that incident, approximately 75,000 credit card numbers and 860,000 login credentials were posted online. In Canada, 880 federal government workers and 109 provincial government users in nine provinces were affected.

Comment: *There is little doubt we will continue to see repercussions of the STRATFOR website hacking. The client information posted online includes government officials who are interested in STRATFOR's intelligence reports. As of the time of this writing, there were news reports of STRATFOR clients being targeted with malicious e-mails. These e-mails, purportedly originating from the STRATFOR CEO, asked clients to click on a link and fill out a form.*

Canadian computer part of an international malicious network (botnet). CCIRC learned a Canadian computer was part of a FastFlux botnet that appears to be controlled by a Russian website. A Fast Flux botnet is a malicious network of computers that can hide phishing and malware delivery sites behind an ever-changing network of compromised computers.

The Internet services for the Canadian entity are provided by a hosting provider in British Columbia. CCIRC contacted the parent company of the hosting provider and informed law enforcement.

Comment: *Zeus is a common trojan virus used by cyber criminals to gain access to computers and recruit them for botnets. It has evolved over time and proven to be very resilient. The international community keeps a reasonably up to date map of computers infected with this virus, called the "Zeus Tracker". Organizations are encouraged to check this map periodically to see if they are inadvertently hosting the Zeus virus.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonated Canadian financial institutions and tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in Russia, France, Vietnam, Germany and the U.S. Almost half of the phishing attempts originated from the U.S. The entity linked to the German website spoofed two different well known Canadian banks.

CCIRC notified the Phishing Intake Centres of the impersonated financial institutions. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website defacements. CCIRC discovered a provincial department of health's website was defaced. This was also observed by the local IT staff and mitigated before any loss of personal data or content occurred. Similarly, the websites of a first nation's health organization, an educational institution and student/community organization, were defaced.

CCIRC notified all the relevant technical contacts in each situation and offered mitigation advice where required.

> ***Comment:*** *Many websites have built-in technical vulnerabilities from the design stage. Website vulnerabilities such as cross-site scripting are well known to hackers. CCIRC is seeing instances where websites are scanned for well-known vulnerabilities with automated tools and lists of the vulnerable websites posted online.*
>
> *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

Federal Government Sector

Fraudulent Government of Canada website is malicious. A malicious website, spoofing a federal government department, solicited sensitive private information from computer users. It is unknown whether any information was given by users. This website was hosted in the U.S.

CCIRC contacted the Internet Service Provider hosting the website and requested remedial action. CCIRC also requested CIRA help deactivate this fraudulent domain and informed US CERT. While the malicious content from this website has now been removed, the website itself is still accessible by Internet users. CCIRC continues to work on this case.

Government of Canada Agency logo used in on-line extortion case. Cyber criminals, impersonating a Government of Canada agency, caused extortion messages to appear on some users' computers. The messages informed users that they were "caught" looking at child porn and that their internet access would be shut down immediately unless a ransom was paid. CCIRC has passed this case to Law Enforcement for investigation.

> ***Comment:*** *Trusted entities are frequently impersonated by cyber criminals for fraud purposes. At the time of this writing, the same scheme was being perpetrated outside Canada where cyber criminals impersonated Scotland Yard.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

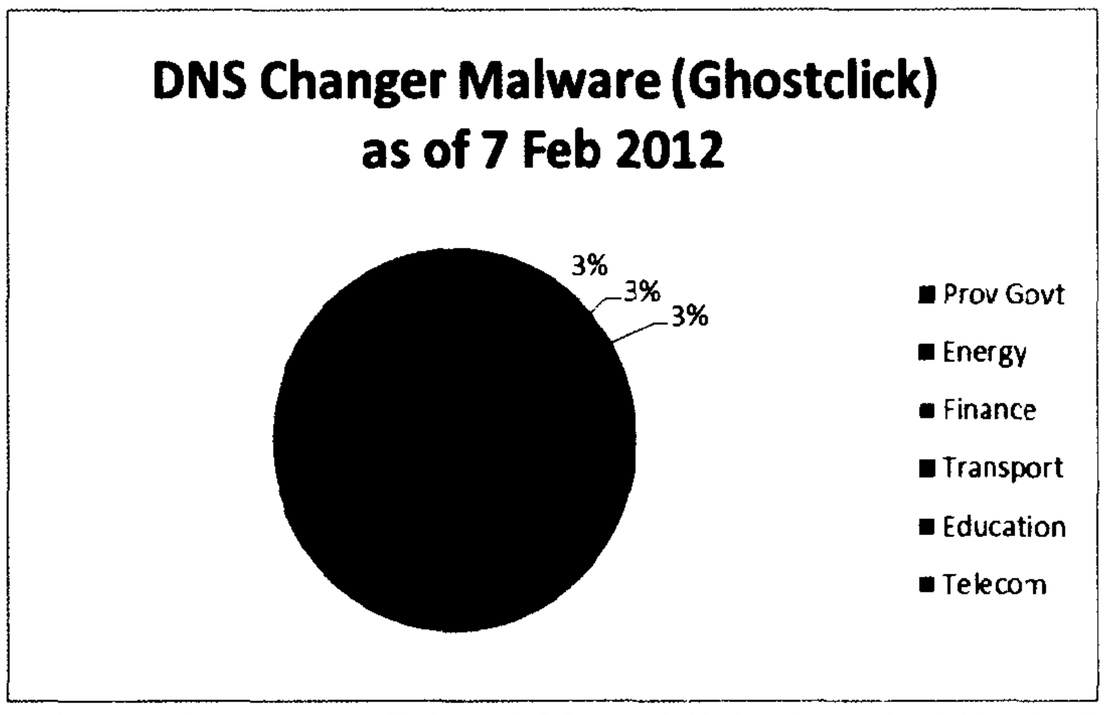
Ghostclick Fraud – DNS Changer malicious software. There were new and continued reports of infected computers in the provincial government, energy, finance, health, transportation, educational and telecommunication sectors.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are reports that the deadline may be extended to July 2012.

Canadians may now check to see if their computers have been affected by clicking on www.dns-ok.ca. This website, the result of a CCIRC-CIRA cooperation, is hosted by CIRA. Canada is now one of the four countries in the world that offer such a website to their citizens and the world.

Operation Ghostclick in Canada – as seen by CCIRC

- Initial count: 20,481
- Current count: 16,671
- 11th in 54 countries with more than 1000 IPs
- Most improved: Universities



While 61% of the remaining infections seen by CCIRC in Canada are traced to the telecommunications companies, it is more than likely that it is the companies' customers' computers that remain infected. These telecommunications companies provide Internet service to corporate and individual clients.

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in.

NOTEWORTHY NEWS IN THE MEDIA:

Hacker Group Anonymous releases FBI conference call recording and hacks DHS website. As what is widely presumed to be a resumption of Anonymous's Operation against law enforcement, the hacker group eavesdropped on an internal conference call at the FBI. The recording of that call was then released publicly. FBI has confirmed the recording was authentic. The hacker group was able to accomplish this by obtaining the conference call information e-mail sent to invited participants.

Anonymous also took credit for hacking the U.S. Department of Homeland Security's (DHS) website. Though this happened on the same Friday as the event above, the exact reason is unknown. The DHS website was back online within minutes of the incident.

The French Government website is hacked by Anonymous. The reason given for this hacking was opposition to ACTA, the controversial Anti-Counterfeiting Trade Agreement (ACTA). The same week, hundreds of people across 36 cities in France demonstrated against ACTA. The European Parliament has not yet ratified this agreement but 22 members of the EU, including France, have signed on. Canada has also signed ACTA.

Hackers in Europe release names of persons involved with hate movements, including 74 Canadians. The identities were revealed on a website called Nazi Leaks, which is now offline.

The UN website is hacked. TeamPoison, a hacker group loosely associated with Anonymous, hacked the UN's website. Though the group cited they were for "freedom on the internet" (sic), the exact reason was unclear.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, Canadian Cyber Incident Response Centre Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

OUR ORGANIZATION

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

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Public Safety Canada | Sécurité publique Canada

Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CYBER SECURITY SUMMARY FOR CIOs

Reporting Period: JANUARY 14-28, 2012
CCIRC CYBER AWARENESS PRODUCT: 12-S-002

Purpose

This product is intended to provide Chief Information Officers in government and in other critical infrastructure sectors cyber-information, which can support operational and security decision-making in their organizations.

This product also provides contextual background information for the technical products released by the Canadian Cyber Incident Response Centre (CCIRC) over the reporting period.

Overview

Domestically, there were no significant cyber incidents reported over the last two weeks. There were reports of Canadian computers being used for malicious purposes, including attacking a US State Police website. A Canadian federal department linked to the signing of the international Anti-Counterfeiting Agreement (ACTA) was targeted through a malicious e-mail. There was also a message on the Internet by hackers to e-mail or launch a cyber attack against this Department. Internationally, hackers attacked government websites in US, Poland, Ireland and the EU to protest signing of ACTA. There are also continued reports of infected computers in Canada and around the world due to the Ghostclick fraud.

Highlights

New Events:

- A Canadian federal department with links to ACTA targeted by hackers
- File server log in credentials of a federal department posted on the Internet
- Incidents of Canadian computers hosting malicious software
- US State Police website attack traced to Canada
- Some Canadian Industrial Control Systems (ICS) reported as being exposed to potential cyber attack".
- Phishing: Fraud attempts in the Financial sector; Cyber criminals impersonating federal organizations
- Website compromises and publicized vulnerabilities in following sectors: Canadian health, non-critical infrastructure sector and a foreign Defence Department

CCIRC Products Released during the reporting period:

- Cyber Flash on cyber attacks by Anonymous related to copyrights and intellectual property (CF12-001)

Noteworthy News in the Media:

- Israeli and Palestinian hackers exchange website attacks
- Hackers around the world protest current and intended anti-piracy measures:
    - MegaUpload's shutdown prompts hacker attacks on US government and music industry websites
    - Proposed US copyright law SOPA being protested: Certain websites elect to go dark for one day in protest; Anonymous attacks US government websites such as DOJ & FBI
    - Signing of the international Anti-Counterfeiting Agreement (ACTA) prompting hacker attacks on US, Poland, Ireland and European government websites.

NEW EVENTS REPORTED IN GOVERNMENT AND OTHER CANADIAN CRITICAL INFRASTRUCTURE SECTORS

Federal Government Sector

Operation SACTA (Stop Anti-Counterfeiting Trade Agreement): An online message signed by Anonymous posted a link to a Canadian federal department website, encouraging users to join the anti-ACTA movement, and attack if necessary. This message was posted on a popular text-file sharing website often used by hackers and is presumably encouraging cyber attacks on websites.

CCIRC provided available technical details to CTEC, the federal Government's CERT, for their further investigation.

> ***Comment:*** *There are provisions in the international Anti-Counterfeiting Trade Agreement that have important implications for content sharing on the Internet. This is a multi-lateral trade agreement which Canada has signed. Canada's new proposed copy-right law, Bill C-11 (former Bill C-32), is currently in Parliament at the second reading stage. There is a great deal of opposition to this agreement around the world by the on-line community and websites of other government have recently been attacked by hackers in protest.*

File Server (FTP) Login Credentials of a Federal Department posted on the Internet. CCIRC learned that the FTP login credentials of a federal department were posted on the Internet. CCIRC advised CTEC and provided known technical details.

> ***Comment:*** *FTP login credentials are used to gain access to a file sharing server where users may upload or download files. If a threat actor used these credentials, the result could be information compromise or the use of the server as a launch point for cyber attacks.*

Non-Federal Government Sector

Canadian computers being used in cyber attacks. CCIRC has learned that a cyber attack on a US State Police website was traced to a Canadian university's computer. In addition, another Canadian university's website was found to host malicious software that could infect website visitors. There were also reports of malicious software being hosted at a website hosting service provider's server and at two other unidentified Canadian entities.

CCIRC contacted the known Canadian organizations, with mitigation advice. The RCMP was informed of items of interest. CCIRC warned the website hosting service provider that the website in question was added to various block lists, possibly resulting in reduced legitimate traffic to this website. The malicious software from the university's website has been removed and is no longer being served.

> ***Comment:*** *It is possible that cyber criminals compromised these Canadian computers to use them remotely for malicious purposes, without their owners' knowledge. Organizations that offer computers for public use, such as universities, can be particularly susceptible to such compromises.*

Some Canadian Industrial Control Systems exposed to potential cyber attacks. A trusted international partner alerted CCIRC that information that could allow remote access to certain Canadian houses and apartment buildings' heating and air conditioning systems, was posted on the Internet. CCIRC alerted those responsible for the buildings and houses, offering mitigation advice. There is no report of any cyber attack in these cases at this time.

> ***Comment:*** *Many Industrial Control Systems (ICS), such as the ones used for heating and cooling buildings, are monitored or even maintained remotely through the use of certain software. It is likely that the technicians responsible for the set-up and maintenance of the heating systems for these buildings did not take cyber security into consideration or did not know the standard practices for protecting against such exposure.*
>
> *Since the Stuxnet virus attack on an Iranian nuclear facility, there has been a heightened awareness, both domestically and internationally, of cyber security for ICS. The trusted international partner who alerted CCIRC is focussed primarily on securing ICS. CCIRC recently moderated discussion at a ICS conference in Montreal.*

Fraud attempts (Phishing). The Canadian Anti-Fraud Centre reported that cyber criminals impersonating Canadian financial institutions, tried to solicit personal information and financial credentials of computer users via e-mail. It is unknown if any computer users provided their credentials. The links in these e-mails led to websites hosted in United States and Taiwan.

Cyber criminals also attempted to solicit personal information by impersonating Service Canada and Canada Revenue Agency.

CCIRC notified the impersonated financial institutions of these fraud attempts and the Government CTEC for the federal government cases. Microsoft Smartfilter, Google and the Anti-Phishing Working Group were also informed so they can warn computer users if they visit these malicious sites.

Website compromises and publicized vulnerabilities. CCIRC discovered a small health organization's website was defaced and offered mitigation advice. CCIRC also discovered a foreign Defence Department's website was compromised and contacted the organization, as well as CCIRC's equivalent organization. There was also a list of vulnerable websites posted on the Internet, which includes a Canadian university.

There were additional website compromises in the health and non-critical infrastructure sectors. Website usernames and passwords were posted on the Internet by hackers.

> ***Comment:*** *Organizations should monitor their websites and be vigilant against website defacements. Website defacement can be done for a variety of reasons, which range from mischief, intent to embarrass the organization, or testing the vulnerability of a particular website. A website vulnerable to defacement may also be used to compromise the computers of that website's visitors.*

UPDATES ON PREVIOUSLY REPORTED EVENTS:

Ghostclick Fraud. There were new and continued reports of infected computers in three provincial governments, three provincial health organizations, an airport authority, an energy organization, two banks, 19 Canadian universities, a national media organization and 13 telecommunications companies.

Infected computer owners/operators will lose their connection to the Internet if they do not take mitigation measures by March 8, 2012. There are currently websites around the world for computer users to check whether their machine is infected by the malicious software used in this fraud. These sites can be found by searching with the keywords "dns-ok".

CCIRC provided technical details and mitigation advice for this fraud via the Information Note (IN11-002) published on Public Safety Canada's website on November 9, 2011. CCIRC continues to notify known stakeholder organizations as new reports come in. CCIRC is also working with the Canadian Internet Registration Authority (CIRA) to provide notifications to affected users.

Operation Ghostclick was worldwide fraud campaign, exposed in late 2011 by the FBI. Cyber criminals hijacked users' Internet web searches and diverted them to websites that generated advertising and sales revenues. Computers across multiple sectors, in organizations large and small, and those belonging to the general public have been affected.

> ***Comment:*** *Organizations should ensure they have taken the mitigation measures outlined in CCIRC's Information Note. CCIRC noted that the type and size of affected organizations varied, and were spread across Canada. The number of affected telecommunications companies more than likely indicates number of infected client computers of Internet via Service Providers. These Internet Service Providers receive information from CCIRC.*
>
> *Organizations that offer Internet access, including those that provide publically accessible wireless networks, may be particularly vulnerable. In addition to the cooperative effort underway between CCIRC and CIRA, the Canadian government has launched a website for cyber security public education..*

CCIRC PRODUCTS RELEASED:

Hacktivist attacks related to proposed anti-piracy legislation. There have been coordinated distributed denial-of-service (DDoS) attacks on websites by hacktivists, claiming to be associated with Anonymous. There were multiple international targets, which included governments (Canada, US, Poland, Ireland and EU) and entertainment industry organizations associated with U.S. copyrights regulatory efforts: Stop Online Piracy Act (SOPA), Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) and Anti-Counterfeiting Trade Agreement (ACTA).

In response, CCIRC issued Cyber Flash CF12-001, titled *"Hacktivist Group Anonymous - DDoS Activity Related to Copyrights and Intellectual Property"*. This Cyber Flash, was sent to technical and security contacts within stakeholder organizations in government and other critical infrastructure

sectors . Government and industry organizations involved with the Copyright legislation and copyrighted material were encouraged to assess their risk exposure to coordinated DDoS attacks on their networks.

NOTEWORTHY NEWS IN THE MEDIA:

Israeli and pro-Palestinian hackers exchange website attacks. Open sources reported that the websites of Israel's main stock exchange, several banks and the national airline were attacked. Pro-Palestinian hackers claimed responsibility and even claimed to have posted the login credentials for several industrial control systems in Israel on the Internet. Shortly thereafter, there were reports of suspected Israeli hackers bringing down the Saudi Stock Exchange, interfering with the Abu Dhabi Security Exchange, and publishing e-mail addresses & passwords of 30,000 Arab Facebook users.

Comment: *It is now becoming commonplace to carry real-world grievances into the cyber world. There could be an adverse impact from these attacks for Canadians and Canadian businesses that do business with the stock exchanges or banks involved. There were some media reports that some of the Israeli banks could block international access to their sites.*

Hackers around the world attack government websites to protest anti-piracy measures.

- **Retaliation for file-sharing service Mega Upload's shutdown:** Hackers, claiming to be with Anonymous, attacked the websites of the FBI, Department of Justice, Universal Music Group, RIAA, Motion Picture Association of America and Warner Music.

- **Signing of the international Anti-Counterfeiting Agreement (ACTA) and proposed US copyright laws:** Wikipedia shut down for one day to protest the proposed SOPA and PIPA bills. SOPA and PIPA were also cited by Anonymous as a reason for their attacks on the DOJ and FBI websites. Operation STOP ACTA by Anonymous also prompted hacker attacks on websites for US, Poland, Ireland governments as well as for the European Parliament.

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Ken Bendelier, CCIRC Acting Strategic Program Manager, at kenneth.bendelier@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

OUR ORGANIZATION

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

REPORTING CYBER INCIDENTS

Canadian Critical Infrastructure Operators wishing to report incidents may send associated email report to the Government Operations Centre, using the CCIRC Cyber Duty Officer PGP encryption key, found here: (http://www.publicsafety.gc.ca/prg/em/ccirc/enc-eng.aspx).

CCIRC PRODUCTS

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

The day the web went dark - U.S. anti-piracy bills spark outrage online
The Issue: Many of the Internet's most-used websites went dark on Wednesday to protest the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA), anti-piracy bills currently wending their way through U.S. Congress. The protest appeared to work with impressive efficiency - many proponents withdrew support for the bills, seen as deeply flawed. While Google's dramatic blacked-out logo was visible only to U.S. users, the self-imposed disabling of major sites such as Wikipedia affected users worldwide, including Canadians. Toronto Star, IN2; Charlottetown Guardian (Red Deer Advocate; Winnipeg Free Press)

SOPA blackouts: Free speech or 'abuse of power'?
The unprecedented wave of "blackouts" and other forms of protest that swept the web on Wednesday was designed to call attention to legislation that critics contend will stifle free speech. But the dramatic move sparked debate over whether the protest itself was appropriate for websites that are often themselves arbiters of free speech online. .. **FULL ARTICLE**

CCIRC is monitoring a recent post by the hacktisvist group "Anonymous" on pastebin referred to Operation SACTA (Stop Anti-Counterfeiting Trade Agreement)

(http://pastebin.com/5S3k090H)

This post refers to two a Federal Department Sites:

http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=eng&view=d
http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/intellect_property.aspx?view=d

DETAILS

These sites identify the following Canadian and international stakeholders:

- Canadian Intellectual Property Office
- Industry Canada's Intellectual Property Policy Information Page
- Canadian Heritage - Copyright Policy
- World Intellectual Property Organization (WIPO) Treaties
- World Trade Organization (WTO) – TRIPS

The post is encouraging supporters to:

1) "Spread the word! (twitter, piratepad, pastebit, WWP, flyers, you name it!)"
2) "mail the s**t out of your government demanding that ACTA is to be put away."
3) "Attack if necessary."
4)"???????????"
5)"Profit."

CCIRC has already observed reports of Anti-ACTA hackers attacking other websites such as Polish Government websites.
Reference: http://www.siliconrepublic.com/strategy/item/25451-anti-acta-hackers-attack-po

CURRENT ACTION

This information was provided to GC-CTEC for their action and mitigation of federal government stakeholders. CCIRC is actively monitoring the situation.

Des pirates s'en prennent au FBI
La fermeture jeudi par les États-Unis du site de téléchargement Megaupload a entraîné depuis 48 heures une série de contre-attaques de pirates informatiques. Le Federal Bureau of Investigation (FBI), le ministère de la Justice et le palais présidentiel français ont tous été touchés par le mouvement Anonymous. Hier, la police néo-zélandaise a procédé à l'arrestation de quatre personnes reliées au site de partages de fichiers Megaupload. Kim Dotcom (de son vrai nom Kim Schmitz), l'ancien président et chef de la direction de Megaupload, fait partie des suspects arrêtés. Avec 150 millions d'utilisateurs et 50 millions de téléchargements chaque jour, Megaupload trônait parmi les sites les plus achalandés. Mais son contenu - musique, films, séries télé - était jugé illégal et violait les droits d'auteur. Le Soleil, 24; Victoria Times-Colonist; Toronto Star; National Post; Montreal Gazette; Le Devoir

Megaupload et Anonymous
Megaupload était l'un des sites de partage de fichiers les plus notoires au monde avec 150 millions d'utilisateurs. Son fondateur, Kim Dotcom, avait gagné 42 millions $US l'an dernier. Pour l'industrie cinématographique, le site fonctionnait avec des fichiers piratés. Le site a été fermé jeudi et est accusé d'avoir facilité le téléchargement illégal de plusieurs millions de fichiers, violant les droits de leurs auteurs. Le groupe de pirates informatiques Anonymous se présente comme un défenseur des libertés sur Internet. Le blocage de ces sites est la dernière cyberattaque d'Anonymous, un groupe de pirates disséminés dans le monde entier et représentés par un masque blanc et noir au sourire sarcastique, qui s'en est déjà pris à l'Église de scientologie ou au ministère de la Défense syrien. Le Soleil, 25

Hacktivist group Anonymous hacked into the US' Department of Justice website to protest the FBI's shut down of Megaupload, a popular peer-sharing (read: pirated content) site. The DoJ's site remained down for several hours, and the hacker group promised to be back with more attacks to demonstrate their position against SOPA.

Google Expands Hacked Sites Label In Search Results
A year ago, Google began labeling hacked sites and sites with malware as sites that may compromised in the search results snippets. Yesterday, Google's Matt Cutts announced on Google+ that Google has expanded that feature. Matt said the change they just launched will "expand our [Google's] coverage of labeling search result pages." Search Engine Roundtable

Spammers target childrens' games
With adults wising up to the dangers of clicking unknown links, spammers are increasingly targeting children. Anti-virus firm Avast says it's identified more than 60 individual sites during the last month containing 'game' or 'arcade' in their URL address, all aimed squarely at children. The most visited site was cutearcade.com, a collection of online games with dressing up and coloring games - and even Hello Kitty. Avast says its users have reported an infection at this site over 12,600 times. The malicious Trojan redirects viewers to linuxstabs.com, a known distribution point for malware. TG Daily

Suspicion grows China was behind hack of U.S. commission
Suspicion is growing that operatives in China, rather than India, were behind the hacking of emails of an official U.S. commission that monitors relations between the United States and China, U.S. officials said. News of the hacking of the U.S.-China Economic and Security Review Commission surfaced earlier this month when an amateur "hacktivist" group purporting to operate in India published what it said was a memo from an Indian Military Intelligence unit to which extracts from commission emails were attached. Reuters

Anonymous hacks FTC website OnGuardOnline.gov

By **Alice Lipowicz**
Jan 24, 2012

The online collective Anonymous on Jan. 24 claimed credit for hacking a Federal Trade Commission website aimed at helping consumers with cybersecurity advice, OnGuardOnline.gov.

The website is managed by the FTC and hosted in partnership with several federal agencies. The consumer protection agency reported the hack publicly on Twitter and Facebook and has taken the website offline for assessment and repairs.

Early on Jan. 24, the hacking group initially replaced the OnGuardOnline website's front page with its own logo, according to an **article** in TheNextWeb.com.

New stealthy botnet Trojan holds Facebook users hostage
A new strain of cybercrime Trojan is targeting Facebook users by taking over their machines and shaking them down for cash. Carberp, like its predecessors ZeuS and SpyEye, infects machines by tricking punters into opening PDFs and Excel documents loaded with malicious code, or attacks computers in drive-by downloads. The hidden malware is designed to steal account information, and harvest credentials for email and social-networking sites. A new configuration of the Carberp Trojan targets Facebook users to ultimately steal e-cash vouchers. Previous malware attacks on Facebook have been designed purely to slurp login info, so this latest skirmish, spotted by transaction security firm Trusteer, can be considered something of an escalation. The Carberp variant replaces any Facebook page the user navigates to with a fake page notifying the victim that their Facebook account is temporarily locked. Effectively holding Facebook users hostage, the page asks the mark for their first name, last name, email, date of birth, password and a Ukash 20 euro ($25) voucher number to verify their identity and unlock the account. Trusteer warns the cash voucher attack is in some ways worse than credit card fraud, because with e-cash it is the account-holder, not the financial institution, who assumes the liability for fraudulent transactions. The Register; Techworld

Malware targets smart ID cards, say researchers
Cybersecurity researchers say they've uncovered a variant of malicious software known as Sykipot that specifically targets smart identity cards used by a number of federal agencies, including the departments of Defense and Homeland Security. In a July 12 blog post, researchers from alienvault labs say the variant appears to have been compiled in March 2011. Once downloaded onto a computer via a phishing attack (in which an email containing an infected attachment or link to a malware-controlled website appears to originate from a legitimate source), the Sykipot variant uses a keylogger to steal PINs users enter to authenticate their identity, the Campbell, Calif.-based company says. Fierce Homeland Security

1. Israel/Palestinian "Cyber War"

http://tech.slashdot.org/story/12/01/17/1846258/israel-faces-escalating-cyberwar

Description:
"The NY Times describes what may be the beginning of an actual cyberwar between a pro-Palestinian group and Israeli companies, specifically El Al and the Tel Aviv stock exchange. From the article: 'A hacker identifying himself as oxOmar, already notorious for posting the details of more than 20,000 Israeli credit cards, sent an overnight warning to Israel's Ynet news outlet that a group of pro-Palestinian cyberattackers called Nightmare planned to bring down the sites in the morning.' Though the article is skimpy on technical details, the group appears to have engaged merely in a DDOS attack. Hamas praised the attack as opening 'a new resistance front against Israel.' Is this the first acknowledged cyberwar?"

http://www.haaretz.com/news/diplomacy-defense/israeli-hackers-bring-down-saudi-uae-stock-exchange-websites-1.407846

Description:
Israeli hackers brought down the websites of both the Saudi Stock Exchange (Tadawul) and the Abu Dhabi Securities Exchange (ADX) Monday, in the latest episode of a continuing cyber war between hackers in the two countries.

The Israeli hackers, who go by the name IDF-Team, were able to paralyze the Tadawul website, while causing significant delays to the ADX exchange site.

The hackers wrote that the attack came in response to the pathetic hacking of Israeli sites on Monday. The hackers warned that if the attacks continue, they will move to the next stage and paralyze websites for a period of two weeks to a month.

Earlier Tuesday, a pro-Israel hacker published a list of 30,000 e-mail addresses and Facebook passwords of "helpless Arabs" on a popular hacking site. The hacker, who goes by Hannibal, wrote that his actions - which began Friday - are a "counter-attack" following the publication of Israeli credit card details on the Internet by a reportedly Saudi hacker.

http://arstechnica.com/business/news/2012/01/israeli-and-palestinian-hackers-trade-ddos-attacks-in-rising-cyber-gang-war.ars

Description:
Pro-Palestinian and pro-Israeli hackers are waging a cyber street-fight in a tit-for-tat exchange of posturing, threats of mass credit card exposures, and denial-of-service attacks. As Hamas has egged on hackers in recent weeks, promoting more "hacktivist" attacks against Israeli targets, pro-Israel hackers have responded in kind, today taking down the websites of stock exchanges in Saudi Arabia and the United Arab Emirates. Both sites appear to be back online.

Those site takedowns are in response to denial of service attacks yesterday (January 16) and today against the websites of the Tel Aviv Stock Exchange, First International Bank of Israel, the Israeli national airline El Al, and at least two other Israeli businesses. While El Al's and FIBI's sites have been restored, the TASE site remains unavailable. The attacks are allegedly the work of pro-Palestinian hackers, including one hacker going by the name of OxOmar claiming to be from Saudi Arabia assisted by a team calling itself "Nightmare."

http://news.cnet.com/8301-27080_3-57360584-245/middle-east-cyberwar-hits-israeli-banks-stock-exchange-airline/

Description:
Hackers in Israel and other Middle Eastern countries are in the middle of a cyberwar that has led to disruptions of the Tel Aviv Stock Exchange, several Israeli banks, and an airline. As a result, some Israeli banks have blocked or are threatening to block international access to their sites to avoid attack.

No one has claimed responsibility for the attacks Monday that crippled the Web sites of the Tel Aviv bourse Web site and El Al Airlines, as well as the marketing sites of the First International

Bank of Israel (Fibi), Massad bank, and Otzar Hahayal bank, according to Reuters. Stock trading and flights were uninterrupted, as were online services for bank customers, the report said. The Tel Aviv Stock Exchange site was not accessible this afternoon from the United States.

Israël: des pirates affirment avoir touché le site de la bourse saoudienne
Un groupe de pirates informatiques israéliens a affirmé mardi s'être introduit sur les sites des bourses de Ryad et d'Abou Dhabi, pour répliquer à des cyberattaques lancées la veille contre plusieurs sites israéliens, ont rapporté des médias israéliens. La Presse; Arutz Sheva; Financial Times

Saudis deny stock exchange website infiltrated by Israeli hackers
Saudi Arabian authorities on Wednesday denied claims that Israeli hackers had crippled the website of the oil-rich country's capital market, saying the system was operating normally. Israeli hackers claimed they brought down the websites of both the Saudi Stock Exchange (Tadawul) and the Abu Dhabi Securities Exchange (ADX) on Tuesday, in the latest episode of a continuing cyber war between hackers in Israel and other countries. The Israeli hackers, who go by the name IDF-Team, said on Tuesday they were able to paralyze the Tadawul website, while causing significant delays to the ADX exchange site. Haaretz

Scammers Utilize Leaked Mailing ids from Stratfor for 'Phishing' Customers
CEO George Friedman of Stratfor cautioned customers who had their e-mail ids exposed on the Net that a fraudulent, phishing e-mail was circulating while trying to steal confidential client database, published DAILY CALLER on January 6, 2012. Claiming as a declaration by Friedman, the fake e-mail refers to updated services of Stratfor such as making obtainable the company's premium content at zero cost as availability of the services had become inconvenient. SPAMfighter

---

CCIRC ADVISORY
****

Number: AV12-003

Date: 19 Jan 2012

****

Oracle Critical Patch Updates - January 2012
****

PURPOSE

The purpose of this advisory is to bring attention to the following critical patch updates for Oracle products.

ASSESSMENT

Oracle has released its quarterly security update, which addresses 78 vulnerabilities affecting many of their products. Several of these vulnerabilities can be exploited remotely without authentication.

Affected products include:

Oracle Database 11g Release 2, versions 11.2.0.2, 11.2.0.3 Oracle Database 11g Release 1, version 11.1.0.7 Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4, 10.2.0.5 Oracle Database 10g Release 1, version 10.1.0.5 Oracle Fusion Middleware 11g Release 1, versions 11.1.1.3.0, 11.1.1.4.0, 11.1.1.5.0 Oracle Application Server 10g Release 3, version 10.1.3.5.0 Oracle Outside In Technology, versions 8.3.5, 8.3.7 Oracle WebLogic Server, versions 9.2.4, 10.0.2, 11gR1 (10.3.3, 10.3.4, 10.3.5) Oracle E-Business Suite Release 12, versions 12.1.2, 12.1.3 Oracle E-Business Suite Release 11i, version 11.5.10.2 Oracle Transportation Management, versions 5.5, 6.0, 6.1, 6.2 Oracle PeopleSoft Enterprise CRM, version 8.9 Oracle PeopleSoft Enterprise HCM, versions 8.9, 9.0, 9.1 Oracle PeopleSoft Enterprise PeopleTools, version 8.52 Oracle JDEdwards, version 8.98 Oracle Sun Product Suite Oracle VM VirtualBox, version 4.1 Oracle Virtual Desktop Infrastructure, version 3.2 Oracle MySQL Server, versions 5.0, 5.1, 5.5

POTENTIAL HEADLINES FOR WEEKLY SUMMARY FOR WEEK OF DEC 5, 2011

Item Description: **Draft Bill Eyes Strong DHS Role in Cybersecurity.** "Draft legislation that proposes the establishment of a so-called National Information Sharing Organization will be the subject of a hearing to be held Tuesday by the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies. The not-for-profit National Information Sharing Organization would share cyber-threat information among various government and private-sector constituencies and would consist of representatives from federal, state and local governments, businesses representing the nation's critical infrastructure as well as from seven specific sectors - including banking and healthcare - and the privacy and civil liberties communities."

- Reference: http://www.govinfosecurity.com/articles.php?art_id=4303&rf=2011-12-06-eg&elq=334c15c7561c4564874cdae4b975215c&elqCampaignId=919
  Rana's comment: We reported on a competing Bill last week that got endorsed by the U.S. House Intelligence Panel. This one is more "privacy friendly". Canadian nexus is that Canada is studying policy gaps in cyber security in Canada and could get ideas from US. In addition, given Canadians use some of the US internet infrastructure (and things like gmail, Hotmail, etc), Canadians have an interest in how US telcos will be sharing their customer information with US authorities...

New cyber info-sharing measure gets nod from privacy proponents
BY ALIYA STERNSTEIN 12/06/2011

This story was updated to include comments from a House Intelligence Committee staff member.

A House Homeland Security Committee draft bill that would create a nonprofit entity to share information on cyber threats has gained favor with some privacy advocates who are concerned that a competing bill already passed by the House Intelligence Committee will feed personal information to the government.

The proposed National Information Sharing Organization, or NISO, would be guided by a board of directors composed of two privacy advocates and 10 representatives from critical infrastructure sectors, including the banking, communications, defense contracting, energy and health care industries. Only four federal officials would sit on the board. Most expenses, at least 85 percent, would be paid by member companies. The board would set rules for privacy protections, handling of intellectual property and limitations on liability. And the bill would legitimize the Homeland Security Department as the lead government agency for coordinating with the private sector on reinforcing critical infrastructure networks rather than the Defense Department or intelligence agencies.

For these reasons, the Center for Democracy and Technology, a civil liberties group, says the information sharing stipulations in the draft are superior to those in H.R. 3523, which, CDT says, would allow Internet service providers to share private communications with the government.

http://www.nextgov.com/nextgov/ng_20111206_5033.php?oref=rss?zone=NGpopular

---

- **New legislation has come into force to protect children from online sexual exploitation.** Bill C-22, which took effect Thursday, makes it mandatory for Internet service providers to report online child pornography. Prior to the bill, Internet providers didn't have to monitor what their clients were doing. The legislation applies to suppliers

of Internet services to the public, electronic mail services and social networking sites. London Free Press, B1 s.16(2)(c)

Rana's comment: Not really a cyber security issue, in many people's opinions wasn't legally necessary, but it is a new Canadian legislation re internet.

Cyber attacks could wreck world oil supply

Hackers are bombarding the world's computer controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil supply disruption. Oil company executives warned that attacks were becoming more frequent and more carefully planned. Computers control nearly all the world's energy production and distribution in systems that are increasingly vulnerable to cyber attacks that could put cutting-edge fuel production technology in rival company hands. Luehmann said hackers were increasingly staging attack over long periods, silently collecting information over weeks or months before attacking specific targets within company operations with the information they have collected over a long period. Chicago Tribune

Agencies, contractors get rules of the road for cloud security approvals

BY ALIYA STERNSTEIN 12/08/2011

US Federal cloud providers by June 2012 will have to comply with new uniform security controls so that multiple agencies can piggyback off the certifications for faster installation, White House officials announced Thursday.

To more quickly slice $5 billion from the government's annual $80 billion information technology tab, the Obama administration has released requirements for expediting cloud security approvals. Protecting data in the cloud -- or remote storage and software accessible online --
http://www.nextgov.com/nextgov/ng_20111208_9699.php?oref=rss?zone=NGtoday

Rana's comment: This item would be of interest to potential Canadian suppliers to the US govt, and govt officials in Canada who are considering a move to the cloud, or have heard of it

. Item Description: **Feds launch cloud security standards program.** "Federal agencies will soon have a government-wide security standard for assessing, authorizing and monitoring cloud products and services. The Federal Chief Information Officer December 8 unveiled the Federal Risk and Authorization Management Program (FedRAMP), which establishes a set of baseline security and privacy standards all cloud service providers will need to meet to sell their products to government agencies. The program requires that all agencies use only FedRAMP-certified cloud services and technologies for public clouds, private clouds, hybrid clouds, and community clouds. The program also covers all cloud service models, including Software as a Service (SaaS) and Platform as a Service (PaaS). FedRAMP will also provide federal agencies with standard procurement language to use in requests for proposals from cloud service vendors. A Joint Authorization Board, comprising of security experts from the DHS, General Services Administration, and the Department of Defense will be responsible for updating the FedRAMP security requirements on an ongoing basis. A group of third-party assessors hired from the private sector will be responsible for independently assessing cloud service providers and certifying their compliance with the standards."
Reference:
http://www.computerworld.com/s/article/9222525/Feds_launch_cloud_security_standards_program?taxonomyId=17

For the Analysis of article above:

If you think you'll save money with cloud computing, think again (NextGov) BY JOSEPH MARKS 12/06/2011

More than half of organizational users saved little or no money after transitioning to cloud computing, according to a new study, and only 14 percent actually downsized their information technology departments after moving to the cloud....Computer clouds are essentially large banks of off-site computer servers that can pack data more tightly than traditional servers and move that data more nimbly as one customer surges in use and another declines.

.....According to the CSC study, accessing data and programs on multiple devices was the most popular reason for corporate and public sector users to move to the cloud, accounting for about one-third of all transitions.

6. Item Description: **Resurgent LulzSec Attacks Government Sites In Portugal.** "The hacktivist group LulzSec was back in action last week, launching distributed denial-of-service (DDoS) attacks on government websites in Portugal. The group says it was driven to the attacks by Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest on Nov. 24, according to news reports. On Friday, LulzSec Portugal launched a DDoS attack against the website of Banco de Portugal (Bank of Portugal), making the site inaccessible, according to the reports. In addition to taking down the Bank of Portugal website, LulzSec Portugal has been credited with successful attacks on numerous state services. Earlier this week, LulzSec disabled the websites of the Portugal House of Parliament, several political parties, and the national police."
Reference: http://www.darkreading.com/security/attacks-breaches/232300133/resurgent-lulzsec-attacks-government-sites-in-portugal.html

1. Portuguese Under Massive Cyber Attack From Lulzsec
   http://www.voiceofgreyhat.com/2011/12/portuguese-under-massive-cyber-attack.html

International hackers Anonymous shut down Colombian Army website
http://colombiareports.com/colombia-news/news/20878-anonymous-hacks-colombian-army-website-video.html

Rana's comment: Anonymous has threatened Canadian interests before (but at least in 2011, nothing happened that I recall). However, these incidents confirm LulzSec and Anonymous have the capability to launch a DDoS and disable government websites...

Microsoft to fix Duqu virus
Microsoft Corp said it will release a security update to protect personal computers from getting attacked by Duqu, a mysterious virus that researchers suspect was built by the same group behind Stuxnet. Times of India

Duqu Perpetrators Remove Clues of C&C Servers, Following Exposure
According to security researchers from Kaspersky Lab, soon after Symantec the security company hyped the Duqu Trojan on the Internet during October 2011, those secretly unleashing the data-stealing malicious program eliminated all evidences of their existence off the command-and-control servers they operated for hiding their tracks. SPAM Fighter

---

Symantec confirms Flash exploits targeted defense companies. "Security researchers at Symantec confirmed December 7 that exploits of an unpatched Adobe Reader vulnerability

targeted defense contractors, among other businesses. "We've seen [this targeting] people at telecommunications, manufacturing, computer hardware and chemical companies, as well as those in the defense sector," said a senior security manager in Symantec's security response group. Symantec mined its global network of honeypots and security detectors — and located e-mail messages with attached malicious PDF documents — to reach that conclusion. Adobe warned Reader and Acrobat users hackers were exploiting a "zero-day" bug on Windows PCs December 6, crediting Lockheed Martin's security response team and the Defense Security Information Exchange (DSIE), a group of major defense contractors that share information about computer attacks, with reporting the vulnerability.
Reference:
http://www.computerworld.com/s/article/9222496/Symantec_confirms_Flash_exploits_targeted_defense_companies?taxonomyId=17

TRENDS – here in the Weekly or in a Monthly?

- **Cyber crime going mobile**
  Cybercrimes are becoming more mobile. As more smartphones and tablets are being used, cyber thieves aren't just targeting personal computers to steal information for financial gain, say antivirus security experts. Young men between the ages of 18 and 31 are targets because of the large amount of time they spend online every week, said Hargrove, director of consumer solutions for Symantec Inc. Known as the "millennium males," they spend more than 49 hours online a week, she said. Mobile malware is on the rise, especially with the Android devices, said Doug Cooke, director of sales engineering at McAfee Canada. Red Deer Advocate, C5

Information Security Forum predicts 'perfect storm' with 2012 security challenges
With 2011 coming to an end, security threats show no sign of slowing down. This is according to independent information security body, the Information Security Forum (ISF). ISF's top three security challenges for 2012… 1. Consumerisation of IT… 2. Cyber (in) security … Converging threats. Information Security Forum News Release

Imperva predicts top nine cyber security trends for 2012
The rise in so-called big data and application DDoS (distributed denial of service) attacks are among concerns for the foreseeable future, according to data security specialist Imperva, which has issued a top nine cyber security trends for 2012. Number one is an assertion that security will finally trump compliance – reversing the traditional position. Imperva believes that more companies will make cyber security decisions based on security, rather than regulations, such as PCI and SOX. Imperva's number two is the rise of 'cyber brokers', as a result of an increasing supply and demand for compromised machines, as well as for sensitive corporate information. Such individuals will match the buyers of stolen data or compromised machines (bots) with sellers. Works Management

Employees' Droids among biggest government cyber menaces
BY ALIYA STERNSTEIN 11/15/2011

In 2012, agencies should worry about hackers attacking the growing number of federal employees toting their own iPhones and Droids to work, according to a forecast of next year's greatest cyber dangers compiled by M86 Security Labs.

On Tuesday, the network security firm is expected to release its annual predictions of the top computer threats to business and government organizations. At federal agencies, the biggest targets are likely to be employee-owned devices, a department's own public website and cloud services.

"The Android is very much a victim of its own success" because any developer can publish innovative -- or malicious -- software applications to Google's Android Market, Bradley Anstis, M86 vice president for technical strategy, said in an interview. Apple is more selective in vetting programs for its App Store. Most government agencies that M86 works with, including NASA, have a bring-your-own-device policy, he said.

http://www.nextgov.com/nextgov/ng_20111115_9168.php?oref=rss?zone=NGhealthit

Symantec: spam nearing three-year low, targeted attacks on the rise
E-mail spam across the world is close to a three-year low, now accounting for 70.5 percent of all messages sent. That may sound like a lot until you consider that 90 percent of e-mail sent in 2009 was spam, according to Symantec's November Intelligence Report. The 25 page report also highlights that one in 302 e-mails was identified as a phishing attempt and one in 255.8 messages contained malware. Most alarming, however, is that nearly 5,000 malicious websites are blocked each day, an increase of 47.8 percent since October 2011. Symantec reports that Russia was the most spammed region in November at 76.7 percent, followed closely by Saudi Arabia at 76.6 percent and China at 74.5 percent. The US had a 69.9 percent spam rate while Canada was slightly better at 69.5 percent. TechSpot

. Item Description: **Anonymous hacks Monsanto PR firm Bivings Group.** "Tango down: Operation End Monsanto claims first victim. The Bivings Group, a public relations firm associated with Monsanto, has been permanently shut down after a devastating attack by those claiming to represent the nebulous and notorious international Internet hacktivist collective known as Anonymous. According to the Anonymous hacktivists, The Bivings Group website was defaced, their database was hacked and dumped, hundreds of emails were stolen and are now viewable, and a database of Monsanto documents were acquired."
Reference: http://www.examiner.com/anonymous-in-national/anonymous-hacks-monsanto-pr-firm-bivings-group
http://pastebin.com/UZTcLMGT

Anonymous attacks Mexican Government (Operation SafeRoads)

On Saturday, December 10, a global cadre of Anonymous hacktivists launched a number of successful strikes against numerous Mexican transportation and government websites, protesting the dangerous travelling conditions present in Mexico.
Government agencies and bus companies were targeted for being complicit in allowing the dangerous traveling conditions in Mexico to exist. At least a dozen Mexican institutional portals, among them the Federal Roads and Bridges Access and Related Services, as well as several natioal bus companies, were the subject of Anonymous cyber attacks.
Websites were taken down via well orchestrated DDoS (distributed denial of service) attacks as well as defaced by Anonymous hacktivists. For an accounting of the many strikes, with links of verification, go to Blog.AtHack.Net and/or el5antuario.org

5. Item Description: **Information: Threat Trends in 2011 - The Signals and the Noise**.
Reference http://regmedia.co.uk/2011/11/29/jwalter_mcafee_labs_threatbrief112011_v3.pdf

Canada sorely lacking cyber security: report
Canada has fallen short in protecting its critical infrastructure from a whole host of risks, says a new report published by public policy think-tank Macdonald- Laurier Institute. Report author and Queen's University professor Andrew Graham says computer hacking traced back to China shows Canada's cyber-security needs, especially, are "mushrooming." Some action has already taken place on the issue through **Public Safety Canada's** cyber-security strategy. Meanwhile,

Colin Robertson of the Canadian Defence and Foreign Affairs Institute, another think-tank, expects to see a new North American perimeter security agreement take things further. Edmonton Sun, 75

Rana's Comment: This was in the Daily Media, and Martin e-mailed us the report. The actual report really takes aim at the whole of CI and cyber attack is identified as a risk that needs to be addressed. But the report is far less alarming and sensationalist than the headlines – honestly nothing really new or earth shattering from my perspective. Should we report?

Ultimate Bet Players Accounts Compromised, 3.5 Million Records Freely Available Online For Weeks Still In Google Cache

In a breach of security at Ultimate Bet, information from every player's account had been publicly posted on the internet, revealing personal information of approximately 3.5 million poker players holding accounts at the nearly-dead poker site.

A popular poker forum website posted a link to the account information via an anonymous posting, but removed the link roughly eight minutes later. In that short span of time, enough people identified the link and apparently passed the information around privately.

The data leaked from the accounts included each player's name and screen name; birth date; email, mailing and IP addresses; phone number; deposit methods typically used; VIP, affiliate and blacklist statuses; account balance; and players' UB account numbers, but not bank account numbers as far as we know.

part of doc - not a redaction

The data listed was organized by specific countries, with about 2 million accounts from the U.S., 319,000 Canadian accounts, 137,000 United Kingdom accounts, and approximately 1 million accounts from all other countries combined.

Hackers mock RIM's patch efforts

- Hackers say they are a step ahead of Research In Motion's efforts to plug a security breach in the PlayBook tablet computer. Chris Wade, one of three researchers who gained authorized access to the "root" control system of RIM's first QNX device last month, said in a tweet this week that he had found a workaround only hours after RIM issued a security patch. Wade said the beta DingleBerry tool the group had developed and released on Twitter has been updated and is exploiting a second vulnerability in the PlayBook OS, software the company has called bulletproof and that RIM plans to roll out to its new smartphones next year. He said the workaround lets Windows users to load custom operating systems and apps from their desktop PC onto the PlayBook, activating features not permitted by the manufacturer. Toronto Star, B4

Dutch certificate authority reportedly hacked after access gained through PHP MyAdmin

Another Dutch certificate authority (CA) has been hacked with access gained to a management database and documents. According to a story on the Dutch news site Webwereld, Gemnet was compromised, although this does not appear to have affected certificate issuance. A provider of security consultancy and authentication technologies to nearly all parts of the Dutch government, including the Ministry of Security and Justice, Bank of Dutch Municipalities and the police, the company reportedly detected and closed the leak on Wednesday. The report claimed that the database was managed by PHP MyAdmin and access was gained without a password. The attacker was able to extract information from the database and partially control the network; among the documents was information about the technical design of the trusted network between Dutch telecommunications and ICT service provider KPN and governments or companies. SC Magazine UK

5. Item Description: **Site of Dutch CA Gemnet Offline After Web Server Attack.** "Another certificate authority in The Netherlands has been hacked, though this time the attack does not appear to have affected the certificate-issuing operations of Gemnet, a subsidiary of KPN. The company, which does business with the Dutch government among other organizations, said it has taken its Web site offline while it investigates the attack. The attack came to light Wednesday, and while the details are limited at this point, the company said that the attackers went after the public Web site and were able to compromise the server and access some private data and documents stored on the back-end database. Gemnet is owned by KPN, a large Dutch telecom and Internet company. "The hack of the site has no connection with the issuance and management of Government PKI certificates. The general website Gemnet (www.gemnet.nl) since Wednesday December 7 temporarily not accessible to visitors. The website, part of KPN, by Internet journalist Brenno de Winter Wednesday afternoon reported a possible hack. The hack would be performed on the server: the server that the general visitor information visible. KPN was immediately launched an investigation into possible causes and origins," a translation of a KPN press statement says in part."
Reference: http://blogs.technet.com/b/mmpc/archive/2011/12/09/backdoor-win32-fynloski-a-a-short-history-of-abuse.aspx

Item Description: **Australian Defence Signals Directorate's (DSD) Finds 4 Controls Stop Targeted Intrusions.** "In October, the Australian Defence Signals Directorate received a US national Cybersecurity Innovation Award for identifying and implementing (across the Australian civilian and military agencies) four security controls that could defeat more than 85 percent of targeted cyber intrusions. The four controls top a list of 35 strategies, but unlike any other government initiative, the Australians say "do the top 4 controls first" and then decide which of the other controls to implement. This is the first strategy for mitigating targeted attacks that resonates with top executives inside and outside government. The DSD just published new documents explaining exactly how to implement the four controls in the "Sweet Spot."

Reference: http://www.dsd.gov.au/publications/Implementing_Top_4_for_Windows.pdf
http://www.dsd.gov.au/publications/Assessing_Security_Vulnerabilities_and_Patches.pdf
https://www.sans.org/press/australian-defence-signals-directorate-national-cybersecurity-award.php

Rana's comment: I heard CSEC is doing something similar to this

POTENTIAL HEADLINES FOR WEEKLY SUMMARY FOR WEEK OF DEC 5, 2011

Item Description: **Draft Bill Eyes Strong DHS Role in Cybersecurity.** "Draft legislation that proposes the establishment of a so-called National Information Sharing Organization will be the subject of a hearing to be held Tuesday by the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies. The not-for-profit National Information Sharing Organization would share cyber-threat information among various government and private-sector constituencies and would consist of representatives from federal, state and local governments, businesses representing the nation's critical infrastructure as well as from seven specific sectors - including banking and healthcare - and the privacy and civil liberties communities."

- Reference: http://www.govinfosecurity.com/articles.php?art_id=4303&rf=2011-12-06-eg&elq=334c15c7561c4564874cdae4b975215c&elqCampaignId=919
  Rana's comment: We reported on a competing Bill last week that got endorsed by the U.S. House Intelligence Panel. This one is more "privacy friendly". Canadian nexus is that Canada is studying policy gaps in cyber security in Canada and could get ideas from US. In addition, given Canadians use some of the US internet infrastructure (and things like gmail, Hotmail, etc), Canadians have an interest in how US telcos will be sharing their customer information with US authorities...

New cyber info-sharing measure gets nod from privacy proponents
BY ALIYA STERNSTEIN 12/06/2011

This story was updated to include comments from a House Intelligence Committee staff member.

A House Homeland Security Committee draft bill that would create a nonprofit entity to share information on cyber threats has gained favor with some privacy advocates who are concerned that a competing bill already passed by the House Intelligence Committee will feed personal information to the government.

The proposed National Information Sharing Organization, or NISO, would be guided by a board of directors composed of two privacy advocates and 10 representatives from critical infrastructure sectors, including the banking, communications, defense contracting, energy and health care industries. Only four federal officials would sit on the board. Most expenses, at least 85 percent, would be paid by member companies. The board would set rules for privacy protections, handling of intellectual property and limitations on liability. And the bill would legitimize the Homeland Security Department as the lead government agency for coordinating with the private sector on reinforcing critical infrastructure networks rather than the Defense Department or intelligence agencies.

For these reasons, the Center for Democracy and Technology, a civil liberties group, says the information sharing stipulations in the draft are superior to those in H.R. 3523, which, CDT says, would allow Internet service providers to share private communications with the government.

http://www.nextgov.com/nextgov/ng_20111206_5033.php?oref=rss?zone=NGpopular

---

- **New legislation has come into force to protect children from online sexual exploitation.** Bill C-22, which took effect Thursday, makes it mandatory for Internet service providers to report online child pornography. Prior to the bill, Internet providers didn't have to monitor what their clients were doing. The legislation applies to suppliers

of Internet services to the public, electronic mail services and social networking sites. London Free Press, B1
Rana's comment: Not really a cyber security issue, in many people's opinions wasn't legally necessary, but it is a new Canadian legislation re internet.

Cyber attacks could wreck world oil supply
Hackers are bombarding the world's computer controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil supply disruption. Oil company executives warned that attacks were becoming more frequent and more carefully planned. Computers control nearly all the world's energy production and distribution in systems that are increasingly vulnerable to cyber attacks that could put cutting-edge fuel production technology in rival company hands. Luehmann said hackers were increasingly staging attack over long periods, silently collecting information over weeks or months before attacking specific targets within company operations with the information they have collected over a long period. Chicago Tribune
Rana's comment: Lots of world-class Canadian energy companies who are also potentially vulnerable. It's significant that a prominent oil company's executive publicly identified cyber attacks as a threat.

Agencies, contractors get rules of the road for cloud security approvals
BY ALIYA STERNSTEIN 12/08/2011

US Federal cloud providers by June 2012 will have to comply with new uniform security controls so that multiple agencies can piggyback off the certifications for faster installation, White House officials announced Thursday.

To more quickly slice $5 billion from the government's annual $80 billion information technology tab, the Obama administration has released requirements for expediting cloud security approvals. Protecting data in the cloud -- or remote storage and software accessible online --
http://www.nextgov.com/nextgov/ng_20111208_9699.php?oref=rss?zone=NGtoday

Rana's comment: This item would be of interest to potential Canadian suppliers to the US govt, and govt officials in Canada who are considering a move to the cloud, or have heard of it

. Item Description: **Feds launch cloud security standards program.** "Federal agencies will soon have a government-wide security standard for assessing, authorizing and monitoring cloud products and services. The Federal Chief Information Officer December 8 unveiled the Federal Risk and Authorization Management Program (FedRAMP), which establishes a set of baseline security and privacy standards all cloud service providers will need to meet to sell their products to government agencies. The program requires that all agencies use only FedRAMP-certified cloud services and technologies for public clouds, private clouds, hybrid clouds, and community clouds. The program also covers all cloud service models, including Software as a Service (SaaS) and Platform as a Service (PaaS). FedRAMP will also provide federal agencies with standard procurement language to use in requests for proposals from cloud service vendors. A Joint Authorization Board, comprising of security experts from the DHS, General Services Administration, and the Department of Defense will be responsible for updating the FedRAMP security requirements on an ongoing basis. A group of third-party assessors hired from the private sector will be responsible for independently assessing cloud service providers and certifying their compliance with the standards."
Reference:
http://www.computerworld.com/s/article/9222525/Feds_launch_cloud_security_standards_program?taxonomyId=17

For the Analysis of article above:

If you think you'll save money with cloud computing, think again (NextGov) BY JOSEPH MARKS 12/06/2011

More than half of organizational users saved little or no money after transitioning to cloud computing, according to a new study, and only 14 percent actually downsized their information technology departments after moving to the cloud....Computer clouds are essentially large banks of off-site computer servers that can pack data more tightly than traditional servers and move that data more nimbly as one customer surges in use and another declines.

.....According to the CSC study, accessing data and programs on multiple devices was the most popular reason for corporate and public sector users to move to the cloud, accounting for about one-third of all transitions.

6. Item Description: **Resurgent LulzSec Attacks Government Sites In Portugal.** "The hacktivist group LulzSec was back in action last week, launching distributed denial-of-service (DDoS) attacks on government websites in Portugal. The group says it was driven to the attacks by Portuguese austerity measures, social inequalities, and recent police violence against demonstrators during a protest on Nov. 24, according to news reports. On Friday, LulzSec Portugal launched a DDoS attack against the website of Banco de Portugal (Bank of Portugal), making the site inaccessible, according to the reports. In addition to taking down the Bank of Portugal website, LulzSec Portugal has been credited with successful attacks on numerous state services. Earlier this week, LulzSec disabled the websites of the Portugal House of Parliament, several political parties, and the national police."
Reference: http://www.darkreading.com/security/attacks-breaches/232300133/resurgent-lulzsec-attacks-government-sites-in-portugal.html

1. Portuguese Under Massive Cyber Attack From Lulzsec
   http://www.voiceofgreyhat.com/2011/12/portuguese-under-massive-cyber-attack.html

International hackers Anonymous shut down Colombian Army website
http://colombiareports.com/colombia-news/news/20878-anonymous-hacks-colombian-army-website-video.html

Rana's comment: Anonymous has threatened Canadian interests before (but at least in 2011, nothing happened that I recall). However, these incidents confirm LulzSec and Anonymous have the capability to launch a DDoS and disable government websites...

Microsoft to fix Duqu virus
Microsoft Corp said it will release a security update to protect personal computers from getting attacked by Duqu, a mysterious virus that researchers suspect was built by the same group behind Stuxnet. Times of India

Duqu Perpetrators Remove Clues of C&C Servers, Following Exposure
According to security researchers from Kaspersky Lab, soon after Symantec the security company hyped the Duqu Trojan on the Internet during October 2011, those secretly unleashing the data-stealing malicious program eliminated all evidences of their existence off the command-and-control servers they operated for hiding their tracks. SPAM Fighter

---

Symantec confirms Flash exploits targeted defense companies. "Security researchers at Symantec confirmed December 7 that exploits of an unpatched Adobe Reader vulnerability

targeted defense contractors, among other businesses. "We've seen [this targeting] people at telecommunications, manufacturing, computer hardware and chemical companies, as well as those in the defense sector," said a senior security manager in Symantec's security response group. Symantec mined its global network of honeypots and security detectors — and located e-mail messages with attached malicious PDF documents — to reach that conclusion. Adobe warned Reader and Acrobat users hackers were exploiting a "zero-day" bug on Windows PCs December 6, crediting Lockheed Martin's security response team and the Defense Security Information Exchange (DSIE), a group of major defense contractors that share information about computer attacks, with reporting the vulnerability.
Reference:
http://www.computerworld.com/s/article/9222496/Symantec_confirms_Flash_exploits_targeted_defense_companies?taxonomyId=17

TRENDS – here in the Weekly or in a Monthly?

- **Cyber crime going mobile**
  Cybercrimes are becoming more mobile. As more smartphones and tablets are being used, cyber thieves aren't just targeting personal computers to steal information for financial gain, say antivirus security experts. Young men between the ages of 18 and 31 are targets because of the large amount of time they spend online every week, said Hargrove, director of consumer solutions for Symantec Inc. Known as the "millennium males," they spend more than 49 hours online a week, she said. Mobile malware is on the rise, especially with the Android devices, said Doug Cooke, director of sales engineering at McAfee Canada. Red Deer Advocate, C5

Information Security Forum predicts 'perfect storm' with 2012 security challenges
With 2011 coming to an end, security threats show no sign of slowing down. This is according to independent information security body, the Information Security Forum (ISF). ISF's top three security challenges for 2012... 1. Consumerisation of IT... 2. Cyber (in) security ... Converging threats. Information Security Forum News Release

Imperva predicts top nine cyber security trends for 2012
The rise in so-called big data and application DDoS (distributed denial of service) attacks are among concerns for the foreseeable future, according to data security specialist Imperva, which has issued a top nine cyber security trends for 2012. Number one is an assertion that security will finally trump compliance – reversing the traditional position. Imperva believes that more companies will make cyber security decisions based on security, rather than regulations, such as PCI and SOX. Imperva's number two is the rise of 'cyber brokers', as a result of an increasing supply and demand for compromised machines, as well as for sensitive corporate information. Such individuals will match the buyers of stolen data or compromised machines (bots) with sellers. Works Management

Employees' Droids among biggest government cyber menaces
BY ALIYA STERNSTEIN 11/15/2011

In 2012, agencies should worry about hackers attacking the growing number of federal employees toting their own iPhones and Droids to work, according to a forecast of next year's greatest cyber dangers compiled by M86 Security Labs.

On Tuesday, the network security firm is expected to release its annual predictions of the top computer threats to business and government organizations. At federal agencies, the biggest targets are likely to be employee-owned devices, a department's own public website and cloud services.

"The Android is very much a victim of its own success" because any developer can publish innovative -- or malicious -- software applications to Google's Android Market, Bradley Anstis, M86 vice president for technical strategy, said in an interview. Apple is more selective in vetting programs for its App Store. Most government agencies that M86 works with, including NASA, have a bring-your-own-device policy, he said.

http://www.nextgov.com/nextgov/ng_20111115_9168.php?oref=rss?zone=NGhealthit

Symantec: spam nearing three-year low, targeted attacks on the rise
E-mail spam across the world is close to a three-year low, now accounting for 70.5 percent of all messages sent. That may sound like a lot until you consider that 90 percent of e-mail sent in 2009 was spam, according to Symantec's November Intelligence Report. The 25 page report also highlights that one in 302 e-mails was identified as a phishing attempt and one in 255.8 messages contained malware. Most alarming, however, is that nearly 5,000 malicious websites are blocked each day, an increase of 47.8 percent since October 2011. Symantec reports that Russia was the most spammed region in November at 76.7 percent, followed closely by Saudi Arabia at 76.6 percent and China at 74.5 percent. The US had a 69.9 percent spam rate while Canada was slightly better at 69.5 percent. TechSpot

. Item Description**: Anonymous hacks Monsanto PR firm Bivings Group.** "Tango down: Operation End Monsanto claims first victim. The Bivings Group, a public relations firm associated with Monsanto, has been permanently shut down after a devastating attack by those claiming to represent the nebulous and notorious international Internet hacktivist collective known as Anonymous. According to the Anonymous hacktivists, The Bivings Group website was defaced, their database was hacked and dumped, hundreds of emails were stolen and are now viewable, and a database of Monsanto documents were acquired."
Reference: http://www.examiner.com/anonymous-in-national/anonymous-hacks-monsanto-pr-firm-bivings-group
http://pastebin.com/UZTcLMGT

Anonymous attacks Mexican Government (Operation SafeRoads)

On Saturday, December 10, a global cadre of Anonymous hacktivists launched a number of successful strikes against numerous Mexican transportation and government websites, protesting the dangerous travelling conditions present in Mexico.
Government agencies and bus companies were targeted for being complicit in allowing the dangerous traveling conditions in Mexico to exist. At least a dozen Mexican institutional portals, among them the Federal Roads and Bridges Access and Related Services, as well as several natioal bus companies, were the subject of Anonymous cyber attacks.
Websites were taken down via well orchestrated DDoS (distributed denial of service) attacks as well as defaced by Anonymous hacktivists. For an accounting of the many strikes, with links of verification, go to Blog.AtHack.Net and/or el5antuario.org

5. Item Description: **Information: Threat Trends in 2011 - The Signals and the Noise**.
Reference http://regmedia.co.uk/2011/11/29/jwalter_mcafee_labs_threatbrief112011_v3.pdf

Canada sorely lacking cyber security: report
Canada has fallen short in protecting its critical infrastructure from a whole host of risks, says a new report published by public policy think-tank Macdonald- Laurier Institute. Report author and Queen's University professor Andrew Graham says computer hacking traced back to China shows Canada's cyber-security needs, especially, are "mushrooming." Some action has already taken place on the issue through **Public Safety Canada's** cyber-security strategy. Meanwhile,

Colin Robertson of the Canadian Defence and Foreign Affairs Institute, another think-tank, expects to see a new North American perimeter security agreement take things further. Edmonton Sun, 75

Rana's Comment: This was in the Daily Media, and Martin e-mailed us the report. The actual report really takes aim at the whole of CI and cyber attack is identified as a risk that needs to be addressed. But the report is far less alarming and sensationalist than the headlines – honestly nothing really new or earth shattering from my perspective. Should we report?

Ultimate Bet Players Accounts Compromised, 3.5 Million Records Freely Available Online For Weeks Still In Google Cache

In a breach of security at Ultimate Bet, information from every player's account had been publicly posted on the internet, revealing personal information of approximately 3.5 million poker players holding accounts at the nearly-dead poker site.

A popular poker forum website posted a link to the account information via an anonymous posting, but removed the link roughly eight minutes later. In that short span of time, enough people identified the link and apparently passed the information around privately.

The data leaked from the accounts included each player's name and screen name; birth date; email, mailing and IP addresses; phone number; deposit methods typically used; VIP, affiliate and blacklist statuses; account balance; and players' UB account numbers, but not bank account numbers as far as we know.

The data listed was organized by specific countries, with about 2 million accounts from the U.S., 319,000 Canadian accounts, 137,000 United Kingdom accounts, and approximately 1 million accounts from all other countries combined.

Hackers mock RIM's patch efforts

- Hackers say they are a step ahead of Research In Motion's efforts to plug a security breach in the PlayBook tablet computer. Chris Wade, one of three researchers who gained authorized access to the "root" control system of RIM's first QNX device last month, said in a tweet this week that he had found a workaround only hours after RIM issued a security patch. Wade said the beta DingleBerry tool the group had developed and released on Twitter has been updated and is exploiting a second vulnerability in the PlayBook OS, software the company has called bulletproof and that RIM plans to roll out to its new smartphones next year. He said the workaround lets Windows users to load custom operating systems and apps from their desktop PC onto the PlayBook, activating features not permitted by the manufacturer. Toronto Star, B4

Dutch certificate authority reportedly hacked after access gained through PHP MyAdmin

Another Dutch certificate authority (CA) has been hacked with access gained to a management database and documents. According to a story on the Dutch news site Webwereld, Gemnet was compromised, although this does not appear to have affected certificate issuance. A provider of security consultancy and authentication technologies to nearly all parts of the Dutch government, including the Ministry of Security and Justice, Bank of Dutch Municipalities and the police, the company reportedly detected and closed the leak on Wednesday. The report claimed that the database was managed by PHP MyAdmin and access was gained without a password. The attacker was able to extract information from the database and partially control the network; among the documents was information about the technical design of the trusted network between Dutch telecommunications and ICT service provider KPN and governments or companies. SC Magazine UK

5. Item Description: **Site of Dutch CA Gemnet Offline After Web Server Attack.** "Another certificate authority in The Netherlands has been hacked, though this time the attack does not appear to have affected the certificate-issuing operations of Gemnet, a subsidiary of KPN. The company, which does business with the Dutch government among other organizations, said it has taken its Web site offline while it investigates the attack. The attack came to light Wednesday, and while the details are limited at this point, the company said that the attackers went after the public Web site and were able to compromise the server and access some private data and documents stored on the back-end database. Gemnet is owned by KPN, a large Dutch telecom and Internet company. "The hack of the site has no connection with the issuance and management of Government PKI certificates. The general website Gemnet (www.gemnet.nl) since Wednesday December 7 temporarily not accessible to visitors. The website, part of KPN, by Internet journalist Brenno de Winter Wednesday afternoon reported a possible hack. The hack would be performed on the server: the server that the general visitor information visible. KPN was immediately launched an investigation into possible causes and origins," a translation of a KPN press statement says in part."
Reference: http://blogs.technet.com/b/mmpc/archive/2011/12/09/backdoor-win32-fynloski-a-a-short-history-of-abuse.aspx

Item Description: **Australian Defence Signals Directorate's (DSD) Finds 4 Controls Stop Targeted Intrusions.** "In October, the Australian Defence Signals Directorate received a US national Cybersecurity Innovation Award for identifying and implementing (across the Australian civilian and military agencies) four security controls that could defeat more than 85 percent of targeted cyber intrusions. The four controls top a list of 35 strategies, but unlike any other government initiative, the Australians say "do the top 4 controls first" and then decide which of the other controls to implement. This is the first strategy for mitigating targeted attacks that resonates with top executives inside and outside government. The DSD just published new documents explaining exactly how to implement the four controls in the "Sweet Spot."

Reference: http://www.dsd.gov.au/publications/Implementing_Top_4_for_Windows.pdf
http://www.dsd.gov.au/publications/Assessing_Security_Vulnerabilities_and_Patches.pdf
https://www.sans.org/press/australian-defence-signals-directorate-national-cybersecurity-award.php

Rana's comment: I heard CSEC is doing something similar to this

St-Louis, Danielle

From: Beaudoin, Luc S
Sent: January-23-12 12:42 PM
To: [redacted]
Cc: Danaitis, Algis; 'Tiago Dejesus' (Tiago.Dejesus@rcmp-grc.gc.ca); Maurizio Rosa (Maurizio.Rosa@rcmp-grc.gc.ca); [redacted]; Darren Sabourin (Darren.Sabourin@rcmp-grc.gc.ca); [redacted]
Subject: Anonymous anti-ACTA threat

Ref: CE12-2590 s.16(2)(c)

FY Awareness.

SITUATION:

CCIRC is monitoring a recent post by the hacktisvist group "Anonymous" on pastebin referred to Operation SACTA (Stop Anti-Counterfeiting Trade Agreement)

[redacted]

This post refers to two a Federal Department Sites:

http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/acta-acrc.aspx?lang=eng&view=d
http://www.international.gc.ca/trade-agreements-accords-commerciaux/fo/intellect_property.aspx?view=d

DETAILS

These sites identify the following Canadian and international stakeholders:

- Canadian Intellectual Property Office
- Industry Canada's Intellectual Property Policy Information Page
- Canadian Heritage - Copyright Policy
- World Intellectual Property Organization (WIPO) Treaties
- World Trade Organization (WTO) – TRIPS

The post is encouraging supporters to:

1) "Spread the word! (twitter, piratepad, pastebit, WWP, flyers, you name it!)"
2) "mail the s**t out of your government demanding that ACTA is to be put away."
3) "Attack if necessary."
4)"???????????"
5)"Profit."

CCIRC has already observed reports of Anti-ACTA hackers attacking other websites such as Polish Government websites.
Reference: http://www.siliconrepublic.com/strategy/item/25451-anti-acta-hackers-attack-po

CURRENT ACTION

This information was [redacted] CCIRC is actively monitoring the situation.

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

s.16(2)(c)

SECRET

Bradley, Kees

From:
Sent: Friday, January 20, 2012 9:40 AM
To: Bradley, Kees
Subject: Hacking /

s.15(1) - Def

Attachments: IA 201199E.pdf; IA201128E.pdf

IA 201199E.pdf
(294 KB)

Hi Kees,

Please find assessments, on Anonymous (could be related to your cyber file),

Regards,

NHQ/AC

SECRET

Intelligence Assessment

SECRET
CSIS IA 2011-12/99
2012 01 16

ANONYMOUS: An Overview

ANONYMOUS

Key Judgments

- ANONYMOUS is the new hacktivist (hacker-activist) model. The global reach of the Internet, the availability of numerous open-source/free attack tools, and the flourishing of social networking venues facilitates the organization and carrying out of cyber-attacks by hacktivist groups. The purpose of these attacks is to bring media and public attention to their issues of concern. Thus, cyberspace is both a venue and vector for activists.
- [redacted]
- In June 2011, ANONYMOUS publicized its goal of launching cyber-attacks against governments, major organizations and financial institutions. The purpose is to obtain classified information from these organizations and publicly disclose it. [redacted]

- [redacted]

[redacted] Head, IAB

[redacted]

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS

CAVEAT

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

ANONYMOUS CANADA

1. The impetus for this assessment was ANONYMOUS' 2011 11 13 threat to "remove Toronto from the Internet" due to the city's plans to remove *Occupy Toronto* protesters from their St. James Park encampment.

2. In a video posted on YouTube on 2011 12 02, ANONYMOUS took credit for redirecting traffic from 50+ Toronto-area business websites to that of *Occupy Toronto*. The latter denounced this action and claimed that it played no part in its planning and/or execution. ANONYMOUS also stated it had "taken down" the Canadian version of Craigslist and gained access to what it claimed is a "very important email address and address book" that they plan to publicly release should the City of Toronto continue to oppose the *Occupy Movement*.[1]

4. ANONYMOUS has shown some interest in Canada and Canadian targets, especially since the 2011 06 08 defacement and hack of the Conservative Party's website. The attacker, going by the name LulzRaft , posted a fake alert claiming PM Harper had been rushed to hospital due to his choking on hash browns. LulzRaft also broke into the Party's donor database, parts of which he/she posted on *Pastebin*.

5. ANONYMOUS has recently trained its sights on the Alberta Oil Sands and the corporations involved in its associated extraction, transportation, refining and financing operations. Anonymous has thrown its support behind Project TARMAGEDDON, via #OpGreenRights, which identified specific Canadian targets including Canadian Oil Sands Ltd., the Canadian Association of Petroleum Producers and other corporations that have a presence/involvement in the Oil Sands.

ANONYMOUS – Current Situation

6. In June 2011, ANONYMOUS publicised its goal of launching cyber-attacks against governments, major organizations and financial institutions. The purpose is to obtain classified information from these organizations and publicly disclose it.

[1] www.youtube.com/watch?v=NLm-YFyjMC&feature=player_embedded#!

7. On at least two occasions, insiders identifying with ANONYMOUS' goals released sensitive corporate information to the collective. Moreover, on 2011 12 24, as part of the AntiSec (Anti Security) campaign, ANONYMOUS claimed responsibility for a cyber-attack against STRATFOR, the national security think tank. An unofficial spokesman for the group said the attackers sought to access the millions of emails held on STRATFOR's servers; emails the group reckoned would shed light on the alleged "state-corporate alliance against the free information movement."[2]

8. In spite of arrests of its members in many countries - including Australia, the US, Spain, France, the UK, the Netherlands and Turkey - throughout 2011, ANONYMOUS continues to launch operations in multiple countries, including Canada, and primarily against governmental and corporate targets.

9. ANONYMOUS' continuing cyber and real-world activities underscore the fact that it is, first and foremost, a social movement, one that has such strong "brand recognition" that it continues to attract as media attention.

[2] Barrett Brown, "On Stratfor," http://pastebin.com/WPE73rhy.

ANONYMOUS: A GROUP?

11. Currently, ANONYMOUS defines itself as an international cyber-activist collective that is leaderless and animated by the spirits of *Wikileaks* and the *Occupy Movement* as it challenges any and all attempts by the powerful (i.e. governments, corporations and other major organizations) to curtail free speech and the free-flow of information.

12. ANONYMOUS did not, however, start off as a hacktivist group. ANONYMOUS germinated (circa 2003) on an Internet Relay Chat (IRC) message board known as 4chan/b/ (www.4chan.org). To this day, the channel's central ethos is anonymity; users do not have to register using their personal information – thus remaining anonymous and having *#anonymous* as their username – and no archives are kept. At first, most people who joined 4chan/b/ were looking for "Lulz", which roughly translates into laughs derived from the misfortunes of others. These misfortunes were the result of digital pranks that 4chan/b/ participants, known as ANONS, would play on targets such as gamers. It is over time, and as a result of specific incidents, that ANONYMOUS became more politically motivated.

13. Thus, ANONS are not reformed criminal hackers seeking redemption or an ideological justification for their actions. Rather, they are individuals who were drawn by the group's ethos, which is not profit-driven.

15. In January 2008, the Church of Scientology, using the pretext of copyright infringement, sought to remove all traces of a leaked internal video[4] from the Internet. This effort galvanized individuals on 4chan/b/ into organizing a response against what they considered to be an abuse of copyright enforcement and an egregious example of the Church's attempts to silence opponents. As a result, ANONYMOUS launched *#OpChanology*[5] which sought to disrupt, through a number of measures, the

[4] This is the infamous video in which the actor and church member Tom Cruise extols the virtues of Scientology and its followers, www.youtube.com/watch?v=oM-LeRLiqA0

[5] The use of the hash-tag # preceding the operation's name is standard for ANONYMOUS and reflects the fact that each one can be followed on Twitter.

Church's operations. To do so, ANONYMOUS used Distributed Denial of Service (DDoS)[6] attacks, prank calls, black faxes[7] and protests in cities around the world.[8] It was at these protests that ANONS started wearing the now infamous Guy Fawkes mask[9] (as seen in picture) as they feared retribution from the Church, which they claim deals aggressively (including illegal harassment) with critics. This operation is ongoing, with protests being organized and held around the world, including Canada.[10] Thus, *#OpChanology* marks ANONYMOUS' political and operational awakening.

16. *#OpChanology* also cemented the mythology that continues to surround ANONYMOUS in terms of it being a collective, a social movement in which all are equal irrespective of their tenure and dedication or their technical skills. In this view, ANONYMOUS resembles a leaderless hive in which each is given a role in accordance with their skill-sets and, driven by a sense of common purpose, members swarm those that threaten it, its members, its core values or have otherwise been identified as targets by ANONYMOUS.

17. ANONYMOUS is a collective[11], a big tent in which one finds individuals and cells (usually city-based) that share the same basic ethos of Internet freedom and free speech.

18. That being said, to become an ANON one only needs to login to the chat-rooms and participate in an operation.

---

[6] A DDoS attack is one in which a multitude of compromised systems flood a single target with so many incoming messages that the target can no longer respond and essentially shuts down, thereby causing a denial of service for users of the targeted system.

[7] This refers to the faxing of entirely black documents in order empty the target's toner cartridge.

[8] Including: Kitchener, Montreal, Edmonton, Ottawa, Toronto, Vancouver and Winnipeg.

[9] The mask was made popular by the movie *V for Vendetta* (2006) in which an anarchist revolutionary dons a Guy Fawkes mask in his violent campaign against a totalitarian state.

[10] See: http://forums.whyweprotest.net/events/

[11] It is very difficult to estimate how many core ANONS there are worldwide, but if one takes the turnout to anti-Scientology protests as a proxy there are likely in the high hundreds.

19. As a result, smaller more goal-oriented splinter groups can emerge. This was the case with *LulzSec*, which went on a 50-day (Spring/Summer 2011) hacking spree against law enforcement, security intelligence, private security, government and corporate targets including the CIA, the FBI and the UK Serious and Organized Crime Agency (SOCA). As a result, sensitive data including intelligence reports, usernames and passwords, and the personal information of police officers and their families was posted on *The Pirate Bay*, one of the largest illegal downloading websites on the Internet.

21. ANONYMOUS' success lies in its ability to communicate its message to a world audience. Its media capabilities are impressive, but are more a reflection of the greater availability, and effective use, of media-making software than "deep pockets". ANONYMOUS does ask for donations, however. ANONYMOUS largely takes advantage of free services like *4chan, Pastebin, Twitter, Tumblr, Youtube* to communicate with each other and the world;

22. ANONYMOUS' tool of choice is the DDoS attack. The latter can take many forms depending on the target system and the attackers' objectives, and exploit either network (hardware/connection) or application (software) vulnerabilities. It is very difficult and expensive to defend against a DDoS attack because of its distributed nature; in other words a victim can block traffic from one or a handful of distinct Internet Protocol (IP) addresses, but not necessarily from hundreds let alone thousands. A DDoS attack produces one of three outcomes: 1) consume all your bandwidth by flooding your network with so much traffic that all communications to and from you are impossible; 2) exhaust your resources by overloading/targeting specific services (i.e. email, web site access) with bogus requests; and 3) exploit an application weakness or vulnerability to render them unusable for a period.

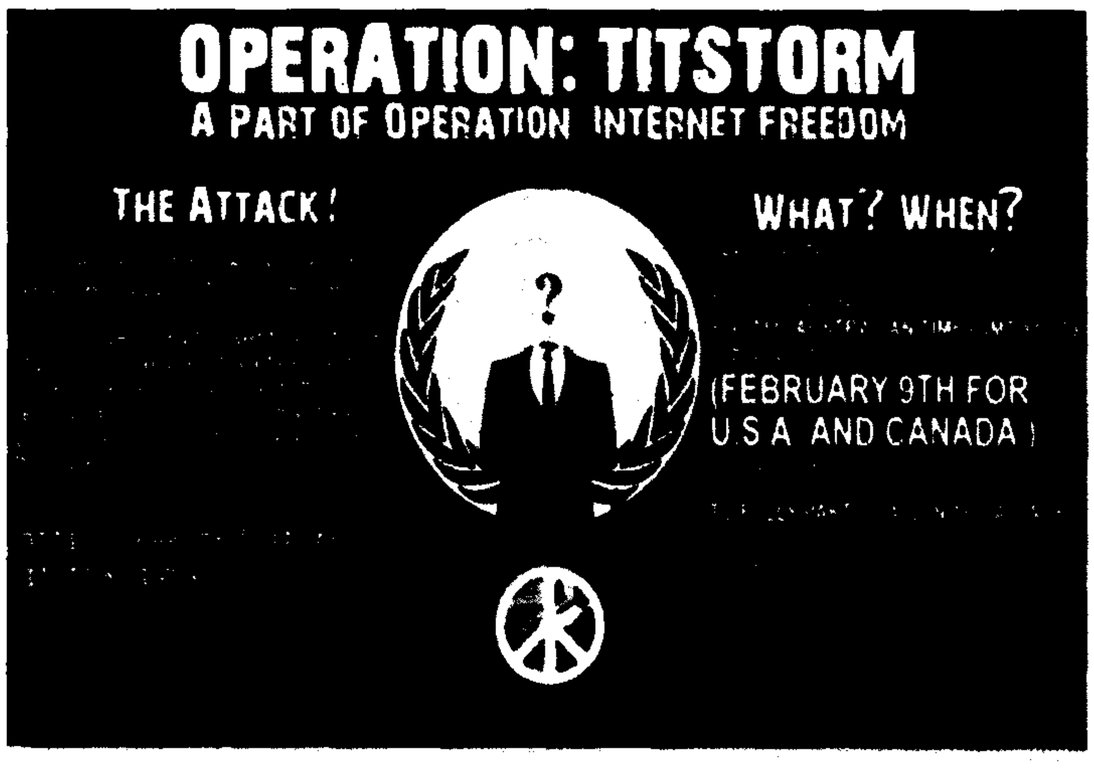
23. Returning to *#OpChanology*, it is clear that it was the first of several events that have helped crystallize ANONYMOUS' ideology, which is centered on the protection of free speech and unfettered access to all information even if it is protected by copyright or government security classifications.

24. Deeply anti-authority and libertarian at its inception, it was only in 2011 that the group adopted the more stringent anti-capitalist, animal rights, environmentalist (with frequent references to Aboriginal rights) and anti-law enforcement/security service attitudes more commonly associated with left-wing activists.

25. In the period between *#OpChanology* (January 2008) and the start of the *Wikileaks* scandal (October 2010), ANONYMOUS launched a number of operations, all aided by the use of social networking and micro-blogging services like *Facebook*, *Twitter*, *Reddit* and *Tumblr*. For instance, ANONYMOUS claims to have assisted Iran's Green Movement in the wake of Mahmood Ahmadinejad's controversial June 2009 election win. Another example is *#OpTitstorm*, which targeted Australian government websites because of Canberra's efforts to introduce a national Internet filter, thus threatening free speech and the free flow of information in Australia. From the advertising poster, it is clear that organizers expected Canadian and American members to participate. *#OpTitstorm* resulted in certain Australian government websites being inaccessible for several hours.

Julian Assange, Aaron Barr & Kalle Lasn

26. In December 2010, ANONYMOUS launched *#opPayback/Avenge Assange* against Amazon.com for no longer hosting *Wikileaks* on its servers, as well as PayPal, Visa and MasterCard for refusing to process donations to the website.



27. In February 2011, ANONYMOUS focused its attention on Aaron Barr, CEO of *HBGary Federal*, an offshoot of the well-known technology security company *HBGary*. At the time, Barr made public the fact that he had been "investigating" *#opPayback* by mining social networking and micro-blogging sites to identify key members and understand the inner workings of ANONYMOUS. He had also intimated that this investigation was conducted for the FBI. Before he could present the results at a conference, ANONYMOUS defaced *HBGary*'s website, broke into its servers and stole some tens of thousands confidential company emails and posted them on *The Pirate Bay*. ANONYMOUS also disclosed Barr's social security number, home address and cell phone number, as well as compromised his personal email, *Twitter* and *LinkedIn* accounts. Some members even claimed to have erased one Terabyte of information off the *HBGary's* servers and gotten hold of the STUXNET worm among other things.

28. The impact of ANONYMOUS' cyber-attack on *HBGary Federal* was dramatic for all parties. *HBGary* had to reassure clients that their source codes to proprietary malware and other software (crown jewels) were never accessed by ANONYMOUS; in spite of its denials, *HBGary*'s reputation was damaged. The attack underscored how ANONYMOUS can mount operations targeting one individual, and the extent to which a determined actor can use open-source information and well-known vulnerabilities –

29. The emails stolen from *HBGary* showed how closely it was working with US Federal authorities, as well as with large financial institutions to whom *HBGary* had proposed doing a cyber-attack against the *Wikileaks* in an effort to stop it from leaking documents pertaining to their activities. This confirmed many of the ANONYMOUS' worst fears about what *Wikileaks* is now describing as a growing "international mass surveillance industry" in which private companies provide tools and techniques for state entities such as law enforcement and security intelligence to more effectively capture and follow individuals' and groups' digital trails online. These technologies allow users to map social networks, track cell phones, do locational tracking and deep packet inspection (i.e. capture and look at the content of messages).[12] From an ANONYMOUS perspective, these revelations reinforce the notion that it is not only authoritarian regimes that seek to censor the Internet and persecute those who seek to exercise their rights to free speech and assembly, but Western corporations and democracies as well; as *Wikileaks* states "[i]n the last ten years systems for indiscriminate, mass surveillance have become the norm."

30. Vancouver-based Kalle Lasn's call to *Occupy Wall Street* (OWS), in *Adbusters* magazine, was heeded early on by ANONYMOUS as evidenced by the presence of members in most, if not all the occupations that have taken place in Europe, Australia, North and South

---

[12] "The Cyber-security Industrial Complex," Technology Review, 2011 12 06; "Big Data meets big brother," PrivacyInternational.org, 2011 11 30; "The Spyfiles," http://wikileaks.org/the-spyfiles.html

America. It is not happenstance that the Guy Fawkes mask is now seen by many as the emblem of the *Occupy Movement*. Moreover, ANONYMOUS claimed it was releasing a new attack tool, RefRef, to coincide with the "Day of Rage" (2011 09 17) which officially launched the *Occupy Movement*.

31. The ANON developer claimed that RefRef exploited known vulnerabilities and that it precluded the need for the heavy firepower of a botnet[13] as it essentially turns the target server against itself, leading to resource exhaustion.

32. ANONYMOUS remains committed to the *Occupy Movement*. It has launched a number of operations in support of the movement, especially after evictions of OWS participants from most occupation sites. For instance, ANONYMOUS has announced *#opHorizon* which calls for protests to take place on 2011 12 17 in order to commemorate the death of Mohamed Bouazizi and the start of the Arab Spring, the three month anniversary of the *Occupy Movement* and the birth of Pfc. Bradley Manning. The following statement sums it up:

We are Anonymous
We are Bradley Manning
We are Arab Spring, European Summer, American Autumn
We are 99%
We do not forgive
We do not forget
Expect us

[13] A botnet is a network of computers that have been infected with malicious software and is being instructed to accomplish automated tasks on the Internet unbeknownst to the owners. Criminals use botnets to send out spam email, spread viruses and attack computers and servers.

Outlook

33. ANONYMOUS is the face of modern hacktivism. Though hacktivism has existed since the time of the first dial-up connections, it is only now - with the ubiquity of the Internet, the greater availability of free attack tools and techniques, and the flourishing of social networking tools - that groups can bring media and public attention to issues that concern them.

38. Foreign governments may view groups like ANONYMOUS either as serious national security threats that must be dealt with using "muscular" means or as an extension of Western governments' and intelligence services' operations. The potential for negative diplomatic impacts is a reality as certain governments may see the hidden hand of Western governments and intelligence services behind the actions of ANONYMOUS. (C)

Pages 1267 to / à 1273

are withheld pursuant to sections

sont retenues en vertu des articles

16(1)(c), 15(1) - Subv, 16(1)(a)(iii)

of the Access to Information

de la Loi sur l'accès à l'information

Dincoy, Rana

From: Bendelier, Kenneth
Sent: January-18-12 10:35 AM
To: Dincoy, Rana
Subject: Re: [redacted]

s.16(2)(c)

Ok, this was just for level of content reference anyway, not specific content

From: Dincoy, Rana
Sent: Wednesday, January 18, 2012 10:31 AM
To: Bendelier, Kenneth
Subject: RE: [redacted]

What's missing from this synopsis is that Anonymous claims they are not responsible for this hack... I found an "emergency Christmas Anonymous press release" in Pastebin stating this. I put that in the Weekly Summary...

Rana Dincoy
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773

From: Bendelier, Kenneth
Sent: January-18-12 10:21 AM
To: Dincoy, Rana
Subject: FW: CIIT Update - STRATFOR Breach

From: Scott Foster [mailto:Scott.Foster@rcmp-grc.gc.ca]
Sent: January-03-12 11:04 AM
To: Scott Foster
Subject: [redacted]

Good day,

Pages 1275 to / à 1276

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Canada

PROTECTED B
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-004

For the Week of

5 Nov – 10 Nov 2011

Issued: 17 Nov 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released:** (1) Information Note IN11-002 (DNS Changer Infrastructure) – Massive internet fraud scheme linked to the week's FBI arrests – victims in Canada include federal government departments; (2) Technical Report TR11-001(Malware Infection Recovery Guide); and (3) Advisory AV11-048 (Highlights of Microsoft Security Bulletin for November 2011).

- **Reported Incidents:** (1) A lapsed federal government department website used to advertise escort services; (2) Website vandalism in the manufacturing, health, and information technology sectors; (3) Computer infections in federal and provincial governments, health, energy and education sectors; (4) Threat actors masquerading as Canadian financial and telecommunication companies luring internet users to malicious websites (phishing); and (5) Computers in the manufacturing and telecommunication sectors being used to control "zombie" computer networks (botnets) that steal data.

- **Noteworthy Open Source Reports:** (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

PROTECTED B
DRAFT

s.16(2)(c)
s.20(1)(c)

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and other noteworthy open source reports.

NOTABLE INCIDENTS– 5 NOVEMBER THROUGH 10 NOVEMBER 2011:

Government Systems.

Federal. CCIRC learned of media reports that a lapsed Transport Canada domain (i.e. no longer used nor registered by Transport Canada) was being used to advertise escort services. CCIRC informed the Cyber Threat Evaluation Centre (CTEC), the Government's cyber incident handler. It was reported that the link between Transport Canada's website and this formerly government domain has been severed.

Analysis: Although the Transport Canada related event may not be considered as a cyber incident, it illustrates the challenges with maintaining control of one's brand on the internet. Since this website did not violate any copy rights by using Government of Canada logos, there appears to be no legal recourse.

CCIRC continued to receive infection reports for computers at The reports concerned botnet type malicious software designed to take control of a computer and use it to do malicious activity online. CCIRC notified CTEC.

- **Analysis:** This week, CCIRC received infection reports on this type of malicious software in a variety of sectors, which included provincial, health, energy and education.

Provincial. CCIRC received infection reports for computers on the government system. CCIRC notified cyber contacts of these reports and provided mitigation advice. The impact on the organization is unknown.

- **Analysis:** These infections were a common type of malware designed to compromise computers, then steal information and/or use them for illegal activities online. CCIRC continues to receive reports of possible infections on computers of provincial governments. This may be because these governments connect to a large provincial population who don't all practice good cyber security.

Canadian Critical Infrastructure:

Financial Sector. Threat actors impersonating well known Canadian financial institutions attempted to persuade users to disclose their on-line banking credentials and click on links to malicious websites. CCIRC notified , whose customers were being lured to a malicious website

still in operation. CCIRC also notified Google phishing, the Anti-Phishing Working Group, and Microsoft, so internet users may be alerted if they encounter these specific malicious websites.

- **Analysis:** This type of malicious activity is commonly seen by CCIRC and continues to cause financial losses for Canadians. Canadian banks react to these types of incident reports in a very timely manner and are usually quite proficient at ensuring these malicious websites are no longer accessible to the public. The new anti-SPAM legislation, expected to come into force in 2012, is meant to address these situations. However, enforcement of this legislation could be challenging when these malicious websites are located outside of Canada.

Telecommunications Sector. Threat actors impersonating [redacted] tried to persuade internet users to disclose personal information. CCIRC notified the [redacted] Unit and as well as the [redacted] liaison person at the Canadian Telecom Cyber Protection (CTCP) unit in Industry Canada.

- **Analysis:** The type of personal information being requested by the threat actors would allow them to carry out identity theft. It is unknown whether there were internet users in Canada who provided the requested personal information to the threat actors.

  CCIRC also received reports that a computer at [redacted] Technologies, a web-hosting firm in Montreal, was being used as a controller of a network of compromised computers used for malicious purposes (a Zeus botnet). CCIRC notified the company and the RCMP. The company took action to ensure its computer was no longer being used for this malicious purpose.

Analysis: A computer compromise at a company that hosts websites for several organizations, can have a bigger impact on internet security than a compromise at a single company. These website hosting companies have varying levels of internal monitoring for IT security.

Energy Sector. CCIRC continued to receive infection reports on computers of [redacted] a large oil & gas producer. CCIRC notified the company of the potential infections and provided mitigation measures. The impact on the organization is unknown.

Health Sector. CCIRC continued to receive infection reports for [redacted] CCIRC notified the company and provided mitigation measures. The impact on the organization is unknown.

- **Analysis:** Since CCIRC receives infection reports for organizations, continued infection reporting for the same organizations does not necessarily mean the previous reports were not actioned by the organization. It could mean that the infection was not completely removed from that organization's network and new computers in that organization became infected

Transportation Sector. CCIRC received reports that a computer at [redacted] was being used as a controller of a network of compromised computers used for malicious purposes (a Zeus botnet). [redacted] is located in [redacted] BC, and is a sales and service centre for aircraft avionics products. CCIRC notified the company and their hosting internet service provider, and provided them with mitigation advice. The RCMP was also notified. The impact of this compromise is unknown.

- **Analysis:** [redacted] is a Transport Canada accredited company that is using a Canadian web hosting organization ([redacted]. Reports show that a computer hosted by [redacted] is serving as the botnet controller, which could indicate this web hosting organization itself has been compromised. The organization is known to host 164 web sites, which may have been compromised. This compromise may have also affected [redacted] clients' or business partners' computers.

Public. CCIRC received infection reports on computers of nine universities across Canada and included the Universities of [redacted] This is down from seventeen last week.

CCIRC Products:

1. **Information Note IN11-002 (DNS Changer Infrastructure):** This information product was publicly released to help potential Canadian victims of the world-wide internet fraud uncovered by the FBI after a two year investigation. There were 4.2 Million infected sites in over 100 countries and Canadian victims identified so far include federal government departments. There may be more than 10,000 victims in Canada. Eight Estonian individuals were arrested and one Russian national is still at large. The known impact of this fraud was theft of personal data, including credit card numbers as well as defrauding companies who placed on-line advertisements.

   In this highly sophisticated fraud which had been ongoing for four years, threat actors remotely compromised computers around the world. These criminals then used rogue DNS servers, which caused those internet users of those computers to be redirected to malicious websites. The US indictment alleges that the defendants, who masqueraded as legitimate publishers in the internet advertising industry, had financial incentives to have many internet users click on the links for certain websites and on-line advertisements. The US Government has allowed a non-governmental organization to temporarily replace the rogue DNS servers by "clean ones", so users with infected computers do not lose their ability to connect to the internet.

   CCIRC continues to work with the FBI and other Computer Emergency Response Teams around the world to gather more information about this fraud and identify Canadian victims.

2. **Technical Report TR11-001 (Malware Infection Recovery Guide):** This was a publicly released report, also sent directly to CCIRC's government and critical infrastructure stakeholders. The report contained general technical advice to organizations that may be

infected with certain types of malicious software, which can be difficult to remove. It was thought to be timely advice given the type of internet fraud publicized this week, as explained above.

3. **Advisory AV11-048 (Microsoft Security Bulletin Summary for November):** CCIRC brought to stakeholders' attention important Microsoft Security Bulletin highlights by publicly releasing this product, which was also sent directly to stakeholders.

Noteworthy Open Source Reports:

Hackers threaten Toronto over Occupy policy – The hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp.

- **Analysis:** Anonymous is an activist group of loosely affiliated hackers, who have in the past successfully carried out threats. They last targeted Canada in an operation called 'Tarrmageddon' (i.e. targeting oil sand companies in Alberta). It is possible that the City of Toronto's services could be affected by such an attack. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat – they are taking precautionary measures.

Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world – A new survey by the Anti-Phishing Working Group (APWG) reveals that phishing attacks perpetrated against Chinese e-commerce and banking sites soared by 44 percent in the first half of 2011. Some 70 percent of all maliciously registered domain names in the world were established by Chinese cyber criminals for use against Chinese brands and enterprises.

- **Analysis:** As elsewhere in the world, Chinese internet users are also targeted for their financial information by cyber criminals impersonating reputable companies. It seems that Chinese cyber criminals preferred to register their own domain names rather than hack another domain as other cyber criminals do. This survey is believed to contain reliable information not available to many western sources.

  The APWG is a reputable non-profit global pan-industrial and law enforcement association, where Government of Canada officials (ex: Justice and Industry Canada) also participate. Chinese information for this survey was provided by the China Internet Network Information Centre, who is also the secretariat for the Anti-Phishing Alliance of China (APAC). APAC has more than 140 member institutions in the country, including banks, e-commerce sites, and domain registrars, and has an efficient reporting and domain suspension program.

The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker: – DARPA funded researchers are building a program for "generating and distributing believable misinformation." Their ultimate goal is to plant auto-generated, false documents in classified networks and program them to trace intruders' movements. The program

aims to both: (1) scare off individuals browsing WikiLeaks; and (2) minimize insider threats (according to some sources, the greatest vulnerability in military networks).

- **Analysis:** The US government is creating products capable of tracking individuals, and as such, there may be legal / privacy implications. It is possible this public discussion of the project is a way to discourage those individuals inclined to leak US government information and test public opinion on the project.

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Public Safety Canada | Sécurité publique Canada

Canada

PROTECTED B
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-004

For the Week of

5 Nov – 10 Nov 2011

Issued: 17 Nov 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released:** (1) Information Note IN11-002 (DNS Changer Infrastructure) – Ma on the massive internet fraud scheme linked to the week's FBI arrests – victims in Canada include federal government departments; (2) Technical Report TR11-001(Malware Infection Recovery Guide); and (3) Advisory AV11-048 (Highlights of Microsoft Security Bulletin for November 2011).

- **Reported Incidents:** (1) A lapsed federal government department website used to advertise escort services; (2) Website vandalism in the manufacturing, health, and information technology sectors; (3) Computer infections in federal and provincial governments, health, energy and education sectors; (4) Threat actors masquerading as Canadian financial and telecommunication companies luring internet users to malicious websites (phishing); and (5) Computers in the manufacturing and telecommunication sectors being used to control "zombie" computer networks (botnets) that steal data.

- **Noteworthy Open Source Reports:** (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

Comment [T1]: Fix formatting

Page 1284

is a duplicate

est un duplicata

Page 1285

is a duplicate

est un duplicata

Page 1286

is a duplicate

est un duplicata

Page 1287

is a duplicate

est un duplicata

Page 1288

is a duplicate

est un duplicata

Dvorkin, Corey

From: [redacted]
Sent: January-12-12 10:08 AM
To: DAVID.LEHMAN@forces.gc.ca; DONALD.NEILL@forces.gc.ca; serge.stang@forces.gc.ca; Dvorkin, Corey; [redacted]
Subject: Fwd: HOMELAND SECURITY UPDATE DEC 28 2011 - JAN 8, 2012
Attachments: 010912 CQ - House Cybersecurity Bill.docx; 010912 CQ - The Year of the Lone Wolf.docx; 010912 CQ - Where to Cut and Where to Spend.docx

Of note:

"DEC 29 - According to recent studies by university researchers and security companies, cars and trucks have become increasingly vulnerable to cyberattacks. One found that a car's computer controls could be remotely accessed through its Bluetooth, Wi-Fi or OnStar connections, potentially allowing terrorists to control the brakes of numerous cars simultaneously, corporate spies to eavesdrop on a motoring executive's phone calls, or thieves to electronically locate, break into and start cars they've targeted to steal."

By not having a car, I'm doing my part to defeat the terrorist. And Skynet.

>>> <Katie.Tolan@international.gc.ca> 1/9/2012 4:01 pm >>>

SUMMARY OF KEY ITEMS OF INTEREST:

I. PEOPLE: (1) Department of Homeland Security (DHS) Secretary Janet Napolitano held a change of command ceremony for US Customs and Border Patrol (CBP) DEC 30 , announcing that CBP Commissioner **Alan Bersin will be now hold the position of Assistant Secretary for International Affairs in the Office of Policy at DHS. Deputy CBP Commissioner David Aguilar stepped up to become acting CBP Commissioner** and **Thomas Winkowski**, Assistant Commissioner of Field Operations, **became acting Deputy Commissioner**. Mr. Bersin had served as International Affairs Assistant Secretary for almost a year, when in March 2010 he accepted a recess appointment valid through DEC 31, 2011 from President Barack Obama to become Commissioner of CBP (note - the title at that time was Assistant Secretary for International Affairs and Special Representative for Border Affairs). During the change of command ceremony, **Secretary Napolitano signalled that in holding the Assistant Secretary position Mr. Bersin will oversee the department's international engagement, leading the strategic development and execution of DHS international plans and policies and forging new partnerships with foreign governments and international organizations.** The Secretary noted that this is the Department's "chief diplomatic officer" (See DHS for related links).

(2) The Assistant Attorney General for the Office of Justice Programs (OJP), **Laurie Robinson,** announced JAN 3 that she would be leaving her position at the end of February. Assistant Attorney General Robinson was confirmed by the Senate in November, 2009. **Principal Deputy Assistant Attorney General Mary Lou Leary will serve as acting assistant attorney general** following Robinson's departure. (See DOJ for related link)

II. BUREAU OF COUNTERTERRORISM: The **Department of State (DOS) announced the establishment of the Bureau of Counterterrorism JAN 4,** fulfilling one of the key recommendations of the Quadrennial Diplomacy and Development Review concluded in December 2010. The Bureau of Counterterrorism will lead the Department's engagement in support of U.S. government efforts to counter terrorism abroad and to secure the United States against foreign terrorist threats. The new Bureau will assume

the responsibilities of the Office of the Coordinator for Counterterrorism. The Fact Sheet released noted that the United States faces a continuing terrorist threat from al-Qaida and other groups and individuals who subscribe to violent extremism. While good progress has been made in combating terrorism since the 9/11 attacks, challenges remain. Together with defense, intelligence, law enforcement, and homeland security, diplomacy and development are critical to keeping America safe. To secure the future, there is a need to continue to strengthen the international coalition against terrorism, build foreign partner capacity to mitigate terrorist threats, reinforce resilience against attacks, and counter the ideologies and ideas that fuel violent extremism around the world. **The Bureau of Counterterrorism will implement its mission by:**

• **Developing and implementing counterterrorism strategies, policies, and operations:** The U.S. government has no greater responsibility than to protect the American people. The Bureau of Counterterrorism will play an integral role in meeting this obligation by leading the Department's engagement to develop and implement counterterrorism strategies, policies, and operations to disrupt and defeat the networks that support terrorism. The Bureau will work to safeguard American security interests while promoting U.S. values, including support for human rights, democracy, and the rule of law.

• **Strengthening counterterrorism diplomacy:** Strengthening existing partnerships and building new relationships is a cornerstone of U.S. counterterrorism policy. The Bureau of Counterterrorism will engage with bilateral partners, regional organizations, and the United Nations to broaden and deepen counterterrorism cooperation. **In one of many initiatives, the Bureau will lead U.S. government efforts on behalf of the State Department to support the Global Counterterrorism Forum,** a new multilateral initiative focused on setting the international counterterrorism agenda for the 21st century.

• **Strengthening homeland security:** Securing the homeland from external terrorist threats is central to U.S. foreign policy. The Bureau of Counterterrorism will be the principal State Department link with the Department of Homeland Security on counterterrorism strategy and operations. The Bureau will work in partnership with DHS, as well as other agencies and bureaus, to strengthen international cooperation on a wide range of homeland security issues including transportation security, the interdiction of terrorist travel, and critical infrastructure protection.

• **Countering violent extremism:** To defeat terrorists, there is a need to undermine their ability to recruit. The Bureau of Counterterrorism will focus the State Department in U.S. government efforts to counter violent extremism, thereby reducing radicalization and mobilization abroad. The Bureau will work to delegitimize the violent extremist narrative, to develop positive alternatives for populations vulnerable to recruitment, and to build partner government and civil society capacity to counter violent extremism themselves.

• **Building the capacity of foreign partners:** The security of the United States depends on the strength of its partners and allies abroad. With capable partners who are able to manage the threats within their borders and regions, the likelihood of U.S. forces being called into action is greatly reduced. The Bureau of Counterterrorism will work with other bureau and agency partners in supporting U.S. government work to build international partner counterterrorism capacity in the civilian sector and will contribute to efforts in the military and defense sectors. (See DOS Section for related link)

THIS WEEK IN WSHDC:

JAN 9: An American man is reported to have been sentenced to death in Iran after a court there convicted him of working for the CIA and going to the Persian nation to spy. The family of Amir Mirzaei Hekmati, a 28-year-old former U.S. Marine, says he was in Iran to visit his grandmothers. According to Iran's state-run Press TV, "the verdict was issued by Tehran's Revolution Court on JAN 9 after the defendant was found guilty of collaboration with the US government and its intelligence agency, the CIA, against the Islamic Republic of Iran." The Associated Press reports that Hekmati was born in Arizona, graduated from high school in

Michigan and was an Arabic translator while in the Marines. The wire service adds that "his family is of Iranian origin. His father, a professor at a community college in Flint, Mich., has said his son is not a CIA spy and was visiting his grandmothers in Iran when he was arrested." Iran Sentences American To Death In Spy Case

JAN 4 - A New Mexico sheriff said a retired Sandia Labs scientist was apparently building bombs at his home before he died. Torrance County Sheriff Heath White tells KOB-TV it appears 81-year-old David O'Keefe spent his retirement on the outskirts of Estancia continuing his work up until he died a few months ago. White says O'Keefe was trying to make a new type of explosive and was experimenting with different chemicals and different compounds to make that explosive, which put neighbors within a half mile in great danger. Deputies discovered the explosives Saturday when the property owner went to check on the home and found the chemicals. White says cleanup will take some time. Article

JAN 4 - Police departments across the country are looking into a startling statistic. For the last two years the number of officers killed in the line of duty has jumped. Local officers say the threat of violence is present at every call they respond to and they say it's not easy knowing 177 fellow officers were killed this past year. Article

JAN 4 - Health researchers and wildlife biologists say the number of infectious diseases that have jumped the boundary from animals to humans and between animal species is on the rise. Scientists believe the increase may be a result of more frequent contact between humans and wild animals, as well as the growing trade in wild animals, both legal and illegal. Article

JAN 3 - China-based hackers for months have been targeting federal agencies and contractors through infected emails apparently to spy on the Pentagon's drone strategy and other intelligence matters, according to Internet security researchers. The reported espionage employed a tactic known as spear-phishing where infiltrators, operating under the guise of a legitimate sender, email specific victims a virus-laden file or link. In this case, the hackers used email addresses from military and other government organizations, Jaime Blasco, manager of AlienVault Labs, said JAN 3 Article

JAN 1 - International hacker group Anonymous claims responsibility for hacking and releasing information about members of the California State-wide Law Enforcement Association union. Anonymous released the names, addresses and phone numbers of members; plus, credit card information taken from the association's online gift store was posted. The information dump was called "pr0j3ct m4hy3m". Article

DEC 29 - According to recent studies by university researchers and security companies, cars and trucks have become increasingly vulnerable to cyberattacks. One found that a car's computer controls could be remotely accessed through its Bluetooth, Wi-Fi or OnStar connections, potentially allowing terrorists to control the brakes of numerous cars simultaneously, corporate spies to eavesdrop on a motoring executive's phone calls, or thieves to electronically locate, break into and start cars they've targeted to steal. Article

DEC 28 - It's a case of drug dealing, international money laundering and funneling money to a known terrorist group, Hezbollah. And there's a Georgia connection. 11Alive's Center for Investigative Action spent the day digging for clues as to how a local family has been caught up in it. The family ran a used car dealership out of Fairburn and is alleged to have made more than $1 million in profit by selling used cars that ended up being part of an elaborate money laundering scheme to fund Hezbollah in Lebanon. The family is not accused of anything illegal and is not charged with a crime, but the dealership is one of 30 that federal agents have moved in on over the last couple of weeks to recover money. It's all in a **75 page complaint filed by the US attorney** in Manhattan. Thirty used car dealers in the U.S. are caught up in it, including Fairburn's Baaklini North America, Inc., which is alleged to have made $1.4 million, possibly selling cars to help fund Hezbollah. Here's

how it's supposed to have gone down: Since 2007 about $300 million in Lebanese drug money was reportedly funneled through financial institutions in North America. The money went to buy used cars in the U.S., which were then shipped to West Africa and sold. The laundered money was alleged to have been smuggled back to Lebanon. Article

WHITE HOUSE:

JAN 7: President Obama shares his New Year's resolution: doing whatever it takes to move the economy forward and ensure that middle class families regain the security they've lost in the last decade. http://www.whitehouse.gov/blog

JAN 5 - President Obama traveled to the Pentagon to discuss a major shift in the nation's strategic military objectives -- with a goal of moving away from the expansive wars in Iraq and Afghanistan and toward a different posture that emphasizes a new focus for the future. Blog

JAN 4 - President Obama announced today his intent to recess appoint four individuals to fill key administration posts that have been left vacant: Richard Cordray, Director, Consumer Financial Protection Bureau; Sharon Block, Member, National Labor Relations Board; Terence F. Flynn, Member, National Labor Relations Board; and Richard Griffin, Member, National Labor Relations Board. Press Release

DEC 31 – President Obama signed into law H.R. 1540, the "National Defense Authorization Act for Fiscal Year 2012" which authorizes funding for the defense of the United States and its interests abroad, crucial services for service members and their families, and vital national security programs that must be renewed. Press Release

DHS:

JAN 6 : Underscoring the Obama Administration's commitment to family unity and administrative efficiency. this morning U.S. Citizenship and Immigration Services posted a Notice of Intent in the Federal Register to begin a regulatory change that would reduce the amount of time that U.S. citizens are separated from their families while their family members go through the process of becoming legal residents of the United States. USCIS Proposes Regulatory Change to Decrease the Time U.S. Citizens are Separated from Family Members who are Legally Immigrating to the U.S.

DEC 30 - DHS Secretary Janet Napolitano held a change of command ceremony for US CBP, announcing that CBP Commissioner Alan Bersin has returned to the position of assistant secretary for international affairs in the policy shop at the DHS. Deputy CBP Commissioner David Aguilar stepped up to become acting CBP commissioner and Thomas Winkowski, assistant commissioner of Field Operations, became acting deputy commissioner. Bersin served as international affairs assistant secretary for almost a year, when in April 2010 he accepted a recess appointment good through Dec. 31 from President Barack Obama to become CBP chief. Remarks http://www.dhs.gov/xabout/structure/bio_1269973987071.shtm http://www.dhs.gov/ynews/releases/pr_1239820176123.shtm

DEC 29 – DHS announced a new partnership between DHS' "If You See Something, Say Something™" public awareness campaign and the National Hockey League (NHL) - highlighting the Department's continued partnership with the sports industry to ensure the safety and security of employees, players and fans. Press Release

DEC 28 - DHS officials were among the first to discover that the Public Advocate's Office website was hacked over Christmas weekend. The federal Multi-State Information Sharing and Analysis Center notified the city's tech department about the cyberattack in which data about thousands of users was stolen. Article

DEC 28 - Many prisons and jails use SCADA (Supervisory Control And Data Acquisition) systems with Programmable Logic Controllers (PLCs) to open and close doors. Researchers discovered significant vulnerabilities in PLCs used in correctional facilities and were able to remotely flip the switches to "open" or "locked closed" on cell doors and gates. Article

DEC 28 – FEMA mailed out 83,000 debt notices this years seeking to recover more than $385 million it says was improperly paid to victims of hurricanes Katrina, Rita and Wilma. The debts, which average about $4,622 per recipient, represent slightly less than 5 percent of the roughly $8 billion that FEMA distributed after the storms. At least some of the overpayments were due to FEMA employees' own mistakes, ranging from clerical errors to failing to interview applicants, according to congressional testimony. Article

CBP:

JAN 4 - The U.S. Customs and Border Protection agency is disputing the assertion that a Canadian man gained entry into the U.S. by only using a scanned photo of his passport on his iPad. Agency spokeswoman Jenny Burke said scanned documents are not accepted. She says if an individual does not have a passport, an enhanced driver's license or an expedited travel pass the border officer must determine identity and citizenship using a variety of other means, or deny entry. Burke says Reisch had both a driver's license and birth certificate. Article

DEC 29 - Federal law enforcement authorities are rapidly expanding a military-style unmanned aerial reconnaissance operation along the US-Mexico border. Eight Predators fly for the Customs and Border Protection agency — five, and soon to be six, along the southwestern border. Drones now patrol most of the southern boundary, from Yuma, Arizona, to Brownsville, Texas. Planning documents for the CBP envision as many as 24 Predators and their maritime variants in the air by 2016, giving the agency the ability to deploy a drone anywhere over the continental United States within three hours. Article

ICE:

JAN 5 – DOJ's most recent Summary of Major U.S. Export Enforcement Prosecutions cited that more than 74 percent of the government's most significant counter-proliferation investigation prosecutions were either led by ICE or had a significant contribution from ICE HSI agents. Press Release

DEC 29 - ICE announced new measures to ensure that individuals being held by state or local law enforcement on immigration detainers are properly notified about their potential removal from the country and are made aware of their rights. The new measures include a new detainer form and the launch of a toll-free hotline. Press Release

TSA:

JAN 5 – The TSA has found 1,200 guns, snakes, C4 explosives and inert landmines in the past year at airport checkpoints around the country. TSA has compiled a list of their top 10 good catches of 2011. Press Release

DEC 29 - Although overall appropriations for the DHS are down slightly this year from Fiscal Year (FY) 2011, the TSA received about $7.85 billion, up $153 million from 2011. Article

DOS:

JAN 4 - The U.S. State Department announced JAN 4, the elevation of its counterterrorism office to a full-scale bureau. The mission of the new bureau will be to lead the Department in the U.S. Government's effort to counter terrorism abroad and to secure the United States against foreign terrorist threats. The bureau will have a number of concrete responsibilities. In coordination with Department leadership, the National Security Staff, and U.S. Government agencies, other U.S. Government agencies, it will develop and implement counterterrorism strategies, policies, operations, and programs to disrupt and defeat the networks that support terrorism. The bureau will lead in supporting U.S. counterterrorism diplomacy and seek to strengthen homeland security, countering violent extremism, and build the capacity of partner nations to deal effectively with terrorism. Briefing; State Department Fact Sheet: New Bureau of Counterterrorism

DOJ

JAN 3 - The Assistant Attorney General for the Office of Justice Programs (OJP), Laurie Robinson, announced y that she would be leaving her position at the end of February. Assistant Attorney General Robinson was confirmed by the Senate in November, 2009. Principal Deputy Assistant Attorney General Mary Lou Leary will serve as acting assistant attorney general following Robinson's departure. Press Release

FBI:

JAN 4 - U.S. Attorney William J. Hochul, Jr. announced today that Minnetta Walker, 44, of Buffalo, N.Y., who was convicted of conspiracy to defraud the United States, was sentenced to 24 months in prison, to be followed by one year supervised released. Ms. Walker while on official duty with the TSA, assisted certain individuals in bypassing the normal security procedures, measures, and requirements at the Buffalo Airport. Press Release

JAN 4 - Trey Scott Atwater, of Hope Mills, N.C., was arrested DEC 24 while trying to go through security at an airport in Texas where he was planning to fly back home. Authorities say the 30-year-old had a carry-on bag containing C4, a powerful explosive used in Iraq and Afghanistan to blow the hinges off doors or destroy unexploded ordinance. Atwater was detained at the Fayetteville, N.C., airport on Dec. 24 when security agents found a military smoke grenade in his carry-on bag. Article

JAN 3 - Three people reported falling ill JAN 3 after exposure to a suspicious powder in the mail room of the state attorney's office in West Palm Beach, Florida, a city spokesman said. Article

JAN 2 - The FBI Seattle Division joined the National Park Service (NPS) in announcing the end to the multi-agency manhunt for the subject suspected of killing Ranger Margaret Anderson on January 1, 2012 in Mount Rainier National Park. FBI, NPS, and PCSD officials confirmed that the suspect, Benjamin Barnes, was found dead. Press Release

ODNI:

JAN 4 - Statement by Director of National Intelligence James R. Clapper on the signing of the Intelligence Authorization Act for fiscal year 2012. Statement

AFGHANISTAN/PAKISTAN WAR:

JAN 6 - Husain Haqqani, Pakistan's embattled former ambassador to Washington, fears he will be murdered if he leaves his sanctuary in the official residence of the country's Prime Minister Yusuf Raza Gilani. Article

JAN 5 - The Afghan government said JAN 5 that it was shutting down the operations of one of the largest foreign security companies operating in the country after detaining two of its contractors on suspicion of gun smuggling. After months of growing tension between the government and foreign security contractors, the decision marks a sharp escalation into public action by the Afghan authorities. President Hamid Karzai is in the midst of replacing foreign security contractors with Afghan guards. The Interior Ministry said it was immediately withdrawing the company's license, although the company, GardaWorld, a private Canadian security outfit, said it was in discussions with the government and hoped to be able to continue to operate. The Interior Ministry said that the contractors, two Britons, who were detained on JAN 3 after being found with an arsenal of unlicensed AK-47 assault rifles in their sport utility vehicle, were among the 341 Afghan guards and 35 foreign contractors employed by GardaWorld in Afghanistan. Article

JAN 5 - Afghanistan President Hamid Karzai is demanding that the U.S. detention center at Bagram Air Base be handed over to Afghan control within a month. Article

JAN 3 - The Afghan Taliban said JAN3 they have reached a preliminary agreement to set up a political office in the Gulf nation of Qatar, and asked for the release of prisoners held at the U.S. military prison in Guantanamo Bay. Article

JAN 3 - The United States will support Afghan-led efforts to reach a negotiated end to the war with the Taliban, including a possible Taliban political office in the Gulf state of Qatar if that is agreed by all sides, the U.S. State Department said on JAN 3. Article

JAN 2 - Pakistani Taliban factions and their allies have set up a council of elders in hopes of coordinating efforts against NATO troops in Afghanistan, a spokesman said. Article

JAN 2 - Afghanistan's national power company says it will cut the electricity supply to the main prison unless it pays its overdue bills in the next few weeks. It says it is contemplating similar action against several government departments which have also failed to pay bills. It estimates it is owed approximately $40m. Article

JAN 2 - In what could be the biggest change in a decade in a relationship that has been a mainstay of U.S. military and counterterrorism policy since the 9/11 terror attacks, the United States and Pakistan are lowering expectations for what the two nations will do together and planning for a period of more limited contact. Article

GAO:

JAN 6 – GAO released its report concerning the US Coast Guard finding that continued improvements were needed to address potential barriers to equal employment opportunity. Report

CONGRESS:

Note: Congress is currently in recess. The 2nd Session of the 112th Congress will convene on January 17, 2012. Announcement

JAN 3 – For a business community looking for any sign that the federal government is taking action on cybersecurity, a recent information-sharing bill from the House Intelligence Committee looks like a promising start, according to officials from the computer security firm McAfee. The measure (HR 3523), which the panel approved in early December, has attracted support from groups such as the U.S. Chamber of Commerce and the National Cable and Telecommunications Association. McAfee also has endorsed the measure. While some in the private sector have concerns about the legislation, it has received mostly positive reviews among industry leaders said Tom Gann, McAfee's vice president of government relations, and Phyllis Schneck, vice president and chief technology officer for the firm's global public sector. The officials told CQ that the bill represents a critical first step in establishing information-sharing relationships that will allow companies to better protect themselves and their customers. (See attached for CQ Article)

DEC 30 - The Disaster Relief Fund (DRF) administered by the Federal Emergency Management Agency (FEMA) received appropriations at the full level requested by FEMA for Fiscal Year (FY) 2012 through two spending bills signed by President Barack Obama last week -- the Consolidated Appropriations Act (Public Law 112-074) and the Disaster Relief Appropriations Act (PL 112-077). President Obama signed the bills into law on Dec. 23, funding the DRF with $700 million in the consolidated spending act and another $6.4 billion in the disaster relief legislation. Article

UPCOMING HEARINGS:

Nothing to report. Both house are in recess although the Senate has been meeting sporadically. The 2nd Session of the 112th Congress will convene on January 17, 2012.

THINK TANKS:

JAN 6: Successful Exercise Demonstrates Implementation of Nuclear Detection Architecture
http://blog.dhs.gov/

JAN 6 – Centre for Strategic and International Studies hosted a discussion of "The Al Qaeda Factor: Plots Against the West", a new book from Mitchell D. Silber, Director of Intelligence Analysis, Analytic and Cyber Units, New York City Police Department. The Al Qaeda Factor: Plots Against the West

JAN 5 – The Council on Foreign Relations published an interview with Michael Elleman, Senior Fellow for Regional Security Cooperation, International Institute for Strategic Studies on "How Serious are Iran's Threats?" Interview

JAN 5 – The Center for American Progress published an article by Ken Sofer and Jennifer Addison

"The Unaddressed Threat of Female Suicide Bombers - Women Terrorists an Increasingly a Problem" discussing why we need to acknowledge the growing number of female attacks in our counterterrorism strategy. Article

UPCOMING EVENTS:

JAN 10: The Centre for Strategic and International Studies will host: "The Future of the Internet – Who Decides?" 15:30-17:000 1800 K Street, N.W.

ARTICLES/ REPORTS OF INTEREST:

JAN 4: A Whole Community Approach to Emergency Management - **Posted by: David Kaufman, Director, Office of Policy and Program Analysis - FEMA Blog**

JAN 3 – Homeland Security Experts Weigh In: Where to Cut and Where to Spend. See attached for CQ Article)

JAN 2 - President Obama Signed The National Defense Authorization Act - Now What? Forbes. Article

JAN 2 - Homeland Security Experts Weigh In: The Year of the 'Lone Wolf'. (See attached for CQ Article)

DEC 29 - Terrorists Struggle To Gain Recruits On The Web. NPR. Article

Kathleen Tolan
Counsellor
Public Safety and Border Security
Public Safety Canada
501 Pennsylvania Avenue, N.W.
Washington, D.C. 20001-2114
Tel: (202) 448-6338 Cell: 202 497-5898
Fax: (202) 682-7792
Email: katie.tolan@international.gc.ca

Page 1298

is a duplicate

est un duplicata

Page 1299

is a duplicate

est un duplicata

Page 1300

is a duplicate

est un duplicata

Page 1301

is a duplicate

est un duplicata

Page 1302

is a duplicate

est un duplicata

Page 1303

is a duplicate

est un duplicata

Page 1304

is a duplicate

est un duplicata

Page 1305

is a duplicate

est un duplicata

Page 1306

is a duplicate

est un duplicata

DATE	SECTOR	INCIDENT/ACTIVITY #	TYPE OF INCIDENT	# OF AFFECTED ORGS	COMMENTS	ACTION (If applicable)
3 Jan 2012	Financial	CE11-2552 [Phishing] CE11-2553 [Trust Phishing]	Phishing		- 2552 appears to originate from Paris - 2553 is routed through Paris but directed to US server	
4 Jan 2012	Government (Fed, Prov/Dept Education) Transportation Universities	CE11-2554 [Sinkhole Notification – Multiple Organizations]	Hosts within these organizations were infected with DNS Changer malware.			
					Federal: Reported to Federal Gov't CERT Provincial: Reported to Provincial Department of Education Transportation: Reported to City's Airport Authority Academia: Reported to 4 Universities.	
5 Jan 2012	Telecom	CE12-2555 [Defacement hosting provider website] - Summary: CCIRC observed that a website operated by an Internet hosting service				

		provider located in Manitoba was recently defaced.				
	Financial	CE12-2556 [Phishing] -	- Summary: hxxp://charltonhats[.]com/admin[.]html - 63.247.80.138(Global Net Access – Atlanta Georgia). This site redirected to the final phishing page located at:			
		: CE12-1257 Phishing] -	- (Axarnet Communications – Malaga Spain)			
		CE12-2558 [Phishing]	- 62.193.220.178 (AMEN Networks, Paris France)			
	Government (Fed, Prov); Financial (banks)	CE12-2559 [Drone Notifications - Multiple Organizations]	- Infection types included (DNS Changer, Mebroot, or Torpig). : Federal: 2 departments (via CTEC) Provincial: 3 provincial governments Financial: 2 banks -			
	Fed Govt plus	CE11-2549 [Stratfor Hack affected Canadians]	- Summary: On December 25, 2011, the Anonymous group hacked into a private intelligence agency,			

			Strategic Forecasting Inc. or STRATFOR, based in Austin, Texas. The attack began with the release of STRATFOR's client list, followed by release of accounts in batches believed to belong to STRATFOR's customers. The release includes emails, passwords (hashed with MD5), home/office addresses and credit card information (full 16-digit number, expiry date and CVV number). CCIRC received a report from a LE regarding Stratfor account compromises. - Action/Decision: Update - A. Item: CCIRC received the first set of data, 40,235 compromised accounts. Results: 34 gc.ca accounts – sent to Federal Government CERT for notification. 1803 Canadians – analysing for CI notification. -			

International: IWWN Spring Meeting – Need to sign up – who's going from GoC?

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint principal

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE: JAN 0 9 2012

File No.: 384961
RDIMS No.: 541955

Seen by the DM
Vu par le SM

JAN 1 0 2012

MEMORANDUM FOR THE DEPUTY MINISTER

CANADIAN IMPACTS OF A RECENT DATA BREACH AT AN INTERNATIONAL PRIVATE INTELLIGENCE AGENCY

(Information only)

ISSUE

Eight hundred and eighty federal government workers and 109 provincial government users in nine provinces have been affected by the hacking of a private international intelligence agency.

BACKGROUND

On December 25, 2011, a private intelligence agency, Strategic Forecasting Inc. (STRATFOR), was compromised by the hacking entity Anonymous. Through twitter, they have released STRATFOR's client list including emails, passwords, home/office addresses and credit card information. This data breach involves approximately 75,000 credit card numbers and 860,000 login credentials.

CONSIDERATIONS

There are financial, workplace security, and privacy considerations regarding this incident.

First, there is a financial risk to all impacted individuals as the credit card information posted online contained the full 16 digit number, expiry date, and Card Verification Value number (i.e. everything needed to make purchases).

Second, compromised individuals could be victims of specific and targeted attacks, such as malicious emails, social engineering, and attempts to compromise workplace security.

Third, impacted individuals' privacy could be compromised as home/office telephone numbers and home/office addresses were released. Given the fact that 860,000 login credentials have been compromised, there is also a strong likelihood that additional downstream privacy risks exist for impacted individuals as a significant percentage of the population uses the same password for many Internet sites and work.

NEXT STEPS

There are three main actions that the Canadian Cyber Incident Response Centre (CCIRC) is taking to address this situation.

First, CCIRC is working with RCMP to identify federal government users registered with STRATFOR. Identified users will be notified through the Cyber Threat Evaluation Centre (CTEC).

Second, CCIRC has completed its analysis and identified provincial government users who have been affected. CCIRC has notified each provincial government's lead cyber security department.

Third, CCIRC has recommended that affected government employees change all Internet account passwords that use elements from their compromised password; monitor their credit card transactions and; contact their bank regarding the credit card breach.

CCIRC has closed this incident and will continue to monitor for any significant developments.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Robert Dick, Director General, National Cyber Security, at 613-990-2661.

Lynda Clairmont
Senior Assistant Deputy Minister
National Security

Prepared by: Nate Klassen
Sandra Williston

Deputy
This is useful background material for your meeting later this week with CCIRC.

Anderson, Windy

From: [redacted]
Sent: January-06-12 1:29 AM
To: dominic.lafleur@rcmp-grc.gc.ca
Subject: Rate Stratfor's Incident Response

For the video announcement, please see [redacted]
Read full press release: [redacted] Rate Stratfor's incident response:
[redacted]

Hello loyal Stratfor clients,

We are still working to get our website secure and back up and running again as soon as possible.

To show our appreciation for your continued support, we will be making available all of our premium content *as a free service* from now on.

We would like to hear from our loyal client base as to our handling of the recent intrusion by those deranged, sexually deviant criminal hacker terrorist masterminds. Please fill out the following form and return it to me

[redacted]

s.16(2)(c)
s.19(1)

Williston, Sandra

From: Clow, Patrick
Sent: December-29-11 2:30 PM
To: Galadza, Larisa
Cc: Di Paola, Rosanna; Hunter, Linda; Kravchenko, Christine; Davies, John; Banerjee, Ritu
Subject: RE: !!!IT SECURITY ALERT!!! - Stratfor hack affects Government of Canada Users

Hi Larisa,

In a nutshell, the password used to access the Stratfor web site was compromised and posted on a website. If that password happened to be the same password you use to access the PS network (or any other IT systems), we strongly recommend those passwords be changed ASAP.

As far as the credit card is concerned, if it was used to subscribe to any services that Stratfor offers it may be a good idea that the credit card company be advised of the issue.

I hope this helps.

Thank you

From: Galadza, Larisa
Sent: December-29-11 2:11 PM
To: Clow, Patrick
Cc: Di Paola, Rosanna; Hunter, Linda; Kravchenko, Christine; Davies, John; Banerjee, Ritu
Subject: Re: !!!IT SECURITY ALERT!!! - Stratfor hack affects Government of Canada Users

Hi Patrick - I don't actually remember the password for our Stratfor account; I only ever received their email bulletins on various news/analysis items. I don't entirely understand your email below -- e.g. I don't know what Password hash released but no broken password posted -- so I am not sure what else to do. In any case, my GoC system passwords have changed numerous times since we got our Stratfor account, so I don't think there's a risk there. Should we cancel the Credit Card?

Grateful for any further clarity you could provide. Thanks!

Larisa

From: Clow, Patrick
Sent: Thursday, December 29, 2011 01:06 PM
To: Galadza, Larisa
Cc: Di Paola, Rosanna; Hunter, Linda; Kravchenko, Christine
Subject: !!!IT SECURITY ALERT!!! - Stratfor hack affects Government of Canada Users

Hello Larisa,

CSEC has notified PS IT Security that your Stratfor.com password has been exposed (along with address and credit card information) and this may leave Government of Canada systems at risk if the passwords were the same as on other GC systems.

The hashes for all Stratfor accounts were released allegedly by the hacker group known as 'Anonymous'.

Password hash released but no broken password posted:
larisa.galadza@ps-sp.gc.ca

It is recommended that you immediately change any passwords on Government of Canada systems if they used the same or similar passwords. You are reminded that this case illustrates the importance of using different passwords on different accounts and especially not to reuse passwords that are used on GC systems.

If you have any questions or concerns, please do not hesitate to contact me.

Thank you

Patrick Clow, CISSP
Manager, IM/IT Security | Gestionnaire, Sécurité GI-TI
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West Ottawa ON K1A 0P8 | 269, avenue Laurier ouest Ottawa ON K1A 0P8
Phone: 613-949-9530
Cell: 613-219-1954
Fax: 613-944-4046
Email | Courriel: Patrick.Clow@ps-sp.gc.ca

Williston, Sandra

From: Clow, Patrick
Sent: December-29-11 2:07 PM
To: Mulder, Rene
Subject: Re: Stratfor hack affects Government of Canada users

s.15(1) - Def
s.16(2)(c)

Baal might be able to tell you if they're in [redacted]

From: Mulder, Rene
Sent: Thursday, December 29, 2011 01:54 PM
To: Clow, Patrick
Subject: RE: Stratfor hack affects Government of Canada users

[redacted] but there doesn't seem to be a difference [redacted]s. I've written [redacted]

From: Clow, Patrick
Sent: Thursday, December 29, 2011 1:39 PM
To: Mulder, Rene
Subject: Re: Stratfor hack affects Government of Canada users

Are you able to confirm [redacted] by any chance?

From: Mulder, Rene
Sent: Thursday, December 29, 2011 01:37 PM
To: Clow, Patrick
Subject: RE: Stratfor hack affects Government of Canada users

Hard core!!!

From: Clow, Patrick
Sent: Thursday, December 29, 2011 1:31 PM
To: Mulder, Rene
Subject: FW: Stratfor hack affects Government of Canada users
Importance: High

FYI

[redacted] No action required at this point.

From: [redacted]
Sent: December-29-11 12:03 PM
To: Boal, Bridgit; Clow, Patrick
Cc: [redacted]
Subject: Stratfor hack affects Government of Canada users
Importance: High

Classification: UNCLASSIFIED

Hello,

[redacted]

The hashes for all Stratfor accounts were released allegedly by Anonymous. Some passwords were discovered via a dictionary attack and posted on pastebin [redacted];

[redacted]

[redacted]

It is recommended that users immediately change any passwords on Government of Canada systems if they used the same or similar passwords. Please remind users that this illustrates the importance of using different passwords on different accounts and especially not to reuse passwords that are used on GC systems.

[redacted] If any unusual activity is discovered please report it to GC-CTEC.

Regards,

[redacted]

s.15(1) - Def
s.16(2)(c)

[redacted]
GC-CTEC Cyber Duty Officer

Williston, Sandra

From: Clow, Patrick
Sent: December-29-11 1:03 PM
To: Di Paola, Rosanna
Subject: RE: !!!IT SECURITY ALERT!!! - Stratfor hack affects Government of Canada Users

[redacted]....I'll call you in a couple of minutes.

From: Di Paola, Rosanna
Sent: December-29-11 1:03 PM
To: Clow, Patrick
Subject: RE: !!!IT SECURITY ALERT!!! - Stratfor hack affects Government of Canada Users

[redacted]

Rosanna Di Paola
Chief Information Officer | Dirigeante principale de l'information
Public Safety Canada | Sécurité publique Canada
Tel | Tél: 613-944-4878
Fax | Fac: 613-954-8660
Mobile: 613-769-6930
Email | Courriel: rosanna.dipaola@ps-sp.gc.ca

Administrative Officer | Adjointe administrative: Jean-Bernard Rochefort jean-bernard.rochefort@ps-sp.gc.ca au 613-992-8885

From: Clow, Patrick
Sent: Thursday, December 29, 2011 1:00 PM
To: Banerjee, Ritu
Cc: Di Paola, Rosanna; Hunter, Linda
Subject: !!!IT SECURITY ALERT!!! - Stratfor hack affects Government of Canada Users
Importance: High

Hello Ritu,

[redacted]

The hashes for all Stratfor accounts were released allegedly by the hacker group known as 'Anonymous'.

[redacted]

If you have any questions or concerns, please do not hesitate to contact me.

Thank you

Patrick Clow, CISSP
Manager, IM/IT Security | Gestionnaire, Sécurité GI-TI
Public Safety Canada | Sécurité publique Canada
269 Laurier Avenue West Ottawa ON K1A 0P8 | 269, avenue Laurier ouest Ottawa ON K1A 0P8
Phone: 613-949-9530
Cell: 613-219-1954
Fax: 613-944-4046
Email | Courriel: Patrick.Clow@ps-sp.gc.ca

Williston, Sandra

From: Darren Sabourin [redacted]
Sent: December-28-11 2:27 AM
To: [redacted]
Cc: dave.bachynski@rcmp-grc.gc.ca; Darren - Work; Brian Ferguson; Tim O'Neil; Tiago Alves de Jesus
Subject: Re: Release of Canadian Government and Corporate usernames and passwords
Attachments: specialforces_full.txt

As an update to my previous emails:

1. Stratfor - in my discussions with various Canadian Energy stakeholders in my area, I can confirm that at least 2 have received "spearphishing-type" emails today (Tuesday) which notify them that their information has potentially been recently compromised, and they should follow an attached link to "change their password".

2. The site "specialforces.com" has also purportedly been breached by Anonymous, with 18,000+ email addresses, names and passwords being exposed. Among them are many Canadian users, including those with Government and Corporate email addresses.

Like with Stratfor, a database appears to have been compromised. The links to download the entire 18,000+ names, email address, passwords, company was posted to Twitter at #LulzXmas.

I see today that there is a posting on the Twitter site stating "its fair to assume that if you are one of these lists you WILL get phished or targeted". The posting can be seen as an open invitation.

I would agree that this is quite possible given the positions that may of the Stratfor clients held within their corporations.

Attached is the published list from the specialforces.com website breach.

Darren

Cpl. Darren Sabourin
Technological Crime Unit
Royal Canadian Mounted Police
Regina, SK
w. (306) 780-7334

s.16(2)(c)
s.19(1)

On Tue, Dec 27, 2011 at 12:29 PM, [redacted] wrote:

Hi Darren,

I have at least forward the information to CTEC for the affected Gov of Canada users.

Again thank for your research.

Vireak Phlek

Pages 1321 to / à 1566

are withheld pursuant to section

sont retenues en vertu de l'article

19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Page 1567

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 1568 to / à 1572

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 1573 to / à 1769

are withheld pursuant to section

sont retenues en vertu de l'article

19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Page 1770

is withheld pursuant to section

est retenue en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 1771 to / à 1774

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 19(1)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 1775 to / à 1780

are withheld pursuant to section

sont retenues en vertu de l'article

16(2)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From:
Sent: December-27-11 1:30 PM
To: Darren Sabourin
Cc:
Subject: RE: Release of Canadian Government and Corporate usernames and passwords

Hi Darren,

I have at least forward the information to CTEC for the affected Gov of Canada users. Again thank for your research.

s.16(2)(c)
s.19(1)

Vireak Phlek

From: Darren Sabourin [mailto:darren.sabourin
Sent: December-26-11 10:47 PM
To: Brian Ferguson
Cc: dave.bachynski@rcmp-grc.gc.ca; Darren - Work; Tim O'Neil; Tiago Alves de Jesus
Subject: Re: Release of Canadian Government and Corporate usernames and passwords

I am sending the attachment

I have obtained more information on the Stratfor incident, and it appears that the exposure of personally identifiable information appears to be more serious.

I have located several documents detailing the full account information of what is purported to be Stratfor clients. From a preview of this information, it appears that hundreds of Canadian's (including Corporate and Fed Gov't) have been affected, including:

- name, address and phone numbers
- email addresses
- username for account
- passwords (most are displayed as the MD5 hash)
- credit card number, expiry and CVV numbers

The lists is very detailed and complete. My concerns are as follows:

a. The lists contains full credit card information, most of which are have valid expiry dates and CVV information.
b. The lists contain usernames and passwords (often MD5). This information may be used in other accounts accessed by these account holders, with the same passwords (or similar).

c. The lists contain the email addresses of their clients, often with clear association to the companies they represent.

Given the nature of the business conducted by Stratfor, it follows that many of their customers have fairly strategic positions within the companies they represent. Many of the Canadian companies are obviously

identifiable [redacted]

If I can suggest, it may be worthy to note the possibility that these addresses may be harvested for Spearphishing efforts - possibly with a theme of being their Statfor credentials being stolen.

Attached are the following documents. I have kept all in .txt format and [redacted]

[redacted]

I opened the documents with Notepad++; however, MSWord may also allow for a more readable document as well.

[redacted] 'Anonymous" has indicated that more documents are pending. All documents released have been posted to public sharing websites.

Some of my key stakeholders have been advised where it it directly affects their respective corporations. Many of the clients are in various security positions within the corporations.

[redacted] but feel free to communicate with this email, or leave a message at my desk phone number noted below [redacted]

Cpl. Darren Sabourin
Technological Crime Unit
Royal Canadian Mounted Police
Regina, SK
w. (306) 780-7334

s.16(1)(a)
s.16(1)(b)
s.16(2)(c)
s.19(1)

Williston, Sandra

From: [redacted]@CSE-CST.GC.CA>
Sent: December-27-11 1:22 PM
To: CTEC; [redacted]
Subject: Re: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

Thanks Vireak,
We will follow up on this.

Cheers
[redacted]
GC-CTEC Cyber Duty Officer

From: CTEC
To: [redacted]
Sent: Tue Dec 27 13:15:59 2011
Subject: FW: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]

From: [redacted]@PS-SP.GC.CA]
Sent: Tuesday, December 27, 2011 1:13:50 PM
To: CTEC
Cc: [redacted]
Subject: CCIRC CE11-2549 [Stratfor hack affects Gov of Canada users]
Auto forwarded by a Rule

Greetings GTEC,

We have received a report from a partner that did a research on Stratfor hack mentioned in different news outlet (http://www.cbc.ca/news/world/story/2011/12/25/anonymous-hackers.html). [redacted]

[redacted]

On those different files there are Full name, email, password(md5) and physical address.

[redacted]

Please acknowledge.

s.15(1) - Def
s.16(2)(c)
s.19(1)

Thanks

Vireak Phlek
Cyber Duty Officer
Public Safety Canada
CCIRC
613-991-7000

s.16(2)(c)
s.19(1)

Williston, Sandra

From: Timothy O'Neil <tim.oneil@rcmp-grc.gc.ca>
Sent: December-27-11 5:38 AM
To: darren.sabourin Brian Ferguson
Cc: Darren Sabourin; Dave Bachynski; Tiago Alves de Jesus
Subject: Re: Release of Canadian Government and Corporate usernames and passwords

Thanks Darren. I will review from my office computer. Tim

Sent from my BlackBerry

Tim O'Neil
Senior Criminal Intelligence Research Specialist Critical Infrastructure Intelligence Team National Security Criminal Investigations
613-949-0265
E-mail: tim.oneil@rcmp-grc.gc.ca

-----Original Message-----
From: Darren Sabourin <
Cc: Sabourin, Darren <Darren.Sabourin@rcmp-grc.gc.ca>
Cc: Bachynski, Dave <Dave.Bachynski@rcmp-grc.gc.ca>
To: Ferguson, Brian <Brian.Ferguson@rcmp-grc.gc.ca>
Cc: O'Neil, Timothy <tim.oneil@rcmp-grc.gc.ca>
Cc: Alves de Jesus, Tiago <Tiago.Dejesus@rcmp-grc.gc.ca>
To:

Sent: 26/12/2011 10:46:32 PM
Subject: Re: Release of Canadian Government and Corporate usernames and passwords

---

I have obtained more information on the Stratfor incident, and it appears that the exposure of personally identifiable information appears to be more serious.

I have located several documents detailing the full account information of what is purported to be Stratfor clients. From a preview of this information, it appears that hundreds of Canadian's (including Corporate and Fed Gov't) have been

- name, address and phone numbers
- email addresses
- username for account
- passwords (most are displayed as the MD5 hash)
- credit card number, expiry and CVV numbers The lists is very detailed and complete. My concerns are as follows:

a. The lists contains full credit card information, most of which are have valid expiry dates and CVV information.
b. The lists contain usernames and passwords (often MD5). This information may be used in other accounts accessed by these account holders, with the same passwords (or similar). The MD5 values can be cracked online by at several online websites offering such services.
c. The lists contain the email addresses of their clients, often with clear association to the companies they represent.

Given the nature of the business conducted by Stratfor, it follows that many of their customers have fairly strategic positions within the companies they represent.

If I can suggest, it may be worthy to note the possibility that these addresses may be harvested for Spearphishing efforts - possibly with a theme of being their Statfor credentials being stolen.

Attached are the following documents.

I opened the documents with Notepad++; however, MSWord may also allow for a more readable document as well.

I will continue to research this matter as "Anonymous" has indicated that more documents are pending. All documents released have been posted to public sharing websites.

or leave a message at my desk phone number noted below (

Cpl. Darren Sabourin
Technological Crime Unit
Royal Canadian Mounted Police
Regina, SK
w. (306) 780-7334

s.16(1)(a)
s.16(1)(b)
s.16(2)(c)
s.19(1)

Williston, Sandra

From: Darren Sabourin <darren.sabourin
Sent: December-26-11 4:59 PM
To:
Cc: dave.bachynski@rcmp-grc.gc.ca; Darren - Work; Brian Ferguson; Tim O'Neil; Tiago Alves de Jesus
Subject: Release of Canadian Government and Corporate usernames and passwords

Recent media has announced that "Anonymous" has hacked into the US-based Intelligence thinktank Stratfor.

Usernames (email address) and passwords of Canadian Government and private Corporate accounts.

[redacted]

Media has picked up on these releases ie: http://www.latimes.com/business/la-fi-hacker-christmas-20111226,0,7419423.story and Stratfor appears to have released a public statement as well.

[redacted]

Darren

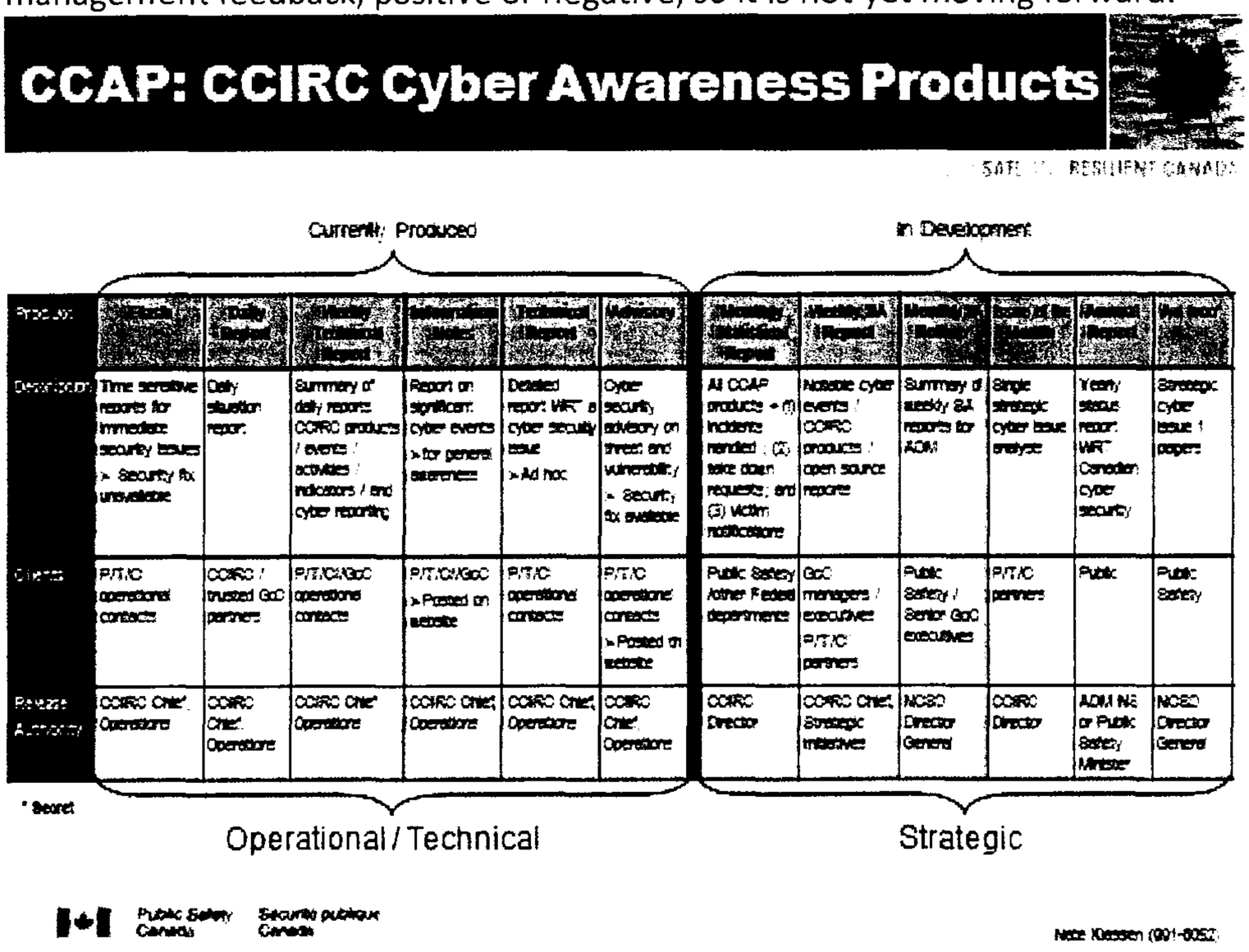
Cpl. Darren Sabourin
Technological Crime Unit
Royal Canadian Mounted Police
Regina, SK
w. (306) 780-7334

s.15(1) - Subv
s.16(1)(a)
s.16(1)(b)
s.16(2)(c)
s.19(1)

Anderson, Windy

From: Cameron, Bud
Sent: December-23-11 9:20 AM
To: McAllister, Andrew
Cc: Anderson, Windy; Beaudoin, Luc S
Subject: Example products
Attachments: PS-SP-#522113-v2-CCIRC_-_policy_-_Cyber_Awareness_Products_-_details_for_coms_-_November_23__2011.PPT; PS-SP-#534501-v1-CCIRC_template_-_v3.DOC; AV11-035_BILINGUAL.txt; AL11-501_EN_UPDATE.txt; CF11-021_EN.txt; CCIRC Situation Report 10 Nov 11.doc; Weekly_Technical_Report_19_Oct_2011.pdf; IN11-507_EN.txt; TR11-001_BILINGUAL.txt

Andrew, as you know we have always sent out the CCIRC products in text format, as the lowest-common-format with no compatibility issues and no risk of being seen as potentially infected (as could be the case for pdf, Office files). This is still the case. The proposed portfolio of products, existing plus those requested by NCSD340, has been briefed to Robert using the attached slides. The CCIRC plan was to call all the products CCIRC Cyber Awareness Products (CCAP) and then have categories including the familiar Flash, Advisory, and the new Reports for SA. This plan has never been given any management feedback, positive or negative, so it is not yet moving forward.



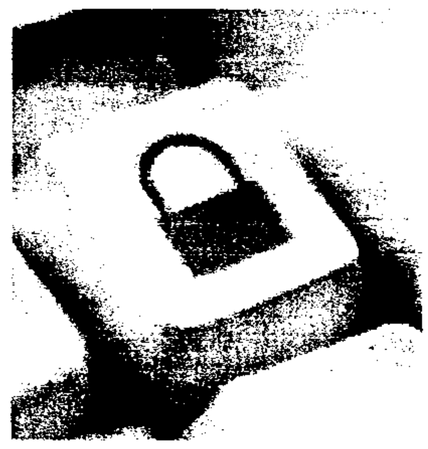
For our draft SA products, we have been using Word and have been experimenting with the format but again, without any feedback from NCSD340. We have a new template with a cool watermark that we would like to use, attached.

Product examples: all attached except for the Weekly Report and an Issue of the Month which I will send separately.

Bud Cameron, CD, MSc
Manager, Cyber Security Programs | Gestionnair, Programmes de sécurité cybernétique
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 +1 613-949-8317
Facsimile | Télécopieur +1 613-954-3097
Bud.Cameron@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-006



For the Week of

19 Nov – 25 Nov 2011

Issued: 1 Dec 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released/Activities:** CCIRC notified 147 Canadian organizations who were affected by Operation "Ghostclick" (reported last week) and offered mitigation advice.

- **Incidents to report:** (1) Newspaper website user credentials stolen; (2) An update on the domain name registrar's customer list theft and misuse reported last week; (3) Financial institution's website vandalized; (4) Threat actors impersonating Canadian a financial institution, luring internet users to malicious websites (phishing);

- **International:** UK Government releases updated Cyber Security Strategy and Program worth £650m over four years to strengthen the UK's cyber capabilities.

- **Noteworthy Open Source Reports:** (1) UK banks undergo for cyber security 'stress test'; (2) More Facebook scams.

s.16(1)(b)
s.16(2)(c)

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and other noteworthy open source reports.

NOTABLE INCIDENTS– 19 NOVEMBER THROUGH 25 NOVEMBER 2011:

Canadian Critical Infrastructure:

Multi Sector Event Update. CCIRC notified 147 organizations in multiple sectors that were affected by Operation "Ghostclick", the massive DNS changer fraud exposed by the FBI two weeks ago and reported in the last two CCIRC Weekly Summary reports. Canadian organizations that were notified this week included internet service providers, information technology companies, post-secondary schools, health and media organizations.

- **Analysis:** This was a world-wide fraud where victims are still being continued to notified by CCIRC and its international equivalents around the world. It is said that the fraud went on for four years.

Financial Sector.

Threat actors impersonating well known financial entities attempted to steal personal information by persuading internet users to click on links to malicious websites (phishing). CCIRC found one malicious website still in operation and notified the entity being impersonated. [redacted] so internet users may be alerted if they encounter these specific malicious websites. The number of victims is unknown.

- **Analysis:** This type of malicious activity is commonly seen by CCIRC and continues to cause financial losses for Canadians. It is known that the malicious website [redacted]

CCIRC also learned that the website of a financial institution was vandalized. CCIRC notified the organization of this website defacement and offered mitigation advice.

- **Analysis:** This type of malicious activity usually does not put a financial institution's operations in jeopardy but could threaten the visitors to that website. A website defacement does, however, indicate the vulnerability of the website to malicious activity by threat actors. A common malicious activity is placement of malicious software on the website that would be passed on to any visitor to that

website, and compromise his/her computer, then steal information or use it to send SPAM e-mails anonymously.

Telecommunications Sector – an Update.

Last week CCIRC reported that a [redacted] was victim of a cyber attack, and that its stolen customer contact list was then used by criminals to persuade customers to provide their credit card numbers. [redacted]

- **Analysis:** While CCIRC regularly sees threat actors impersonating trusted entities to persuade internet users to give their personal and financial information, this is the first time in recent memory [redacted] has been successfully targeted. The impact of a trusted entity's compromise can be much greater than an individual or an organization. [redacted]

Public. CCIRC a Canadian newspaper website's special section's user credentials were stolen. The loss of these credentials would lead to the compromise of these users' personal information.

- **Analysis:** The newspaper's special section is aimed at a specific reader group, which is a small subset of this newspaper's regular readership. However, the stolen user credentials were posted on the internet and could allow any threat actor to gain access to these users' personal information such name, address, phone number and workplace. Unfortunately, this type of compromise is being seen on a regular basis in Canada.

CCIRC Products/Activities: Nothing to report

International:

UK releases updated Cyber Security Strategy. The UK government released an update to its Cyber Security Strategy, which was published two years ago. There is an increased emphasis on information sharing between the public and private sector, reaching out to industry sectors hitherto not considered as part of UK's critical infrastructure, and increased military capability in cyber security to gain comparative advantage. Increased efforts to improve the public's cyber security include working with internet service providers to develop a voluntary code of conduct to help their customers when they suspect their computer has been compromised. In addition, a new Cyber Crime Unit within the National Crime Agency will be created.UK Government intends to continue working internationally to help improve cyber security in the UK and the world.

The National Cyber Security Programme based on this strategy has been allocated £650m over the next four years.

- **Analysis:** The UK sees cyber security in terms of national security and economics. The UK government publicly stated that their aim was to make UK a safe place to do business online, and gave warning it intended to deter and defend itself against advanced threats by nation-states. The Government of Canada released its own cyber security strategy in 2011, which, similarly, focuses on protecting government systems, working with the private sector to protect critical infrastructure systems and help Canadians to be secure online. These initiatives have been allocated $90M over five years. Canada will be watching UK implement this updated strategy with great interest and learn lessons that can be applied in Canada. Canada is a strong partner of the UK in helping determine the global "rules of the road" for cyber security.

Noteworthy Open Source Reports:

UK banks set for cyber security 'stress test'. 87 British banks, including major institutions such as Barclays, HSBC and Royal Bank of Scotland, took part in a simulation exercise that tested their defences against a cyber attack. The test scenarios included automated teller machines (ATMs) being down due to a cyber attack. The exercise also examined how financial institutions would cope if there was a major disruption to the transport infrastructure during the London 2012 Olympic Games. An Exercise Report discussing the results of the test is expected to be published in early 2012. The Financial Services Authority stated there would also be a Post Exercise Conference.

- **Analysis:** It is likely that the London 2012 Olympic Games were a factor in prompting this cyber security exercise. That said, cyber security is an extremely important topic in the UK and is near the top of the UK Government's agenda. The updated UK Cyber Security Strategy was released publicly 25 November 2011 and states the private sector is expected to share more information and to play a more active role in the nation's cyber security.

More Facebook scams reported. Open sources reported two separate scams on Facebook, targeted at Facebook customers. In the first instance, threat actors reportedly impersonated Facebook administrators and sent e-mails to users charging them with violating policy regulations. Users were then asked to pass along their account details, which included personal and financial information.

In the second instance, which occurred during American thanksgiving weekend, Facebook users were lured to give up their personal information by an offer of a program that would allow watching live streaming video of football games. The number of

victims in both instances is unknown, though many Facebook users did report these spams to the legitimate Facebook support site.

- **Analysis:** Facebook is one of the world's most popular social networking websites. There are reportedly 16.6 Million Facebook users in Canada. The largest user age group is 18-24 years old. Federal public servants were recently encouraged by the President of Treasury Board to use social media in the course of their work. The Government of Canada has just released guidelines for the use of social media by Government Departments called "Guidelines for the External Use of Web 2.0". These guidelines encourage the use of social media and suggests federal departments appoint a senior official who will set up a governance structure to ensure compliance.

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

The following minutes capture the discussions and presentations which took place at the Usual 5 meeting in London between Wednesday 29th June and Friday 1st July 2011. The meeting took place in CPNI. They do not cover specific operations which were discussed at a classified level.

Attendees:

[redacted]

AGENDA

Day One – Wednesday 29th June 2011

[redacted]

Page 1796

is withheld pursuant to section

est retenue en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

Session Four: Canadian Update
Luc represented Public safety - CCIRC: National CERT (CI systems, Provinces, Key Partners, Security Vendors/Academia)
[redacted] represented CTEC: Government CERT for government systems.

The CERT roles in Canada changed on June 20th and both teams will work together sharing information and supporting each others roles (CTEC as GovCERT, and CCIRC as National CERT). Staffing: There are now 10 people in CCIRC with plans to extend further. Canada is also working with the USA to increasing their collaboration in the area of security, including cyber security (also referred to as "Beyond Border" initiative). Operationally Luc confirmed that they are seeing bulk phishing and targeted emails.

Luc also highlighted the CTU as an information sharing forum for triage and coordination between mitigation efforts, national security and criminal investigation. Also, GOVIRT a weekly community update (similar to GFirst) and that they working at developing relationships with Universities and R&D organisations. On the Critical Infrastructure side (Energy, Finance, Telecoms) Industry Canada look after telecommunications physical and cyber incidents (CTCP - public/private Telecoms incident group, affiliated with NSIE).

The CRC, under Industry Canada, is an R&D organisation with a Cyber Security Program which CCIRC collaborate with. Other R&D is done jointly with Defence R&D Canada, including a SCADA test-bed project. CCIRC often exchange information with US-CERT and the FIRST community. [redacted] Luc also mentioned using [redacted] information for victim notification and using services such as Virus Total and Threat Experts to share information in a non partisan way.

[redacted]

s.13(1)(a)

s.15(1) - Def

s.16(1)(b)

Pages 1798 to / à 1800

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Day Two – Thursday 30th June 2011

[redacted]

Session Two: Operational – 2010/11 Experiences

Operational issues were discussed which included: Resourcing issues such as how long it takes to refine product and filter out relevant information for audiences versus handling the actual incident.

[redacted]

Session Three: Secure Communications

[redacted]

[redacted]

Session Six: Visit to the Olympic Park.

Delegates were provided with a private tour of the park.

Day Three – Friday 1st July 2011

[redacted]

s.13(1)(a)

Page 1803

is withheld pursuant to section

est retenue en vertu de l'article

13(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Williston, Sandra

From: Bendelier, Kenneth
Sent: December-19-11 1:16 PM
To: [redacted]
Cc: Beaudoin, Luc S
Subject: FW: Crawls

s.15(1) - Def
s.16(1)(a)
s.16(2)(c)
s.20(1)(b)

[redacted] Not a whole bunch of info. We're not supposed to pass it around, [redacted]

From: [redacted]
Sent: December-19-11 12:58 PM
To: Tiago.Dejesus@rcmp-grc.gc.ca; [redacted] Bendelier, Kenneth
Cc: [redacted]
Subject: FW: Crawls

FYI
Any intel you can share?

[redacted]

Pages 1805 to / à 1806

are withheld pursuant to sections

sont retenues en vertu des articles

19(1), 20(1)(b), 20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

Anderson, Windy

From: Labelle, Sébastien
Sent: December-16-11 9:41 AM
To: Hatfield, Adam; Anderson, Windy; Dick, Robert; Gordon, Robert; Dvorkin, Corey
Cc: Panchyson, Dorian; Pitcher Robert; Bencke, Ashley
Subject: FW: International Nuclear Security Event Notification - SECURITY OF INFORMATION TECHNOLOGY (IT) & INSTRUMENTATION AND CONTROL (IC) SYSTEMS AT NUCLEAR FACILITIES Workshop - Toronto Canada - 27 -29 Feb 2012
Attachments: Workshop Cyber Security - Announcement 4th draft.docx

FYI – the Canadian Nuclear Safety Commission is partnering with a number of organisations such as the World Institute for Nuclear Security and Atomic Energy of Canada to host a workshop on Nuclear Cyber Security. The program is attached, and looks quite interesting. We met with the Commission at the Energy Sector meeting in November, and they have invited us to attend.

The event appears to be quite technical, and I would like to get a sense of whether you think this would be useful. They have requested a response by today, but I could ask for an extension if we need more time.

Cheers,
SL

Sébastien Labelle
Director of National Cyber Security Engagement and Partnerships /
Directeur national des Partenariats et de l'Engagement pour la cyber sécurité
National Cyber Security Directorate / Direction générale de la Cyber sécurité nationale
Public Safety Canada / Sécurité publique Canada
Room / pièce 11C079, 340 Laurier, Ottawa, ON,
tel 613-990-2655 ; fax 613-990-3287; mob 613-614-5263
sebastien.labelle@ps-sp.gc.ca

From: Beaudette, Michael [mailto:Michael.Beaudette@cnsc-ccsn.gc.ca]
Sent: December-14-11 12:58 PM
To: Beaudette, Michael
Cc: Awad, Raoul
Subject: International Nuclear Security Event Notification - SECURITY OF INFORMATION TECHNOLOGY (IT) & INSTRUMENTATION AND CONTROL (IC) SYSTEMS AT NUCLEAR FACILITIES Workshop - Toronto Canada - 27 -29 Feb 2012

CNSC is assisting in the facilitation of a three day, international WINS workshop focusing on: SECURITY OF INFORMATION TECHNOLOGY (IT) & INSTRUMENTATION AND CONTROL (IC) SYSTEMS AT NUCLEAR FACILITIES to be conducted 27-28-29 Feb 2012 in Toronto, Ontario Canada . (A draft Agenda is attached.)

We are currently compiling an invitation list of key organizations that would likely benefit the most from this event. If you are receiving this e-mail, it is either because you have already expressed interest in attending or because I believe the event may be of interest / benefit to your organization.

If your organization is interested in participating, I would appreciate it if you could reply to by Friday 16 Dec with the name and contact information (e-mail and mailing address) of who should receive the invitation. Due to the large international participation expected, there are a limited number of invitations for Canadians & US attendees available so please provide only one representative name per organization. Thanks.

Should you have any questions, please feel free to contact me at the numbers below.

Best regards,

Mike

Michael J. Beaudette
Director / Directeur
Nuclear Security Division / Division de la sécurité nucléaire
Directorate of Security and Safeguards / Direction de la sécurité et des garanties
Canadian Nuclear Safety Commission / Commission canadienne de sûreté nucléaire
Phone (Office): 613.943-3085
BBerry: 613 697-4154

WORLD INSTITUTE FOR NUCLEAR SECURITY

WORKSHOP ANNOUNCEMENT

THE WORLD INSTITUTE FOR NUCLEAR SECURITY (WINS),
ATOMIC ENERGY OF CANADA LIMITED (AECL),
BRUCE POWER, AND
ONTARIO POWER GENERATION (OPG)

ARE PLEASED TO ANNOUNCE AN INTERNATIONAL BEST PRACTICE WORKSHOP ON

SECURITY OF INFORMATION TECHNOLOGY (IT) & INSTRUMENTATION AND CONTROL (IC) SYSTEMS AT NUCLEAR FACILITIES

FEBRUARY 27-29, 2012 - DELTA CHELSEA HOTEL IN TORONTO, ONTARIO, CANADA

With the support from:

Canada

AECL EACL

ONTARIO POWER GENERATION

Bruce Power

01809

WORLD INSTITUTE FOR NUCLEAR SECURITY

INTRODUCTION AND AIMS

The workshop will provide participants with the opportunity to share operational experiences and lessons learned from cyber security programmes implemented at nuclear facilities and other critical infrastructures.

This event will contribute to the identification and sharing of best practices for the design, implementation and testing of security arrangements for the protection of information technology (IT) and instrumentation and control (IC) systems at nuclear facilities.

The workshop will cover the key components of an effective and integrated risk management process to protect IT and related systems at nuclear facilities. It will also discuss potential weaknesses and security solutions for access control or any other physical protection measures using computer based systems.

The workshop will offer networking opportunities and a foundation for further follow-up to promote effective cyber security concepts and practices in nuclear and related disciplines, and will strengthen nuclear operators' capabilities to prevent, detect and respond to cyber attacks.

ATTENDANCE BY INVITATION

Attendance is by invitation only and is limited to 120 international delegates who have direct responsibility for security implementation, regulation or policy at nuclear facilities or other critical infrastructures. The event will focus on process operators, safety and security specialists and IT security experts.

Attendees will be expected to meet their own costs for travel and accommodation but all workshop costs will be met by organisers.

WINS may contribute to the attendance costs of potential delegates from developing countries if they have responsibilities that are highly relevant to this workshop.

The workshop will be held in English.

This international best practices workshop is supported by the Canadian Nuclear Safety Commission (CNSC) and the Foreign Affairs and International Trade Canada (DFAIT)

FACILITATED WORKSHOP

In line with WINS' innovative approach to Best Practice Workshops, the workshop will be interactive and professionally facilitated. The event will be built around a number of presentations from invited expert speakers and breakout sessions to further explore cyber security concepts and good practices. An Instant Electronic Voting system will be used to allow participants to anonymously "vote" using keypads, providing their views on questions put to the workshop. All participants need is expertise, enthusiasm and a willingness to engage with their peers. Discussions will be subject to "Chatham House" rules (what was said can be reported but not attributed). Key points will be recorded on flipcharts which will be used to support the revision of the WINS Best Practices Guide on *Security of IT & IC Systems at Nuclear Facilities*.

AECL EACL

ONTARIO POWER GENERATION

Bruce Power

WORLD INSTITUTE FOR NUCLEAR SECURITY

OUTLINE PROGRAMME

The workshop presentations, plenary discussions and breakout sessions will cover the following areas:

UNDERSTANDING THE THREATS, RISKS AND LATEST DEVELOPMENTS

- ✓ Understanding the complexity and the role of IT & IC systems in the management of a nuclear process, and the potential consequences of malicious acts on the IT & IC infrastructure.
- ✓ Distinguishing between perceived threats, artificial threats and real threats. Maintaining the threat assessment up to date in a rapidly changing environment.
- ✓ Defining characteristics and attributes of credible threats to the security of IT & IC systems and discussing the role and structure of the Design Basis Threat (DBT) for Nuclear IT & IC security.

SECURITY, IT AND NUCLEAR ENGINEERING PROFESSIONALS WORKING TOGETHER

- ✓ Clarifying the role, responsibilities and organisational structure for security, nuclear engineering and IT departments. Identifying where accountability lies for IT & IC security. Building a framework for Industry-wide Cyber security.
- ✓ Identifying and sharing good practices in the management of IT & IC security at nuclear facilities.
- ✓ Developing a common terminology between physical protection, IT experts and engineering professionals. Breaking down internal communication barriers.

DETECTING AND RESPONDING TO ATTACKS INVOLVING IT & IC SYSTEMS

- ✓ Reviewing methodologies and tools for detecting and assessing cyber attacks. Defining the content of a response plan. Identifying challenges and possible solutions when defining a response plan.
- ✓ Reviewing case studies involving early detection and discussing opportunities for countering potential and actual attacks. Discussing effectiveness and impact of remedial actions.
- ✓ Defining cyber security incident investigation and reporting activities. Discussing challenges encountered in investigations and possible solutions.

REGULATORY REQUIREMENTS AND INDUSTRY CODES AND STANDARDS

- ✓ Reviewing already existing industry codes and regulatory requirements.
- ✓ Discussing how useful, effective, and comprehensive they are. Identifying possible gaps.
- ✓ Discussing emerging trends in standards and codes, and if the nuclear industry needs its own standards.

IT & IC SECURITY MEASURES AND ADVANCED TECHNOLOGY

- ✓ Discussing how changes in technologies can impact threats and vulnerabilities. Reviewing examples of technology, design practices, and tools that have been used with good results to eliminate/mitigate vulnerabilities and detect threats/active attacks.
- ✓ Integrating IT & IC security within the overall risk management process.

AECL EACL ONTARIO POWER GENERATION Bruce Power

WORLD INSTITUTE FOR NUCLEAR SECURITY

✓Discussing the role of vendors in supporting IT security and associated procurement challenges. Identifying best practices for the procurement and maintenance of software /hardware.

ASSESSING THE EFFECTIVENESS OF IT & IC SECURITY MEASURES

- ✓Reviewing common methodologies and practices for testing and validating security provisions.
- ✓Identifying relevant security indicators and performance metrics. Benchmarking.
- ✓Integrating IT and physical security assessment together. Obtaining approval of the Regulatory Authority.

IMPROVING SECURITY CULTURE

- ✓Understanding and promotion of threat and security issues. Effectively communicating the threat and associated risks to all levels. Getting support and buy in from upper management and all levels.
- ✓Educating staff including what and how. Addressing the social engineering and phishing attacks.
- ✓Measuring tools and incentive.

LOCATION AND HOTEL

The workshop will be held at the Delta Chelsea hotel in Toronto, Ontario, Canada. (www.deltahotels.com/en/hotels/ontario/delta-chelsea)

A number of rooms have been blocked for the participants at the rate of CAD$ 149. Further details regarding room reservations will be made available to accepted applicants.

AECL EACL

ONTARIO POWER GENERATION

Bruce Power

Dincoy, Rana

From: St-Louis, Danielle
Sent: December-09-11 1:47 PM
To: [redacted] Champoux, Martin; Coady, Therese; Danaitis, Algis; Dick, Robert; Dole, Natalie; Dvorkin, Corey; Hatfield, Adam; Labelle, Sébastien; Panchyson, Dorian; Selman, Semira
Subject: CCIRC WEEKLY SUMMARY FOR WEEK OF 28 NOV
Attachments: PS-SP-#527919-v1-FEEDBACK_FORM_FOR_WEEKLY_SUMMARY_FOR_EXECS.DOC; PS-SP-#529606-v3-CCIRC_WEEKLY_SUMMARY_FOR_WEEK_OF_28_NOV_2011.doc

Good afternoon,

please find attached the CCIRC Weekly Summary of significant cyber events and incidents reported to and observed by CCIRC, with analysis where required. Please note this product is *not* intended for wide circulation due to the nature of some of the information in the Summary. Here are the highlights:

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released:** Technical Report TR11-002: Mitigation Measures for Advanced Persistent Threats published on Public Safety Canada's website

- **Incidents to report:**
  - Canadian federal official and university related credentials compromised in the UN Development Program website hack
  - Three provincial governments' computers potentially infected
  - Threat actors impersonating reputable Canadian financial institutions and a telecommunications company, enticing internet users to malicious websites (phishing)
  - A compromised Canadian website redirecting visitors to a malicious website in Russia
  - Distribution of malicious software that steals passwords traced to a Canadian source

- **International:** Foreign government officials' e-mail accounts and passwords compromised

- **Noteworthy Open Source Reports:**
  - Foreign hackers targeted Canadian institutions during Potash bid last year
  - Spoof Health Canada E-mail offers shovelling credit
  - Carrier IQ snoops on US cell users
  - Cybersecurity bill approved by U.S. House Panel

This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

Danielle St-Louis
Administrative Assistant | Adjointe administrative
Canadian Cyber Incident Response Centre | Centre de Réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Canada

CANADIAN CYBER INCIDENT RESPONSE CENTRE (CCIRC)

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-007

For the Week of

26 Nov – 2 Dec 2011

Issued: 8 Dec 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released:** Technical Report TR11-002: ~~Nothing to report.~~Mitigation Measures for Advanced Persistent Threats published on Public Safety Canada's website

- **Incidents to report:**
  - Canadian federal official and university related credentials compromised in the UN Development Program website hack
  - ~~A~~ Three provincial governments's computers potentially infected
  - Threat actors impersonating reputable Canadian financial institutions and a telecommunications company, ~~luring~~ enticing internet users to malicious websites (phishing)
  - A compromised Canadian website redirecting visitors to a malicious website in Russia
  - Distribution of malicious software that steals passwords traced to a Canadian ~~computer~~source

- **International:** Foreign government officials' e-mail accounts and passwords compromised

- **Noteworthy Open Source Reports:**
  - Foreign hackers targeted Canadian institutions during Potash bid last year
  - Spoof Health Canada E-mail offers shovelling credit
  - Carrier IQ snoops on US cell users
  - Cybersecurity bill approved by U.S. House Ppanel

Comment [DR1]: It was really traced to a Canadian IP address, but that's too technical a term for our audience. Computer may not be the technical equivalent to the IP address, but I think the overall message is correct. If you don't like "computers", please suggest other non-technical term - RD

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and noteworthy open source reports.

NOTABLE INCIDENTS– 26 NOVEMBER THROUGH 2 DECEMBER 2011:

Canadian Critical Infrastructure:

Federal Government. Some federal officials' online credentials were compromised in the UN Development Program website hack. TeaMp0ison, a famous hacktivist group ~~that is sometimes allied with the group Anonymous~~, claimed credit for this event. Only a fraction (less than 1%) of the compromised accounts were Canadian and include ~~non-federal entities~~ universities. CCIRC notified the universities as well as CTEC, who advises ~~so affected~~ federal government departments. ~~could be informed.~~

- **Analysis:** ~~The United Nationals~~UN officials stated that information was stolen from an old server during a cyber-attack on the UN Development Program in 2007. ~~UN officials~~They also stated that the stolen account and password information was now invalid. It is unknown whether this ~~is~~ statement is also true for the Canadian credentials as well as the UN ones.

Provincial Government. CCIRC received infection reports for three provincial governments' computer systems and notified the provincial contacts. CCIRC also gave mitigation advice. Impact is unknown.

- **Analysis:** These types of infections ~~seen~~ could potentially lead to a compromise of those governments' computer systems. ~~These systems are facing the Internet.~~ These infections are commonly seen by CCIRC. ~~and~~ There is no information to indicate that these ~~are compromises~~ governments were specifically targeted~~specifically targeted to these provincial governments~~.

Financial Sector. Threat actors impersonating well known financial entities attempted to steal personal information from internet users by entic~~lur~~ing them to click on links to malicious websites (phishing). CCIRC found **five** malicious websites still in operation (up from one last week) and notified the entities being impersonated.

CCIRC also notified Google phishing, and the Anti-Phishing Working Group so internet users may be alerted if they encounter these specific malicious websites. The number of victims is unknown.

- **Analysis:** This type of malicious activity is commonly seen by CCIRC and reportedly continues to cause financial losses for Canadians. It is known that the malicious websites seen during the reporting period are hosted in France and in the U.S.

Telecommunications Sector. CCIRC learned of a phishing incident where fraudsters impersonating a ~~well known~~well-known Canadian organization. They attempted to steal personal information from internet users by ~~luring~~ enticing them to click on a links to a website hosted in the U.S. - CCIRC notified the organization, the company representative at the Canadian Telecommunications Cyber Protection (CTCP) ~~group in Industry Canada~~, the Microsoft Phishing Filter Service and the Anti-Phishing Working Group.

Education:

The websites for a Canadian university and a school board were vandalized. CCIRC notified these organizations and offered mitigation advice. CCIRC also discovered that some user credentials associated with a small number of Canadian universities were compromised in the UN Development Program website hack described in the Federal government section above. CCIRC notified these universities.

- **Analysis:** While website defacement does ~~not in and of itself~~necessarily pose a threat to the organization's information security, it does indicate a vulnerability which can result in malicious acts that threaten the personal information of that website's visitors and the organization's reputation.

- Threat actors could use a website's vulnerability to commit malicious acts on-line while remaining anonymous. If this happens, the website could end up being black-listed on the internet.

General:

- **A compromised Canadian website was redirecting visitors to a malicious website hosted in Russia.** CCIRC notified the Canadian data centre hosting this website. The website has been taken down and is no longer available to internet users.

Formatted: No bullets or numbering

- **Analysis:** While this website does not belong to an entity in Canada's critical infrastructure, it is disconcerting to see Canadian websites being compromised by foreign threat actors and used for malicious purposes. These threat actors are using Canada's good cyber security reputation to perpetrate cybercrime around the world, which threatens this reputation.

- **Malicious software that steals passwords was traced to a Canadian computer.** CCIRC sent a deactivation request to the CTCP ~~(Canadian Telecommunications Cyber Protection)~~ representative for the internet service provider and informed Industry Canada.

Formatted: No bullets or numbering

CCIRC Products: CCIRC published Technical Report TR11-002: Mitigation Measures for Advanced Persistent Threats on Public Safety Canada's website. This report is intended for IT professionals and managers in all government, critical infrastructure and related sectors. It aims to raise awareness and give practical advice on mitigating the threat of targeted cyber attacks against an organization's information systems.

~~Purpose~~

~~Recent media disclosures have reported numerous high-profile computer compromises attributed to entities identified as Advanced Persistent Threat (APT). The intent of this product is to define APT, to describe typical APT attack methodologies and to introduce mitigation and monitoring techniques that may reduce the risk to organizations. While APT actors have traditionally targeted government, military and defence industrial sectors, any organization may be of interest to and be targeted by APT actors.~~

~~Nothing to report~~

International:

On-line credential compromise for a European government's officials. CCIRC learned that the e-mail addresses and passwords belonging to officials of a European government were posted on the internet. CCIRC notified that country's representative on the International Watch & Warning Network. The impact of the compromise is unknown.

Noteworthy Open Source Reports:

Foreign hackers targeted Canadian institutions during Potash bid last year. Multiple open sources reported this week that hackers linked to Chinese computers targeted certain Canadian law firms, financial institutions and public-relations agencies during BHP Billiton's takeover bid of Potash Corporation~~.~~ last year. The Saskatchewan government was ~~also~~ unsuccessfully targeted.

- **Analysis:** Experts have stated to the media that they believed ~~that the~~ hackers were seeking inside information on the takeover bid of Potash Corporation, which was ultimately blocked by the federal government. Canada is one of the world's largest potash exporters. Potash is a mineral used as a fertilizer in agriculture~~., notably in corn production. Though demand from China is growing, almost 75 per cent of Potash Corp.'s sales last quarter were made in Latin America and in Asian countries outside of China and India.~~ Start-up costs ~~to~~ for new potash mines are currently prohibitively expensive, which is why Potash Corp, a highly profitable company, was such an attractive takeover target.

Formatted: Tab stops: 11.75 cm, Left

Formatted: Tab stops: 11.75 cm, Left

s.20(1)(b)

Spoof Health Canada E-mail offers shovelling credit. A press release from a fraudulent Health Canada e-mail address announced seniors would get a fitness tax credit from the Government for shovelling snow if they submitted a photo of themselves during the act. According to CBC, a~~A~~ communications consultant in Winnipeg~~, reached by the CBC~~, admitted to being behind the spoof to make a political statement.

- ~~**Analysis:** This prank was done to make a political statement and does not appear to have done any harm. However, when Canada's anti-spam legislation comes into force, such an act could become illegal.~~

Carrier IQ snoops on U.S. cell users. ~~*I'll do the write up Thursday morning (RD)*~~
. A U.S. researcher published information about a mobile phone monitoring software that is being included on certain cellular phones in the U.S. This news received much press attention in US and Canada, where privacy concerns were raised. Carrier IQ, the software manufacturer, explained that the purpose of the software was to allow mobile phone service providers to monitor and troubleshoot wireless network issues.

- **Analysis:** [redacted] install this monitoring software. -Based on all information received, CCIRC does not believe there is a high impact in Canada.

- –It should be noted that electronic surveillance issues are of keen public and media interest in both U.S. and Canada. ~~The Federal Privacy Commissioner of Canada has expressed a number of times her opposition to proposals where Canadian law enforcement would have access to even basic mobile phone subscriber information from telecommunications service providers.~~ Public Safety Canada collaborates with the Office of the Privacy Commissioner on -electronic privacy issues related to public safety.

Cybersecurity bill approved by U.S. House panel. The U.S. cyber security bill, which will allow greater threat information sharing between the U.S. intelligence agencies and the private sector, was approved by a U.S. House of Representative Intelligence Panel. The bill was amended by the panel to include privacy protections for data that the private sector gives to the government, such as ~~, including, potentially,~~ customer information given by Internet service providers. The next step is a hearing on December 13, 2011, by the House of Representatives Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies ~~I'll do the write up Thursday morning.~~

- **Analysis:** Cyber security is a high priority for the U.S. government. ~~Given~~It is likely that publicized ~~the data breaches and~~ cyber-attacks against U.S. organizations have contributed to the ~~made public, there is~~ general support in both the House of Representatives and the Senate for a cyber-security bill.

Formatted: Font: Bold
Formatted: Indent: Left: 0.63 cm, Hanging: 0.43 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: Bold
Formatted: Indent: Left: 1.27 cm
Formatted: Indent: Left: 0.63 cm, Hanging: 0.43 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: Bold
Formatted: Font: Not Bold, Not Italic
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Font: Not Italic, Not Highlight
Formatted: Indent: Left: 0.63 cm, Hanging: 0.41 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm
Formatted: Font: Bold
Formatted: Indent: Left: 1.27 cm

- -There is no question there will be a new U.S. cyber security bill in the near future – the only question is the extent of government regulation in this area. While the U.S. Senate favours more sweeping cyber security regulations, the House of Representative seems to favour cyber security incentives for private firms to boost their own security and share information, including legal protections. The House version of the bill has industry support.

~~Note: This doesn't mean the bill is approved – it is going to be heard on Tuesday (Dec 6?) by the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies – most interesting feature of the bill is the creation of the not-for-profit National Iformation Sharing Organization that would share cyber threat information among various govt & privae sector constituencies, and have reps from federal, state, local govts, CI sector businesses, privacy and civil liberties communities (RD)~~

FEEDBACK: This is a newly developed product. Your feedback is appreciated and critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Formatted: Indent: Left: 0.63 cm, Hanging: 0.41 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Indent: Left: 0 cm

Public Safety Canada | Sécurité publique Canada

Canada

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-002

24 - 28 Oct 2011

Issued: 4 Nov 2011

HIGHLIGHTS OF THE WEEK:

- **Threat Warnings:**
  - Hacker group Anonymous urged sympathizers to participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5. As of the time of this writing, ITAC believes the risk to be low.
- **Reported Incidents:**
  - Potential attack on a federal department
  - Intrusion attempts into a Canadian Internet Service Provider's core infrastructure
  - On-line recruitment for money laundering targeting Canadians
  - Canadian police personnel computer user information posted on a hacker website
  - Compromised computers in networks of provincial governments, energy companies, universities and a hospital.
  - Individuals tried to lure computer users to malicious web sites by pretending to be reputable Canadian companies in the financial and transport sector.
- **Noteworthy International News:** Japanese missions around the world experiencing targeted cyber attacks; Finland wants cyber war weapons; Chinese military suspected of hacking US satellites.

Comment [P1]: Does this date need a reference? For Week Of. Or something like that.

Comment [P2]: The position of the HIGHLIGHTS to me is not visually pleasing. Just sits right in the middle of the page. Maybe loose the box?

UNCLASSIFIED
DRAFT

- Threat Warnings
- Reported Incidents
- Noteworthy International News

Formatted: Bullets and Numbering

Comment [P3]: What does this mean?

Comment [P4]: Not sure ITAC comment relevant

Comment [P5]: If this is related to the Gaddafi comment, I do not feel that is a "potential attack." Should be "Phishing attempt against federal department"

Comment [P6]: What does this mean?

Comment [P7]: personal

Comment [P8]: Should be "Belonging to"

Comment [P9]: Individuals? Sounds weird. This should say "Identification of malicious websites pretending to be…"

Comment [P10]: Very dramatic. Should read "Finland attempting to build offensive cyber capibilities"

UNCLASSIFIED
DRAFT

PURPOSE

The purpose of this Weekly Summary is to [redacted] government and critical infrastructure management [redacted] notable cyber events [redacted] the Canadian Cyber Incident Response Centre (CCIRC [redacted])

NOTABLE INCIDENTS– 24 THROUGH 28 OCTOBER 2011:

Canadian Critical Infrastructure:

Federal Government. CCIRC received a report [redacted] with [redacted] subject line referencing Gaddafi and Allah. [redacted] Cyber Threat Evaluation Centre (CTEC [redacted])

Analysis: [redacted] CCIRC suspects this phishing e-mail attack was an attempt to compromise computers in that federal department.

Provincial Government. CCIRC received reports on potential compromises of computers on three provincial government systems.

Analysis. CCIRC has no information to indicate that these were targeted attacks on the provinces. Reports indicated that the computers in question were infected with malicious software commonly used by cyber criminals.

Police. CCIRC discovered that user account information for a number of Canadian police organizations was posted on a hacker website. CCIRC sent information to the RCMP for evaluation and notification of the affected police agencies.

Analysis: CCIRC has no information whether police computer networks were compromised as a result of this activity. A similar incident for a Canadian provincial police force and a number of American police organizations occurred earlier in 2011.

Financial Sector.

Phishing. CCIRC received nine phishing reports and actioned the one that continued to pose a threat. In this incident, a threat actor, impersonating a well-known Canadian bank, was luring computer users via e-mail, to a website hosted in Australia. CCIRC notified the bank, Google

Comment [P11]: This needs more context, and his full name as this guy was a state leader.

Comment [P12]: Can we even make this statement? Should this not be a CTEC role. Do we suspect that? Or was this just a general phishing attack using that lure?

phishing, the Anti-Phishing Working Group and Microsoft, so internet users may be alerted if they encounter these websites.

Threats by Anonymous. Anonymous, the famed hacker group, urged sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on November 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on November 5. As of the date of this writing, CCIRC learned the operation to hack the TMX computers on November 7 has been cancelled.

Analysis: Anonymous, a loosely organized hacker group, does have the capacity to organize and launch a Distributed Denial of Service (DDOS) attack that could potentially bring down a website.

When Anonymous called for a November 7 attack on the TMX computers, CCIRC contacted major Canadian financial institutions. They confirmed their awareness of the potential threat from Anonymous, and that their internet service providers were standing by for a DDOS attack. As of the date of this writing, the cyber attack on TMX has been called off.

Money laundering attempt. CCIRC learned of an on-line recruitment campaign in Canada for money laundering, originating from abroad. CCIRC sent summary and technical details sent to the RCMP Anti-fraud centre as well as the RCMP High-Tech Crime Branch for possible further investigation.

Telecommunications Sector.

Phishing Reports. A report was received on a threat actor who spoofed a well-known Canadian telecommunication company, and prompted internet users to provide their subscriber credentials via e-mail. CCIRC notified the company on this matter.

Analysis: Phishing incidents such as the ones reported above are more common in the financial sector, but do occur in the telecommunications sector as well. Free telecommunications services are the likely goal of this threat actor.

Intrusion attempt – Internet Service Provider Core Infrastructure: A Canadian internet service provider informed CCIRC and other Canadian telecommunication companies about recent brute force hacking attempts against their routers, at the rate of 60-100 attempts each day. The reporting internet service provider has taken mitigation measures.

Analysis: Routers of an internet service provider are used to route internet traffic of its subscribers, and possibly other internet users. Having control of a router on the Canadian telecommunication network would enable a hacker to intercept Canadians' communications and information going through that router, and use that information for a variety of purposes.

Comment [RD13]: How about I remove the highlighted item? This is more useful to educate the public -

Energy Sector. CCIRC received infection reports on computers of three energy sector organizations. These organizations are: A large of oil & gas producer, a service & equipment provider to the oil and gas sector, and a provincial electricity producer. CCIRC notified all three organizations of the potential infections.

Health. CCIRC received a computer infection report for a Canadian hospital and notified the organization's IT department.

Transportation. CCIRC received a report of phishing attempts in the aviation sector. Threat actors were seeking on-line customer credentials for an airline.

International News

Japanese missions around the world experiencing targeted cyber attacks. Open sources report that at least dozens of computers used at Japanese missions in nine countries, including Canada, have been compromised since this past summer. Many of the compromises were found to allow a remote hacker to gain access and steal confidential information. The Japanese Foreign Ministry is investigating this incident and assessing its impact.

Finland wants cyber war weapons. Open sources report Finland has joined Sweden in planning to include counter-offensive capability for cyber attacks as part of its defence strategy. The new strategy would be presented to parliament and formalized in 2013.

Chinese military suspected of hacking US satellites. According to a publicized portion of the draft US-China Economic and Security Review Commission annual report, computer hackers, possibly from the Chinese military, interfered with two US government satellites four times in 2007 and 2008. There is currently no public information about the nature of the hackers' interference with these satellites, which are used for earth climate and terrain observations. The report, which is to be released next month, states the interferences occurred through a ground station in Norway.

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in 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.

NOTES

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

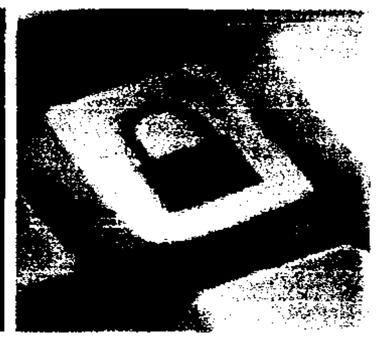
- **Flash**: Perceived threat and/or vulnerability; No patch available
- **Advisory**: Threat present affecting Canadian national infrastructure; Patches available
  (Advisories and Flashe marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Public Safety Canada | Sécurité publique Canada

TLP: AMBER

Canada

OPERATIONAL SUMMARY
CCIRC Cyber Awareness Product



Weekly Technical Report

Issued: 7-Dec-2011

DISCLAIMER

This publication is **UNCLASSIFIED - For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in 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.

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

s.20(1)(b)

Table of Contents

Incident reporting 0
1. CE11-2486 Website Defacement 0
2. CE11-2488 School Board Website Defacement 0
3. CE11-2490 UN Development Program Website Hacked by TeaMp0isoN 0
4. CE11-2493 Foreign Government Email accounts/PW posted on pastebin 0
5. CE11-2494 [redacted] Drone Notifications - Multiple Organizations 0
6. CE11-2495 Malware hosted on a Canadian ISP IP 0
7. CE11-2496 Compromised Canadian website redirecting to exploit site 1
8. CE11-2497 CRA Phishing Sites 1
9. CE11-2498 SQL Injection Canadian Websites 1
10. CE11-2499 [redacted] Drone Notifications - Multiple Organizations 1
11. CE11-2501 Notification to [redacted] - SpyEye Tracker 1
Banking 1
2. CE11-2487, CE11-2492, CE11-2491, Bank Phishing Sites 1
Federal Government 2
Provincial Government 2
Electrical and Energy 2
1. CE11-2500 Energy Company Actively Scanned 2
Partners 2
Watch List 2
Malware Indicators 3
1. Zero-Access Exploit Kit, Tracur and FakeAV 3
2. Black Hole and "redret" Domains 3
3. ZeuS and Black Hole on billycharge[.]com 4
CCIRC Cyber Awareness Products 5
Advisories 5
Information Notes 5
Technical Reports 5
Cyber Flashes 5
Threat and Vulnerability Monitoring 5
Vulnerabilities: 5
1. Skype Discloses IP Addresses to Remote Users 5
2. McAfee SaaS Scan Method Script Injection Code Execution Vulnerability 5
3. HP LaserJet Printers Remote Firmware update flaw 5
4. HP LaserJet Printers Remote Firmware update flaw 6
5. IBM Lotus Domino Controller Auth. Bypass 6
Threat Watch: 6
1. Cutwail Botnet Expands via Facebook 6
2. SQL Injection Attack 6
Malware and SPAM Reports 6
Publicly Reported Compromises 7
SCADA/ICS 7
1. ICS-ALERT-11-332-01 - Siemens Automation License Manager 7
2. ICS-ALERT-11-332-02 - Siemens SIMATIC WinCC Flexible 7
3. ICS-ALERT-11-332-03 - Optima APIFTP Server 7
4. ICS-ALERT-11-333-01 - Microsys Promotic Vulnerability 7

5. ICSA-11-243-03A - GE Proficy Historian Data Archiver 7
6. ICSA-11-243-03A - GE Proficy Historian Data Archiver 7
7. ICS-ALERT-11-332-01A—SIEMENS AUTOMATION LICENSE MANAGER MULTIPLE VULNERABILITIES 7
8. ICS-ALERT-11-332-02A—SIEMENS SIMATIC WINCC FLEXIBLE VULNERABILITIES 7
9. ICS-ALERT-11-336-01—3S CODESYS WEBSERVER BUFFER OVERFLOW 7
Noteworthy News 7
1. Adobe fixes flaw in Flex SDK framework 8
2. Data breaches up 32 percent 8
3. Spoof Health Canada Email Offers Shovelling Credit 8
4. Targeted attacks steal credit cards from hospitality and educational institutions 8
5. Carrier IQ : Mobile carriers to blame for use of secret logging software? 9
6. Tool to detect Carrier IQ 9
7. Cutwail Spam Campaigns Lure Users to Blackhole Exploit Kit 9
8. First National Bank of Long Island, Operation Robin Hood Victim 10
9. New zero-day Yahoo Messenger exploit allows malware to spread via hijacked status updates 10
10. Google Expands Safe Browsing Alerts to Include Malware Distribution Sites 10
11. Google researchers propose fix for ailing SSL system 11
12. Cyber security bill promotes sharing of threat data 11
13. Obama Invokes Cold-War Security Powers to Unmask Chinese Telecom Spyware 12
14. Hackers say they broke BlackBerry PlayBook security 12
15. Measuring Cyber Security 12
16. Foreign hackers targeted Canadian firms 12
17. United Nations agency 'hacking attack' investigated 13
18. HP printers may be remotely set on fire, researchers say 13
19. GameOver ZeuS variants spread via NACHA spam launches DDOS against Financial Institutions 14

Incident reporting

This section contains information related to incidents affecting Critical Infrastructure in Canada.

1. CE11-2486 Website Defacement

CCIRC observed that a website registered by a University was recently defaced. Notification sent to the domain technical contact for the university and their hosting provider.
CCIRC recommendations:
* Check web sever logs for any indication of unusual activity against your website or supporting databases.
* Change administrator and FTP passwords for the server/website.
* Check for any new user accounts with admin privileges that may have been recently created.

2. CE11-2488 School Board Website Defacement

Open source review found a defacement report of a school board in Quebec. Notification was sent to the organisation.

3. CE11-2490 UN Development Program Website Hacked by TeaMp0isoN

CCIRC reviewed reports describing UN Development Program Website Hacked by TeaMp0isoN. Usernames and passwords were posted on pastebin [redacted]. CCIRC notified Canadian organizations potentially affected.

4. CE11-2493 Foreign Government Email accounts/PW posted on pastebin

CCIRC observed that Foreign government email account and password information was posted on Pastebin [redacted] Notification sent to the Foreign Government's Ministry of Interior - Police Service, for their evaluation and mitigation.

5. CE11-2494 [redacted] Drone Notifications - Multiple Organizations

[redacted] Drone Report for Canadian hosts: notifications to multiple organizations. Hosts within these organizations were communicating with a [redacted] sinkhole server or associated data source. Infection types included DNS Changer and Torpig.

6. CE11-2495 Malware hosted on a Canadian ISP IP

CCIRC observed several reports of malware being severed from a Canadian ISP host. [redacted]

The VT report indicates the malware is a password stealer. Deactivation request sent to the ISP technical contact.

[redacted]

7. CE11-2496 Compromised Canadian website redirecting to exploit site

CCIRC observed that the [redacted] website contained a redirect to a malicious domain, which attempts to launch exploits against client browsers. (Exploit.HTML.IESlice.i)

[redacted]

Notification was sent to the domain technical contact and their hosting provider. The account has been suspended until site is cleaned.

8. CE11-2497 CRA Phishing Sites

- [redacted]
-

[redacted]

CCIRC sent a notification to [redacted] recommending deactivation. CCIRC also reported this domain to [redacted]

9. CE11-2498 SQL Injection Canadian Websites

Discovered evidence that the [redacted] may have been the victim of a SQL injection attack. It appears to be redirecting visitors to a 'known bad' domain associated with recent SQL injection activity (source dshield.org). (related to threat entry on SQL injection campaign below)

10. CE11-2499 [redacted] Drone Notifications - Multiple Organizations

[redacted] notifications sent to multiple organizations. Hosts within these organizations were communicating with a [redacted] sinkhole server and other data sources. Infection types included DNS Changer, Mebroot, Torpig, and Zeus. Multiples CI sector organisations and academia were notified.

11. CE11-2501 Notification to [redacted]

CCIRC received a report from a trusted partner regarding the site [redacted] with IP address of [redacted] hosted in Canada, and appearing on the SpyEye Tracker web sites. CCIRC contacted ISP for takedown of the associated files.

Banking

2. CE11-2487, CE11-2492, CE11-2491, Bank Phishing Sites

- hxxp://www[.]jemaenterprise[.]com/wp-includes/wp-includes[.]php
216[.]97.237.203 (Lunar Pages - Anaheim California)
- hxxp://translationtrudy[.]com/api/user/businessbanking[.]tdcommercialbanking[.]com/WBB/
62[.]193.199.232 (AMEN Networks, Paris France)
- hxxp://elrepworld[.]com/assets/doc

205[.]186.131.57 (Media Temple, Culver City Califlornia) s.13(1)(a) s.16(2)(c)

Reported to banks phishing intake and APWG.

Federal Government

NIL

Provincial Government

NIL

Electrical and Energy

1. CE11-2500 Energy Company Actively Scanned

The following IP address [redacted] was reported as scanning the network for a number of days.
The ports that have been scanned are :
[redacted]
CCIRC has contacted the IP operator and engaged with different partners to monitor this activity.
[redacted]
The IP operator stated this was a benign internet survey scan.

Partners

Watch List

Watch List associated with malicious activity in the last period. This is not a block list and CCIRC recommends using the list as indicators only over the last 7 days prior to November 23.

///start of list///

IP	CIDR	Country
[redacted]		

01831

///end of list///

s.16(1)(b)
s.16(2)(c)

Malware Indicators

1. Zero-Access Exploit Kit, Tracur and FakeAV

A member submitted information for their analysis of various redirect to Exploit kits, specifically to one believed to be Zero-Access Exploit Kit. These kits often targets JAVA based vulnerabilities. Specfically, recent exploits of CVE-2011-3544 (Java Rhino Script Engine) were found. CCIRC published AV11-046 to raise awareness of this vulnerability. CCIRC recommends that organizations that have not yet deployed this patch do so at the earliest opportunity.

[redacted]

2. Black Hole and "redret" Domains

An excellent write up by SANS identified the domain name pattern "redret" as largely associated with Blackhole exploit kit sites. Some examples provided include:

[redacted]

[redacted]

s.16(1)(b)

s.16(2)(c)

Reference:
http://isc.sans.edu/diary.html?n&storyid=12145

3. ZeuS and Black Hole on [redacted]

A number of recent reports raised awareness of redirecting sites and spam emails to [redacted] website. Although the site is legitimate, it appears to have been compromised and serving malware. Associated IPs and URL with references are provided below:

[redacted]

CCIRC Cyber Awareness Products

Advisories

NTR

Information Notes

NTR

Technical Reports

- TR11-002: Mitigation Guidelines for Advanced Persistent Threats

Cyber Flashes

- CF11-025: Summary of Recent Spear Phishing Campaigns and Potential APT indicator

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. Skype Discloses IP Addresses to Remote Users

Remote users can initiate a call to a user by their Skype handle and determine the associated IP address and personal information without "incoming call" display at the users end. NO CVE.

- Reference: http://securitytracker.com/id/1026370

2. McAfee SaaS Scan Method Script Injection Code Execution Vulnerability

The flaw in the library myCIOScn.dll can be exploited if the user visits a malicious page and allows script injection that is run at the end of the AV scan. The code is then run with the same permissions as the AV. A vendor patch is available. NO CVE.

- Reference: http://www.securiteam.com/windowsntfocus/6Q02X0K3FC.html

3. HP LaserJet Printers Remote Firmware update flaw

By sending a crafted remote firmware update request to TCP port 9100, it is possible to upload malicious firmware. A workaround is available. NO CVE.

- Reference: http://secunia.com/advisories/47063/

4. HP LaserJet Printers Remote Firmware update flaw

By sending a crafted print job can allow the firmware to be updated with arbitrary code. It can be used to trip the thermal switch and shutdown the printer. If there is a switch malfunction there is a potential risk of a fire hazard. No solution at this time. NO CVE.

- Reference: http://securitytracker.com/id/1026357

5. IBM Lotus Domino Controller Auth. Bypass

By injecting a crafted XML user can gain access to the host system and execute with system privileges. No patch available. CVE-2011-1519

- Reference: http://www.securityfocus.com/bid/46985

Threat Watch:

1. Cutwail Botnet Expands via Facebook

The spam campaign is looking for new types of hosts to infect via Facebook spam via spoofed emails or notifications. The spam only includes a link to a site which verifies the platform and delivers the appropriate malware.

- Reference: http://news.softpedia.com/news/Cutwail-Botnet-Expands-Via-Facebook-Notification-Spam-238075.shtml

2. SQL Injection Attack

Another mass SQL injection campaign is under way. Sites affected are injected with redirection script to hXXp://lilupophilupop.com/sl.php

- Reference: http://isc.sans.edu/diary.html?storyid=12127

[redacted]

s.16(1)(b)

s.16(2)(c)

Malware and SPAM Reports

NIL

01835

Publicly Reported Compromises

NIL

SCADA/ICS

ICS-CERT Information Bulletin

1. ICS-ALERT-11-332-01 - Siemens Automation License Manager

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-332-01.pdf

2. ICS-ALERT-11-332-02 - Siemens SIMATIC WinCC Flexible

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-332-02.pdf

3. ICS-ALERT-11-332-03 - Optima APIFTP Server

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-332-03.pdf

4. ICS-ALERT-11-333-01 - Microsys Promotic Vulnerability

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-333-01.pdf

5. ICSA-11-243-03A - GE Proficy Historian Data Archiver

http://www.us-cert.gov/control_systems/pdf/ICSA-11-243-03A.pdf

6. ICSA-11-243-03A - GE Proficy Historian Data Archiver

http://www.us-cert.gov/control_systems/pdf/ICSA-11-243-03A.pdf

7. ICS-ALERT-11-332-01A—SIEMENS AUTOMATION LICENSE MANAGER MULTIPLE VULNERABILITIES

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-332-01A.pdf

8. ICS-ALERT-11-332-02A—SIEMENS SIMATIC WINCC FLEXIBLE VULNERABILITIES

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-332-02A.pdf

9. ICS-ALERT-11-336-01—3S CODESYS WEBSERVER BUFFER OVERFLOW

http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-336-01.pdf

Noteworthy News

1. Adobe fixes flaw in Flex SDK framework

"Adobe patched a security flaw in its Flex SDK product that could lead to cross-site scripting attacks against some applications that were built using the SDK, threatpost reported December 1. The vulnerability affects versions 3.6 and below, and 4.5.1 and below. The Flex SDK is a free, open source application framework that Adobe produces to enable developers to write apps across a variety of devices and platforms. Flex can be used with other tools to build apps for iOS, Android, BlackBerry, and the Web. The newly patched vulnerability affects the Flex SDK for Windows, Macintosh, and Linux."
Reference: http://threatpost.com/en_us/blogs/adobe-fixes-flaw-flex-sdk-framework-120111

2. Data breaches up 32 percent

"The frequency of data breaches in healthcare organizations has increased by 32 percent, with hospitals and healthcare providers averaging four data breaches, according to the Ponemon Institute. Employee negligence is the primary culprit. According to 41 percent of healthcare organizations surveyed, data breaches involving protected health information (PHI) are caused by sloppy employee mistakes. To compound the problem, half of respondents do nothing to protect mobile devices that are in use in 80 percent of healthcare organizations."
Reference: http://www.net-security.org/secworld.php?id=12031

3. Spoof Health Canada Email Offers Shovelling Credit

Some journalists were left scratching their heads Monday after a fake government press release promising snow shovelling tax credits for seniors hit their inboxes. The spoof release was quickly revealed as a fake by a phone call to the office of Health Minister Leona Aglukkaq. The phony emailed news release said the government would provide fitness tax credits for seniors shovelling snow if they submitted photos as evidence. The email appeared to come from Health Canada's media relations email address, but instead came from a variation on the address.
Reference: http://www.huffingtonpost.ca/2011/11/28/snow-shovelling-health-canada-tax-credit_n_1117022.html

4. Targeted attacks steal credit cards from hospitality and educational institutions

"A little more than a week ago SophosLabs became aware of a resurgence of an attack against the education and hospitality industries. In at least one case the malware has shown up at a financial services company. One thing important to note is that it has only been seen at moderate to small size organizations. These criminals aren't targeting Walmart. They are after organizations with less investment in defensive counter-measures. The goal of this Trojan is to target credit card processing and point of sale (PoS) equipment and make off with all of the card details. It installs itself as a service in Windows and the filename is typically rdasrv.exe, while the service is called rdasrv. More recent samples have changed their name to be A#######.exe, where the # is a random number."
Reference: http://nakedsecurity.sophos.com/2011/11/30/targeted-attacks-steal-credit-cards-from-hospitality-and-educational-institutions/

5. Carrier IQ : Mobile carriers to blame for use of secret logging software?

"The recent revelation that most Android, BlackBerry and Nokia phones are installed with the Carrier IQ software that logs practically all actions made by the mobile phone users and reports/sends it to remote servers has, understandably, created quite a stir. While Nokia was quick to claim that no phone of theirs has ever been shipped with Carrier IQ onboard and the blame for the presence of the software on the devices was pretty fast passed onto the carriers, mobile telephone companies around the world were quick to deny any involvement with the scheme. According to The Register, Australian Telstra, Optus and Vodafone have denied using the software, and were followed by New Zealand's Telecom, Vodafone and Telstra Clear. Thom Holwerda says that smartphones in The Netherlands also seem not to carry the software and speculates that its use might be limited to the US - even though Verizon has also piped up to say that their devices do not include Carrier IQ. Additional investigation by an iPhone developer that goes by the name of "Chpwn" revealed that even users of iOS-run devices are not safe from the spying software. He says that since iOS 3 and up through and including iOS 5, Apple has included a copy of Carrier IQ on the iPhone. He also says that this version of the software does not have access to the same amount of information as those found on other devices. "I am reasonably sure it has no access to typed text, web history, passwords, browsing history, or text messages, and as such is not sending any of this data remotely," he writes."
Reference: http://www.net-security.org/secworld.php?id=12034

Other References:

http://www.theregister.co.uk/2011/12/01/apple_sprint_carrier_iq/
http://www.theregister.co.uk/2011/12/01/al_franken_carrier_iq/
http://www.computerworld.com/s/article/9222319/AT_T_Sprint_confirm_use_of_Carrier_IQ_software_on_handsets?taxonomyId=17
http://nakedsecurity.sophos.com/2011/12/01/carrier-iq-snoops-on-us-cell-users-spyware-or-service-monitoring-tool/

6. Tool to detect Carrier IQ

"Bitdefender announced the availability of a new tool that identifies the presence of the controversial mobile network diagnostic tool from Carrier IQ. Dubbed Carrier IQ Finder, the tool instantly determines if the user's Android device has been equipped with the Carrier IQ tracking package, and if the device is being monitored."
Reference: http://www.net-security.org/secworld.php?id=12045

7. Cutwail Spam Campaigns Lure Users to Blackhole Exploit Kit

"Over the past few days the Cyrwail botnet has been sending out malicious spam campaigns with a variety of themes such as airline ticket orders, Automated Clearing House (ACH), Facebook notification, and scanned document. These campaigns do not have malware attachments, instead the payload is delivered via links to malicious code hosted on the web.
Reference: http://labs.m86security.com/2011/12/cutwail-spam-campaigns-lure-users-to-blackhole-exploit-kit/

8. First National Bank of Long Island, Operation Robin Hood Victim

"In order to prove me wrong and to show theyre still able to pull off a hacking operation, the hacktivists behind Operation Robin Hood revealed the vulnerabilities present in the website of the First National Bank of Long Island. I wanna say, that, we TeaMp0isoN pulled off any project we started, sooner or later of course. As i am not defacer or fame hunting kid/skid, Ill just prove that banks are secure and can(WILL) be hacked, wrote the hackers in response to my article. By making use of an SQL injection flaw, members of the newly formed alliance, p0isAnon, injected a piece of arbitrary code into the website. To prove the attack concept, they posted a link that clearly shows the vulnerability really exists."
Reference: http://news.softpedia.com/news/First-National-Bank-of-Long-Island-Operation-Robin-Hood-Victim-237131.shtml?utm_source=twitter?utm_source=twitter&utm_medium=twitter&utm_campaign=twitter_web

Other related references:
http://www.net-security.org/secworld.php?id=12024
http://www.itworld.com/security/229141/team-poison-anonymous-campaigners-claim-first-victims-oprobinhood
http://www.theregister.co.uk/2011/11/30/anon_oprobinhood/

9. New zero-day Yahoo Messenger exploit allows malware to spread via hijacked status updates

"An unpatched zero-day flaw in Yahoo Messenger allows remote attackers to fiddle with any user's status message - allowing malware to be spread, Bitdefender security researchers revealed on Friday. Vulnerable clients are found in version 11.x of Messenger, including the freshly released 11.5.0.152-us version. The reason the status update vector is so dangerous boils down to trust, the researchers said. Because status updates only go out to a user's small group of friends, those friends are likely to click through, and that's when the nastiness begins."
Reference: http://nakedsecurity.sophos.com/2011/12/03/new-zero-day-yahoo-messenger-exploit-hijacks-users-status-update/

10. Google Expands Safe Browsing Alerts to Include Malware Distribution Sites

"Google is expanding the amount and kind of data that it supplies to network operators about potentially malicious activity happening on their networks and elsewhere. The company is now giving operators information on dedicated domains that are being used for malware hosting and distribution. Last fall, Google began a program through which operators of autonomous systems (AS) could sign up to receive information about any malicious content that Google's scanners found on sites they owned or operated. The Google Safe Browsing Alerts are meant to give operators an early heads-up when a site on their network has been compromised and is being used either as an attack site or as another piece of an attack chain. Legitimate sites often are compromised by attacker through tactics such as SQL injection, and then used as platforms for hosting malware or malicious links redirecting users to other attack sites. Operators of large networks may not know about a

compromise of one of their sites for quite a while, and Google's alerts are meant to fill in that gap. Up until now, Google had been simply alerting administrators about compromised sites on their networks. Now, that program is expanding to include malware distribution sites that could be hidden on a large network. A malware distribution site is different from a compromised legitimate site in that it is set up by an attacker for the specific purpose of hosting and distributing malware. Attackers will often use hosting providers that look the other way for such operations, but if they can somehow latch onto an existing legitimate domain, that's all the better for them. Having their distribution site on a known legitimate domain can lend a bit of legitimacy to the site and up their chances of finding more victims. Google also has services fo network operators that will send them automated messages when the company's scanners find a potential phishing page on their network or will send a code sample when malicious content is found.
Reference: http://threatpost.com/en_us/blogs/google-expands-safe-browsing-alerts-include-malware-distribution-sites-120211

11. Google researchers propose fix for ailing SSL system

"Security researchers from Google proposed an overhaul to improve the security of the Secure Sockets Layer encryption protocol that millions of Web sites use to protect communications against eavesdropping and counterfeiting. The changes are designed to fix a structural flaw that allows any one of the more than 600 bodies authorized to issue valid digital certificates to generate a Web site credential without the permission of the underlying domain name holder. The consequences of fraudulently issued certificates was underscored in late August when hackers pierced the defenses of Netherlands-based DigiNotar and minted bogus certificates for Google and other high-profile Web sites. One of the fraudulent credentials, for Google mail, was used to snoop on as many as 300,000 users, most of them from Iran. Under changes proposed November 29 by Google security researchers, all certificate authorities would be required to publish the cryptographic details of every Web site certificate to a publicly accessible log that has been cryptographically signed to guarantee its accuracy. The overhaul, they said, is designed to make it impossible -- or at least much more difficult — for certificates to be issued without the knowledge of the domain name holder."
Reference: http://www.theregister.co.uk/2011/11/29/google_proposes_ssl_fix/

12. Cyber security bill promotes sharing of threat data

"The House Intelligence Committee introduced legislation Wednesday designed to knock down the barriers that interfere with the federal government and the private sector sharing critical information about cyber security threats. The bill would enable the intelligence community to share classified information with the private sector while at the same time addressing the concerns private companies have with providing information about attacks on their systems to the government. Communications between the two sides has been problematic and difficult. The government has limited the amount of information it provides private industry about cyber attacks for fear of compromising secrets."
Reference: http://security.blogs.cnn.com/2011/11/30/cyber-security-bill-promotes-sharing-of-threat-data/

13. Obama Invokes Cold-War Security Powers to Unmask Chinese Telecom Spyware

"The U.S. is invoking Cold War-era national-security powers to force telecommunication companies including AT&T Inc. and Verizon Communications Inc. (VZ) to divulge confidential information about their networks in a hunt for Chinese cyber-spying. In a survey distributed in April, the U.S. Commerce Department asked for a detailed accounting of foreign-made hardware and software on the companies networks. It also asked about security-related incidents such as the discovery of unauthorized electronic hardware or suspicious equipment that can duplicate or redirect data, according to a copy of the survey reviewed by Bloomberg News. The survey represents very high-level concern that China and other countries may be using their growing export sectors to develop built-in spying capabilities in U.S. networks, said a senior U.S. intelligence official who asked not to be named because he wasnt authorized to speak on the matter."
Reference: http://www.bloomberg.com/news/2011-11-30/obama-invokes-cold-war-security-powers-to-unmask-chinese-telecom-spyware.html?utm_source=dlvr.it&utm_medium=twitter

14. Hackers say they broke BlackBerry PlayBook security

"Three hackers say they have broken the security on the BlackBerry PlayBook tablet, allowing them to run unauthorized applications and control hardware components that users can't normally access. "We've done it. We've broken RIM's fancy security," said a hacker who goes by the alias "neuralic" in a demonstration video posted on Youtube. He said he collaborated on the project with two other hackers, known as Xpvqs and Chris "cmw" Wade. In a statement, Playbook-maker Research in Motion said it was aware of "a claim made on Twitter" by security researchers "that suggests the ability to 'jailbreak' a BlackBerry PlayBook tablet." Jailbreaking a device means altering it to gain access to systems or applications that aren't authorized by the manufacturer. RIM added that it is investigating the claim and has been in contact with one of the security researchers to discuss it."
Reference: http://www.cbc.ca/news/technology/story/2011/11/30/technology-blackberry-playbook-security.html
Related:
http://www.infomedia.gc.ca/ps-sp/articles/unrestricted/2011/12/ps-20111230103733 83_1.htm

15. Measuring Cyber Security

Mitre has been leading efforts to measure cyber security issues for many years, starting with pioneering the CVE and associated CVSS framework. Other related standards are captured under this website, touching on event management, incident management, vulnerability management, Malware, Attacks, etc.
Reference: http://cybox.mitre.org/

16. Foreign hackers targeted Canadian firms

"A leading cyber-crime expert says foreign hackers who launched a massive attack on Canadian government computers last fall also broke into the data systems of prominent Bay Street law firms and other companies to get insider information on an attempted $38-billion corporate takeover. Daniel Tobok, whose international cyber-sleuthing company was called in by a number of the firms hit by the attacks, says the hacking spree from computers in China were all connected to last year's

ultimately unsuccessful takeover bid for Potash Corporation of Saskatchewan. "All those different attacks on companies, law firms and government were all interconnected — they weren't isolated incidents," he said in an interview with CBC News. Tobok said hackers penetrated the computer systems of at least seven of Canada's leading law firms in what experts believe was an attempt to mask the real target of the attacks — the few firms directly involved in the aborted Potash deal. The foreign hack-attack on Canadian law firms was "very sophisticated and highly targeted," he said. The hackers appeared to have been hunting exclusively for information on the Potash deal, and there was no evidence they had penetrated the confidential files of other clients of the firms affected."
Reference: http://www.cbc.ca/news/canada/story/2011/11/29/pol-weston-hacking-firms.html

17. United Nations agency 'hacking attack' investigated

A group of hackers posted more than 100 e-mail addresses and log-in details it claimed to have extracted from the United Nations. Many of the e-mails involved appear to belong to members of the United Nations Development Programme (UNDP). The group, which identifies itself as Teampoison, attacked the UN's behavior and calledit a "fraud". A spokeswoman for the UNDP said the agency believed "an old server which contains old data" had been targeted. "UNDP is taking action to close any vulnerabilities on our Web site," she said. "Please note that UNDP.org was not compromised." The details were posted on the Web site Pastebin under the Teampoison logo. Many of the e-mail addresses gend in undp.org, but others appear to belong to members of the Organization for Economic Cooperation and Development, the World Health Organization, and the United Kingdom's Office for National Statistics. The poster noted that several of the accounts had "no passwords".
Reference: http://www.bbc.co.uk/news/technology-15951883

18. HP printers may be remotely set on fire, researchers say

"Researchers at Columbia University in New York City found a HP LaserJet printer vulnerability that could allow a hacker to remotely control the device to launch cyberattacks, steal data that is being printed, and even instruct its mechanical components to overload until it catches fire. According to MSNBC, the researchers revealed the flaw they found does not affect only HP printers, but also other devices utilized by millions of individuals and companies that so far were considered to be safe. In the case of the HP printers which they thoroughly tested, the researchers relied on the fact remote software updates are not checked for signatures or certificates when they are being installed. In another demonstration, by sending a specially crafted print job, they were able to inject a code that would automatically scan printed documents for sensitive information, transmitting the data to a Twitter feed. They showed an infected computer could instruct the printer's fuser, the one used to dry off the paper, to continuously heat up until the device self-destructs or, if it lacks a fuse, to set itself on fire. They also proved a hijacked printer could act as a gate-opener for a full-effect attack on a company network. They even made a demo from computers running Mac and Linux operating systems. HP representatives argue the situation might not be all that disastrous, claiming their newer models check for signatures while performing firmware updates. However, they are currently investigating the issue to determine exactly what is affected and what can be done about it. Even though later printer models should be more secure, the researchers claim one of the printers used in their tests was purchased not long ago."
Reference: http://news.softpedia.com/news/HP-Printers-May-Be-Remotely-Set-On-Fire-Researchers-Say-237254.shtml

19. GameOver ZeuS variants spread via NACHA spam launches DDOS against Financial Institutions

FBI Denver Cyber Squad advises citizens to be aware of a new phishing campaign.:
Reference: http://www.fbi.gov/denver/press-releases/2011/fbi-denver-cyber-squad-advises-citizens-to-be-aware-of-a-new-phishing-campaign?utm_campaign=email-Immediate&utm_medium=email&utm_source=denver-press-releases&utm_content=51037

Williston, Sandra

From: Murphy, Gregg
Sent: December-07-11 11:15 AM
To: Dincoy, Rana
Subject: RE: Confirming my write-up for an incident you handled (event #2496)

s.13(1)(b)
s.16(2)(c)

No, [redacted] Thanks!

From: Dincoy, Rana
Sent: December-07-11 11:14 AM
To: Murphy, Gregg
Subject: RE: Confirming my write-up for an incident you handled (event #2496)

The affected non-federal entities [redacted] right? I am addressing that (briefly) in a later section under "Education"... Were there other types of orgs we notified?

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

From: Murphy, Gregg
Sent: December-07-11 10:25 AM
To: Dincoy, Rana
Subject: RE: Confirming my write-up for an incident you handled (event #2496)

Hi Rana,

Under Analysis, it should state [redacted]

Thanks,
Gregg

From: Dincoy, Rana
Sent: December-06-11 4:57 PM
To: Murphy, Gregg
Subject: Confirming my write-up for an incident you handled (event #2496)

Hi Gregg,

I do a weekly summary aimed at non-technical executives in the government, containing noteworthy incidents and news. Could you please confirm my writeup below for the [redacted] Thanks so much...

Federal Government. [redacted] TeaMp0ison, a famous hacktivist group that is sometimes allied with the group

Anonymous, claimed credit for this event. [redacted]

Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | 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 +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

s.13(1)(b)
s.16(2)(c)

Williston, Sandra

From: Beaudoin, Luc S
Sent: December-03-11 8:22 AM
To: CYBERDO
Subject: Re: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication

About this topic, could you open an activity. I contacted the

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: CYBERDO
Sent: Friday, December 02, 2011 11:34 AM
To: * NCSD-CCIRC
Subject: FW: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication

FYI

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: Bendelier, Kenneth
Sent: December-02-11 11:33 AM
To: CYBERDO; Turbide, Frank; Beaudoin, Luc S
Subject: FW: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication
Importance: High

FYI

-----Original Message-----
From: E-Secure-IT [mailto:alert@e-secure-it.com]
Sent: December-02-11 11:23 AM

To: Bendelier, Kenneth
Subject: Critical: Heads-Up - FBI Warns of New Fraud Scam - Zeus Variant Can Defeat Two-Factor Authentication
Importance: High

Generated by your Alert Subscription on Folder:
- Scam / Fraud / Hoax Alerts
- - Global Business ICT Risks
Source: Bank Information Security
Complete item: http://ffiec.bankinfosecurity.com/articles.php?art_id=4295&pg=1

Description:
The Federal Bureau of Investigation has issued a warning about a new Zeus malware attack targeting commercial bank accounts, ultimately leading to incidents of corporate account takeover. The Zeus variant used: a malware called Gameover, which the FBI says is able to defeat several forms of dual-factor authentication.

To protect themselves, the FBI suggests consumers and businesses pay attention to suspicious e-mails. In the case of the Gameover attacks, e-mails purporting to come from NACHA-The Electronic Payments Association contained malicious links. NACHA does not traditionally send e-mails directly to businesses or consumers. Receipt of a direct e-mail from an organization such as NACHA should raise a red flag.

But according to the FBI's Denver Cyber Squad, it's not just phishy e-emails and dual-factor get-arounds that have made the Gameover attacks forces to be reckoned with. As it turns out, the fraudsters behind this scheme combined a number of tactics, including the use of money mules and denial of service attacks, to con businesses and banks out of funds.

"After the accounts are compromised, the perpetrators conduct a distributed denial of service (DDos) attack on the financial institution," the FBI states. "The belief is the DDoS is used to deflect attention from the wire transfers, as well to make them unable to reverse the transactions."

Over the past two weeks, since the Gameover scheme was discovered, the FBI has tracked fraudulent wire transfers routed to high-end jewelry stores. And here is where the scheme takes its twist. Money mules, which've been hired to visit these stores, where funds have been fraudulently transferred, go to pick up jewels worth the amount of the fake wire.

"A money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as pending and releases the merchandise to the mule," the FBI states. "Later on, the transaction is reversed or cancelled ... and the jeweler is out whatever jewels the money mule was able to obtain."

Connecting the Dots
Fraudsters' ingenuity in the Gameover scheme is concerning.

"We've gotten fairly good at the Red Flag rules and detecting money mules, so the attackers are now figuring out they need to stall for time to get the cash," says Mike Smith, an online security expert with Akamai Technologies.

To do that, fraudsters are launching DDoS attacks against the banking institutions, just to distract them long enough to get the money and run.

"These attacks kill the interface that the customers are used to seeing, as well as the interface the banks use, like the APIs they use to do their transfers between each other," Smith says.

Cybercriminals have figured out how to connect the dots. They are committing cross-channel fraud.

The scam relies on traditional phishing and spear-phishing tactics to get in the door. Spear-phishing e-mails are sent to executives, who oftentimes are identified via social networking channels like LinkedIn and corporate databases. Additionally, the fraudsters send massive phishing e-mails to every employee in an organization, just waiting for one with access to the corporate online banking account to click a link.

Once the malware is launched, the fraudsters can monitor keystrokes and the online bank sites those infected PCs visit.

But it's the DDoS and money mule additions that bring the fraud full circle.

"You usually see one of three things in a DDoS attack," Smith says:

A protection racket scam, which involves an attack against an ecommerce site that blackmails the site into paying a few to stop the attack;

An activist threat, like the ones the industry has seen waged by groups such as Anonymous against entities for social reasons;

A political threat, which could be waged against a corporation or country by a nation state.

"This is an entirely different scenario," Smith says. "What you're seeing is that the attack is designed to slow down the businesses being defrauded and slow down the bank's response."

Dave Jevans of the Anti-Phishing Working Group says financial institutions have two theories about the reasoning behind the attacks: to shut down access and distract bank security and IT. For large institutions, the attacks likely only serve as distractions.

E-Secure-IT
https://www.e-secure-it.com

Williston, Sandra

From: Beaudoin, Luc S
Sent: December-02-11 6:20 PM
To: [redacted] **s.19(1)**
Subject: Re: ZeuS and NACHA **s.20(1)(b)**

Ack. Tx.

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: [redacted]
Sent: Friday, December 02, 2011 04:03 PM
To: Beaudoin, Luc S
Subject: RE: ZeuS and NACHA

Luc,

[redacted]

From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca]
Sent: December 2, 2011 3:35 PM
To: [redacted]
Subject: ZeuS and NACHA

For CFI Info. Have you guys seen such DDOS ?

//////

Source: Bank Information Security
Complete item: http://ffiec.bankinfosecurity.com/articles.php?art_id=4295&pg=1

Description:
The Federal Bureau of Investigation has issued a warning about a new Zeus malware attack targeting commercial bank accounts, ultimately leading to incidents of corporate account takeover. The Zeus variant used: a malware called Gameover, which the FBI says is able to defeat several forms of dual-factor authentication.

To protect themselves, the FBI suggests consumers and businesses pay attention to suspicious e-mails. In the case of the Gameover attacks, e-mails purporting to come from NACHA-The Electronic Payments Association

contained malicious links. NACHA does not traditionally send e-mails directly to businesses or consumers. Receipt of a direct e-mail from an organization such as NACHA should raise a red flag.

But according to the FBI's Denver Cyber Squad, it's not just phishy e-emails and dual-factor get-arounds that have made the Gameover attacks forces to be reckoned with. As it turns out, the fraudsters behind this scheme combined a number of tactics, including the use of money mules and denial of service attacks, to con businesses and banks out of funds.

"After the accounts are compromised, the perpetrators conduct a distributed denial of service (DDos) attack on the financial institution," the FBI states. "The belief is the DDoS is used to deflect attention from the wire transfers, as well to make them unable to reverse the transactions."

Over the past two weeks, since the Gameover scheme was discovered, the FBI has tracked fraudulent wire transfers routed to high-end jewelry stores. And here is where the scheme takes its twist. Money mules, which've been hired to visit these stores, where funds have been fraudulently transferred, go to pick up jewels worth the amount of the fake wire.

"A money mule arrives at the store, the jeweler confirms the money has been transferred or is listed as pending and releases the merchandise to the mule," the FBI states. "Later on, the transaction is reversed or cancelled ... and the jeweler is out whatever jewels the money mule was able to obtain."

Connecting the Dots
Fraudsters' ingenuity in the Gameover scheme is concerning.

"We've gotten fairly good at the Red Flag rules and detecting money mules, so the attackers are now figuring out they need to stall for time to get the cash," says Mike Smith, an online security expert with Akamai Technologies.

To do that, fraudsters are launching DDoS attacks against the banking institutions, just to distract them long enough to get the money and run.

"These attacks kill the interface that the customers are used to seeing, as well as the interface the banks use, like the APIs they use to do their transfers between each other," Smith says.

Cybercriminals have figured out how to connect the dots. They are committing cross-channel fraud.

The scam relies on traditional phishing and spear-phishing tactics to get in the door. Spear-phishing e-mails are sent to executives, who oftentimes are identified via social networking channels like LinkedIn and corporate databases. Additionally, the fraudsters send massive phishing e-mails to every employee in an organization, just waiting for one with access to the corporate online banking account to click a link.

Once the malware is launched, the fraudsters can monitor keystrokes and the online bank sites those infected PCs visit.

But it's the DDoS and money mule additions that bring the fraud full circle.

"You usually see one of three things in a DDoS attack," Smith says:

A protection racket scam, which involves an attack against an ecommerce site that blackmails the site into paying a few to stop the attack;

An activist threat, like the ones the industry has seen waged by groups such as Anonymous against entities for social reasons;

A political threat, which could be waged against a corporation or country by a nation state.

"This is an entirely different scenario," Smith says. "What you're seeing is that the attack is designed to slow down the businesses being defrauded and slow down the bank's response."

Dave Jevans of the Anti-Phishing Working Group says financial institutions have two theories about the reasoning behind the attacks: to shut down access and distract bank security and IT. For large institutions, the attacks likely only serve as distractions.

E-Secure-IT
https://www.e-secure-it.com

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

Williston, Sandra

From: Murphy, Gregg
Sent: November-30-11 7:55 AM
To: Beaudoin, Luc S
Subject: RE: [redacted] United Nations Hacked by TeaMp0isoN, Details Leaked

No problem. Event created and I'll take care of it this morning.

Gregg

s.16(2)(c)
s.19(1)
s.20(1)(c)

-----Original Message-----
From: Beaudoin, Luc S
Sent: November-29-11 5:34 PM
To: Murphy, Gregg; [redacted]
Cc: Moore, Bruce
Subject: Re: [redacted] United Nations Hacked by TeaMp0isoN, Details Leaked

Yes. Worth an event...sorry catching up.

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: Murphy, Gregg
Sent: Tuesday, November 29, 2011 09:30 AM
To: Beaudoin, Luc S
Cc: Moore, Bruce
Subject: FW: [redacted] United Nations Hacked by TeaMp0isoN, Details Leaked

Item for consideration.

Teampoison hacked UN website and posted usernames and passwords. [redacted]

[redacted]

Would this be an item we follow-up on?

Thanks,
Gregg

-----Original Message-----
From:
Sent: November-29-11 8:48 AM
To:
Subject: [United Nations Hacked by TeaMp0isoN, Details Leaked

Title: United Nations Hacked by TeaMp0isoN, Details Leaked
Author: Eduard Kovacs
Source: Softpedia
Date Published: 29th November 2011

[redacted]

http://news.softpedia.com/news/United-Nations-Hacked-by-TeaMp0isoN-Details-Leaked-237086.shtml

[redacted]

s.19(1)

s.20(1)(c)

[redacted]

'To communicate simply you must understand profoundly'

[redacted]

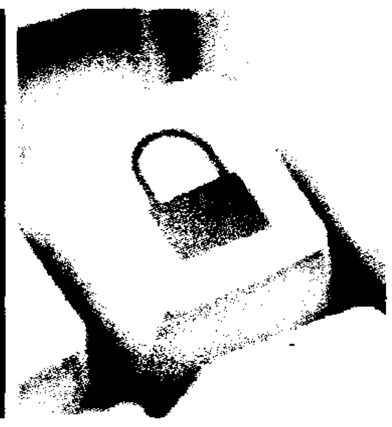
[redacted]

Public Safety Canada | Sécurité publique Canada

Canada

PROTECTED B
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-004



For the Week of

5 Nov – 10 Nov 2011

Issued: 17 Nov 2011

HIGHLIGHTS:

- **Threat Warnings:** Nothing significant to report.

- **CCIRC Products Released:** Information Note IN11-002 (DNS Changer Infrastructure) on the massive internet fraud scheme linked to the week's FBI arrests – victims in Canada include federal government departments; Technical Report TR11-001(Malware Infection Recovery Guide); Advisory AV11-048 (Highlights of Microsoft Security Bulletin for November 2011)

- **Reported Incidents:** (1) A lapsed federal government department website used to advertise escort services; (2) Website vandalism in the manufacturing, health, and information technology sectors; (3) Computer infections in federal and provincial governments, health, energy and education sectors; (4) Threat actors masquerading as Canadian financial and telecommunication companies luring internet users to malicious websites (phishing); (5) Computers in the manufacturing and telecommunication sectors being used to control "zombie" computer networks (botnets) that steal data

- **Noteworthy Open Source Reports:** (1) Hackers threaten City of Toronto; (2) 70 percent of all maliciously registered domain names in the world established by Chinese cyber criminals; and (3) The US plans to trap the next WikiLeaker.

PROTECTED B
DRAFT

PURPOSE

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered by or reported to the Canadian Cyber Incident Response Centre (CCIRC), any CCIRC information products issued during the week, and other noteworthy open source reports.

NOTABLE INCIDENTS– 5 NOVEMBER THROUGH 10 NOVEMBER 2011:

Government Systems.

Federal. CCIRC learned of media reports that a lapsed Transport Canada domain for a special domain was being used to advertise escort services. CCIRC informed the Cyber Threat Evaluation Centre (CTEC), the Government's Cyber Incident Handler of this matter. It is reported the link between Transport Canada's website and this special domain has been severed.

CCIRC continued to receive infection reports for computers at CBC. CCIRC notified CTEC, the federal government's incident handler of these reports.

- **Analysis:** Although the Transport Canada related event may not be considered as a cyber incident, it illustrates the challenges with maintaining control of one's brand on the internet. Since this website did not violate any copy rights by using Government of Canada logos, there appears to be no legal recourse. It is unknown whether the escort service hoped to attract more internet traffic to its website by using and keeping the old contents of this particular domain name.

Provincial. CCIRC received infection reports for computers on the Nova Scotia government system. CCIRC notified contacts of these reports and provided mitigation advice. The impact on the organization is unknown.

- **Analysis:** The infections reported for the provincial computers are commonly found on the internet designed to compromise computers, then steal information and/or force them to do malicious acts online. CCIRC continues to receive reports of possible infections on computers of provincial governments. This may be because these governments connect to a large provincial population who may not practice good cyber security and some of these infections.

Canadian Critical Infrastructure:

Financial Sector. Threat actors, impersonating a range of well known Canadian financial institutions, attempted to lure users to reply to e-mails with their personal information and on-line credentials, as well as visit malicious websites. CCIRC addressed the incident that continued to pose a threat by notifying RBC, as well as Google phishing, the Anti-Phishing Working Group and Microsoft, so internet users may be alerted if they encounter that malicious website.

- **Analysis:** This type of malicious activity is commonly seen by CCIRC and continues to cause financial losses for Canadians. Canadian banks react to these types of incident reports in a very timely manner and are usually quite proficient at ensuring these malicious websites are no longer accessible to the public. The new anti-SPAM legislation, expected to come into force in 2012, is meant to address these situations. However, enforcement of this legislation could be challenging when these malicious websites are located outside of Canada.

Telecommunications Sector. Threat actors impersonating Rogers Communications tried to persuade internet users to disclose personal information.

- **Analysis:** The type of personal information being requested by the threat actors would allow them to carry out identity theft. It is unknown whether there were internet users in Canada who provided the information.

CCIRC also received reports that a computer at iWeb Technologies, a web-hosting firm in Montreal, was being used as a controller of a network of compromised computers used for malicious purposes (a Zeus botnet). CCIRC notified the company and the RCMP. The company took action to ensure its computer was no longer being used for this malicious purpose.

- **Analysis:** Infection reports are one indication of the prevalence of computer infections in Canada among internet service subscribers. In Canada, different service providers have varying levels of protection for their customers.

Energy Sector. CCIRC continued to receive infection reports on computers of Canadian Natural Resources Limited, a large oil & gas producer. CCIRC again notified the company of the potential infections. The impact on the organization is unknown.

Health Sector. CCIRC again received a computer infection report for E-Health Ontario. The impact on the organization is unknown.

Transportation Sector. CCIRC also received reports that a computer for Victoria Avionics was being used as a controller of a network of compromised computers used for malicious purposes (a Zeus botnet). Victoria Avionics is located in Sydney BC, and is a sales and service centre for aircraft avionics products. CCIRC notified and gave mitigation advice to the company and their hosting internet service provider. The RCMP was also notified. The impact of this compromise is unknown.

- **Analysis:** Victoria Avionics is a Transport Canada approved company that is using a Canadian web hosting organization (Uniserve) and could have compromised their clients or business partners' computers. Reports show that a computer at this web hosting organization is serving as the botnet controller, which could indicate this web hosting organization itself has been compromised. The organization is known to host 164 web sites, which may have been compromised.

Public. CCIRC received infection reports on computers of nine universities across Canada and included the Universities of Ottawa, Guelph, and Queens. This is down from seventeen last week.

CCIRC Products:

1. **Information Note IN11-002 (DNS Changer Infrastructure):** This information product was publicly released to help potential Canadian victims of the world-wide internet fraud, uncovered by the FBI after a two year investigation. There were 4.2 Million infected sites in over 100 countries and Canadian victims identified so far include federal government departments. Eight Estonian individuals were arrested and one Russian national is still at large. The known impact of this fraud was theft of personal data, including credit card numbers as well as defrauding companies who placed on-line advertisements.

In this highly sophisticated fraud which had been ongoing for four years, threat actors remotely compromised computers around the world. These criminals then used rogue DNS servers, which caused those internet users of those computers to be redirected to malicious websites. The US indictment alleges that the defendants, who masqueraded as legitimate publishers in the internet advertising industry, had financial incentives to have many internet users click on the links for certain websites and on-line advertisements. The US Government has temporarily replaced the rogue DNS servers by "clean ones", so users with infected computers do not lose their ability to connect to the internet.

CCIRC continues to work with the FBI and other Computer Emergency Response Teams around the world to learn more information about this fraud and identify Canadian victims.

2. **Technical Report TR11-001 (Malware Infection Recovery Guide):** This was a publicly released report, also directly sent to CCIRC's government and critical infrastructure stakeholders. The report contained general technical advice to organizations that may be infected with malicious rootkit software, which can be difficult to remove. It was thought to be timely advice given the type of internet fraud publicized this week, as explained above.

3. **Advisory AV11-048 (Microsoft Security Bulletin Summary for November):** CCIRC brought to stakeholders' attention important Microsoft Security Bulletin highlights by publicly releasing this product, which was also sent directly to stakeholders.

Noteworthy Open Source Reports:

Hackers threaten Toronto over Occupy policy – The notorious hacker group Anonymous is threatening to have the City of Toronto "removed from the Internet" if city officials move forward with plans to evict the Occupy Toronto camp. "The brave citizens of Toronto are peaceful and well mannered occupiers, and we will not let the city . . . get involved," says a computerized voice in a Saturday video by the group.

- **Analysis:** Anonymous is a group of loosely affiliated – socially conscious – hackers that have in the past successfully carried out threats. They last targeted Canada in an operation called 'Tarrmageddon' (i.e. targeting oil sand companies in Alberta). It is possible that the City of Toronto's services could be affected by such an attack. As such, CCIRC has contacted the city of Toronto's Internet Service Providers to inform them of this threat – they are taking precautionary measures.

Chinese cyber criminal have established ~70% of all maliciously registered domain names in the world – A new survey by the Anti-Phishing Working Group (APWG) reveals that phishing attacks perpetrated against Chinese e-commerce and banking sites soared by 44 percent in the first half of 2011. Some 70 percent of all maliciously registered domain names in the world were established by Chinese cyber criminals for use against Chinese brands and enterprises.

- **Analysis:** As elsewhere in the world, Chinese internet users are also targeted for their financial information by cyber criminals impersonating reputable companies. It seems Chinese cyber criminals particularly preferred to register their own domain names rather than hack another domain as other cyber criminals do. This survey is believed to contain reliable information not available to many western sources.

The APWG is a reputable non-profit global pan-industrial and law enforcement association, where Government of Canada officials (ex: Justice and Industry Canada) also participate. Chinese information for this survey was provided by the China Internet Network Information Centre, who is also the secretariat for the Anti-Phishing Alliance of China (APAC). APAC has more than 140 member institutions in the country, including banks, e-commerce sites, and domain registrars, and has an efficient reporting and domain suspension program.

The United States' Defence Advanced Research Projects Agency (DARPA) Plans to Trap the Next WikiLeaker: – DARPA funded researchers are building a program for "generating and distributing believable misinformation." Their ultimate goal is to plant, auto-generated, false documents in classified networks and program them to track down intruders' movements. The program aims to both: (1) scare off individuals browsing WikiLeaks; and (2) minimize insider threats (one of the greatest vulnerabilities in military networks).

- **Analysis:** Basically the US government is creating products capable of tracking individuals, and as such, there may be legal / privacy implications.

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

PROTECTED B
DRAFT

DISCLAIMER

This publication is **UNCLASSIFIED – For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in 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.

NOTES

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 Flashes marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

Williston, Sandra

From: Beaudoin, Luc S
Sent: November-17-11 10:53 AM
To: Ku, Shawn; Mattioli, Mary-Ann; Coady, Therese
Subject: RE: Operation Intersect dashboard - Cyber

we do not have the exact number. you can say:

CCIRC estimates that out of the 4 millions affected computers around the world, approximately 80 000 would be in Canada.

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: Ku, Shawn
Sent: November 17, 2011 9:32 AM
To: Mattioli, Mary-Ann; Coady, Therese; Beaudoin, Luc S
Subject: Re: Operation Intersect dashboard - Cyber

CCIRC provided the numbers verbally in both their CCIRC daily meeting as well as the GOC Operations meeting at 09:15.

Luc, can you address...I'm away from the office at a conference.

Shawn Ku
(613) 991-7054

From: Mattioli, Mary-Ann
Sent: Thursday, November 17, 2011 09:27 AM
To: Coady, Therese; Ku, Shawn
Subject: RE: Operation Intersect dashboard - Cyber

Hello,

Please see the below:

Events of Note:

1. RCMP Anti-fraud Centre reported they are seeing an increase in phishing schemes targeting Air Canada, looking for Aeroplan number or personal information.

2. The FBI uncovered a network of Domain Name System (DNS) servers controlled by cyber criminals. The FBI worked in collaboration with international law enforcement agencies and the cyber security community to disable these malicious DNS servers. Unfortunately, this malicious infrastructure has been used over the last three years to steal personal information from millions of people around the world. Cyber criminals infected these users' computers with malicious code that changes the users' DNS configurations to forward all their web content requests to a rogue DNS rather than a legitimate one.

Public Safety Canada has issued an assessment along with suggested action in order to determine if your computer was infected with this variant of DNS Changer malicious code.
http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-002-eng.aspx

This event generated significant media attention: **FBI arrests six for DNS hijacking scam worth $14 million**. "Charges against Six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries have been raised by the United States Attorney for the Southern District of New York." Reference: http://www.net-security.org/secworld.php?id=11928;

SHAWN: Approximately 80,000 Canadians were affected by the DNS poisoning (directing them to malicious sites, where possible criminal activity was perpetrated). I can't seem to find this information in the articles…where did you get this AND can I use this?

Thanks, Mary-Ann

From: Coady, Therese
Sent: November 17, 2011 8:23 AM
To: Ku, Shawn; Mattioli, Mary-Ann
Cc: Beaudoin, Luc S; Dole, Natalie
Subject: RE: Operation Intersect dashboard - Cyber

Thanks folks. I appreciate all of the efforts and I am well aware of the international aspect of cyber i.e. what happens and is reported in one country likely is affecting others - but that can be said for pretty much everything we do, depending on the context, so, for this audience, my purpose and focus was on the impact to Canada.

Agree about SCADA systems - but we have already reported this to the group, so if we are going to update I believe we need to look for greater Canadian content. I see events of interest #2 and #3 falling into this category and since we cannot provide more info due to confidentiality issues (totally understood), then I don't see the point in raising it.

Anonymous group - would have been great, but it was surpassed by the ITAC - that's all.

#4 - I did not see any reference to 80,000 Canadians being affected, but I admit that I did not open the article being referenced - if it was in the article, then it should be highlighted in the text. If it's extra info that we are at liberty to share with this group, then let's put that in there, since that is indeed what is important.

Thanks,
Therese

From: Ku, Shawn
Sent: November 16, 2011 5:09 PM
To: Mattioli, Mary-Ann
Cc: Coady, Therese; Beaudoin, Luc S; Dole, Natalie
Subject: Re: Operation Intersect dashboard - Cyber

s.16(2)(c)

I highlighted the first article on SCADA systems to bring awareness that SCADA systems have a wide application base (even prison doors, which I wasn't aware of). And due to the focus of the Intersect group, I thought they may be interested. No problem if you want to remove for brevity purposes.

The second article was highlighted due to increasing threats/activity from the Anonymous group. I agree with Therese that we can reference the

As a general comment, I understand these articles are U.S.-based, but cyber attacks are applicable anywhere - especially with the Anonymous Group. The second article provides an assessment of Anonymous's capability to attack ICS, that might be of interest to the Intersect group, given the lack of a Canadian assessment at this time - to note, even the ITAC Laser on Anonymous quotes this article.

In terms of the threat level - although SARA does not deal specifically with threat levels, my latest risk assessment is High. There is a probability that cyber attacks will continue, given historical and present information; as well, these attacks could result in significant impacts to several CI sectors. This provides leads to a high risk. But I am ok if you want to keep the threat level as medium...

Regarding Events of Interest, I do not have more information on #2; however I believe it highlights a significant attack on a CI (albeit unsuccessful). We will not be able to divulge the company due to confidentiality.

I agree we can remove #3, but it does highlight that Canadian companies deploying SCADA systems may be vulnerable to attack, possibly putting Canadian CI at risk.

I think #4 should be kept in. Approximately 80,000 Canadians were affected by the DNS poisoning (directing them to malicious sites, where possible criminal activity was perpetrated).

Just my thoughts. Cheers, Shawn

Shawn Ku
(613) 991-7054

From: Mattioli, Mary-Ann
Sent: Wednesday, November 16, 2011 03:38 PM
To: Coady, Therese; Beaudoin, Luc S; Ku, Shawn
Subject: RE: Operation Intersect dashboard - Cyber

In my humble opinion ;o), although I am no CYBER expert, leaving the threat at MEDIUM is ok. The articles below speak to incidents in the US, so I don't think it warrants us to raise it to HIGH.

However, I do need more guidance with the cyber information:

1. Although the first two articles do not pertain to Canada, does it possibly show a trend that there are vulnerabilities with SCADA systems in general...and that hackers seem to be interested in these vulnerabilities? Can we make that connection to Canada?

2. As for Events of Note, I cannot answer those questions so again, I defer to the CYBER experts.

Thank you!! Mary-Ann

From: Coady, Therese
Sent: November 16, 2011 11:14 AM
To: Mattioli, Mary-Ann; Beaudoin, Luc S
Subject: RE: Operation Intersect dashboard - Cyber

s.16(2)(c)

Hi you two. This is great, but a bit too much in my opinion. I think the group benefits from learning about items that are specific to Canada. In addition, does any of this change our current "status" for our dashboard for Cyber - which, I believe, is at MEDIUM due to continuing events/attacks and criminal cyber activity.

First article: This article speaks to US facilities - is it the same in Canada? If not, then suggest removing.

Second article on Anonymous is timely and interesting, but [redacted] on this yesterday - so I doubt there is anything extra to be provided in the article below - suggest removing please.

Re: Events of Note:

1. This is good.

2. Doesn't tell us much - suggest taking it out if we can't provide concrete details. Is this "new"?

3. Cdn connection - but what does it all mean? I am a neophyte and many of the group don't necessarily make all the connections to how it may affect them or their work in EM response, etc.

4. Interesting, but, again, is there a Cdn connection/reference, which we can reference?

Thanks,
Therese

From: Mattioli, Mary-Ann
Sent: November 16, 2011 10:31 AM
To: Beaudoin, Luc S
Cc: Coady, Therese
Subject: FW: Operation Intersect dashboard - Cyber

Hi Luc,

It's that time again, can you please approve the below before we present this at next weeks Operation Intersect meeting?

Thank you, Mary-Ann

Potential cyber attacks on Industrial control systems (ICS)

SCADA Systems Flaws Exploited to Open Prison Doors: The discovery of the Stuxnet worm has alerted governments around the world about the possibility of industrial control systems being targeted by hackers. As a result, security researchers are concentrating on preemptively finding out the bugs that plague them so that they can be patched before the hackers have the chance to exploit them. These industrial control systems (ICS) – such as SCADA (supervisory control and data acquisition) - are computer systems that monitor and control industrial and infrastructure processes, and often control heating, ventilation, and air conditioning, access, communication and energy consumption inside a variety of private and public facilities. Among those facilities

are also state and federal prisons in the U.S., and seeing that the control of access and communication within them is of critical importance, a group of researchers have set up to discover whether bugs in the SCADA systems allowed remote attackers to take them over. The researchers have relatively easily succeeded in their attempt and have developed attacks that would allow prison doors to be opened (temporarily or permanently) without alerting the guards in the control room about it and that would shut down internal communications and closed-circuit television systems. The U.S. Department of Homeland Security has confirmed the validity of their results.
Reference: http://net-security.org/secworld.php?id=11911

U.S. DHS expects Anonymous to attack infrastructure. The U.S. Department of Homeland Security indicates that Anonymous, a hacker group, is looking at industrial control systems (ICS) for future attacks however its members have yet to demonstrate a capability to inflict damage to these systems. The information available on Anonymous suggests they currently have a limited ability to conduct attacks targeting ICS. However, experienced and skilled members of Anonymous in hacking could be able to develop capabilities to gain access and trespass on control system networks very quickly. Since vulnerabilities in ICS are plentiful, they can be taken advantage of for mounting attacks. Anonymous has still not targeted ICS, but the DHS expects them to start in the near future as the collective has already made it known that its members should be targeting energy companies that don't seem to make an effort towards a "greener" production.
Reference: http://www.net-security.org/secworld.php?id=11807

s.13(1)(a)
s.16(1)(a)
s.16(2)(c)

Events of Note:

1. RCMP Anti-fraud Centre reported they are seeing an increase in phishing schemes targeting Air Canada, looking for Aeroplan number or personal information.

2. A Canadian Internet Service Provider reported brute force password cracking attempts against their core infrastructure (routers) - the attempts were
unsuccessful.

[redacted]

4. The FBI uncovered a network of Domain Name System (DNS) servers controlled by cyber criminals. The FBI worked in collaboration with international law enforcement agencies and the cyber security community to disable these malicious DNS servers. FBI public release: http://www.fbi.gov/DNS-malware.pdf

This event generated significant media attention: **FBI arrests six for DNS hijacking scam worth $14 millions**. "Charges against Six Estonian nationals and one Russian national for engaging in a massive and sophisticated Internet fraud scheme that infected with malware more than four million computers located in over 100 countries have been raised by the United States Attorney for the Southern District of New York."
Reference: http://www.net-security.org/secworld.php?id=11928

Page 1866

is a duplicate

est un duplicata

Page 1867

is a duplicate

est un duplicata

Dvorkin, Corey

From: Porter, Neal
Sent: November-15-11 3:33 PM
To: Dvorkin, Corey
Subject: FW: ITAC 11/260 - "Anonymous" threatens Toronto with cyber attack / Le groupe Anonymous menace de commettre des cyberattaques contre Toronto
Attachments: Laser11260-E.PDF; Laser11260-F.PDF

From: GOC-COG
Sent: Tuesday, November 15, 2011 3:03 PM
To: _GOC Distribution List / Liste de distribution du COG
Subject: ITAC 11/260 - "Anonymous" threatens Toronto with cyber attack / Le groupe Anonymous menace de commettre des cyberattaques contre Toronto

UNCLASSIFIED – For Official Use Only

2011 11 15

Please find attached ITAC 11/260 "ANONYMOUS" THREATENS TORONTO WITH CYBER ATTACK"

This ITAC report is for official use only and is not for public dissemination. Recipients may distribute it, at their discretion, to their **Canadian** security and emergency management contacts.

****

NON-CLASSIFIÉ – Réservé à des fins officielles seulement

2011 11 15

Vous trouverez ci-joint le document CIET 11/260 *«LE GROUPE ANONYMOUS MENACE DE COMMETTRE DES CYBERATTAQUES CONTRE TORONTO»*

Ce rapport CIET est diffusé à des fins officielles seulement et ne doit pas être transmis au public. Les personnes qui le reçoivent peuvent le communiquer, à leur discrétion, à leurs contacts **canadiens** de la sécurité et de la gestion des urgences.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: GOC-COG@PS-SP.GC.CA

11 / 260-E
2011 11 15

UNCLASSIFIED -
See Handling Instructions

"Anonymous" threatens Toronto with cyber attack

KEY POINTS

- On 2011 11 13, the international collective "Anonymous" posted a video on *YouTube* threatening cyber attacks against the City of Toronto if it follows through with plans to bring the Occupy protest movement "to a peaceful conclusion". In the video, "Anonymous" stated that Toronto would be "removed from the Internet" if the city fails to leave the protestors alone.
- As of 1400 hrs, 2011 11 15, media reporting indicates that Toronto city staff have given eviction notices to Occupy Toronto protestors, saying that protestors must leave the area immediately.
-
-

ANALYSIS

1) On 2011 11 13, the international collective "Anonymous" posted a video on *YouTube* threatening cyber attacks against the City of Toronto if it follows through with plans to bring the Occupy protest movement "to a peaceful conclusion". In the video, "Anonymous" stated that Toronto would be "removed from the Internet" if the city fails to leave the protestors alone.

2) "Anonymous" has conducted many successful cyber attacks. For example, in early 2010, the group attacked Australian government web sites with a large Distributed Denial of Service (DDoS) attack. Further, open sources report that the Mayor of St. Louis, Missouri had his emails, political backers, as well as contact information posted online recently by a hacker who claimed to be a member of "Anonymous" after an eviction notice was served to that city's Occupy protestors. There have also been threats made by "Anonymous" that have not materialized, such as a recent claim by the group that they would "erase" the Toronto Stock Exchange (TSX) from the Internet.

3) During the summer of 2011, dozens of "Anonymous" members were arrested in several countries for their attacks on corporate and sensitive government web sites. The group gained notoriety for taking down PayPal and Visa for ceasing to conduct business with *WikiLeaks* after it released thousands of US diplomatic cables. "Anonymous" also took down the web site of Monsanto, a major biotech company, accusing it of being "corrupt, unethical and downright evil". The group has vowed to avenge the arrest of its members.

4) According to open information, in most cyber attacks, "Anonymous" uses a method referred to as DDoS, which consists of directing a large traffic surge to a web site until it becomes overwhelmed and cannot operate efficiently. Depending on the design and capacity of a web site, DDoS attack consequences can range from a slow-down or speed-up to a potential crash of the site. "Anonymous" also uses a hacking tool known as structured query language injection attack, which consists of exploiting a vulnerable code on a computer system. This allows the hacker to bypass security measures, obtain access to the network and steal information.

5) On 2011 10 18, the US Department of Homeland Security (DHS), National Cyber-security and Communications Integration Center (NCCIC), was quoted as saying that the information available on "Anonymous" suggests they currently have a limited ability to conduct attacks targeting Industrial Control Systems (ICS). However, experienced and skilled members could develop capabilities to gain access and trespass on control system networks very quickly. Moreover, free educational opportunities (conferences, classes), presentations at hacker conferences and other high profile events / media coverage have raised awareness to ICS vulnerabilities and have likely shortened the time needed to develop sufficient tactics, techniques and procedures to disrupt ICS.

7) Social media indicates that one means of identifying "Anonymous" individuals or sympathisers may be the wearing of Guy Fawkes masks.

8) ITAC continues to monitor the situation and will provide updates as necessary.

[redacted]

HANDLING INSTRUCTIONS

This document is the property of the Integrated Terrorism Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to ITAC at [redacted] or to ITAC Partnerships at [redacted]

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with ITAC.

CIET ITAC
Centre intégré d'évaluation du terrorisme | Integrated Terrorism Assessment Centre
MENACE L A S E R ALERTE

11 / 260-F
2011 11 15

NON-CLASSIFIÉ -
Voir manipulation de renseignements

Le groupe Anonymous menace de commettre des cyberattaques contre Toronto

FAITS SAILLANTS

- Le 2011 11 13, le groupe international Anonymous a diffusé une vidéo sur *YouTube* dans laquelle il menace la municipalité de Toronto de cyberattaques si elle met fin pacifiquement au mouvement d'occupation comme elle entend le faire. Dans la vidéo, Anonymous affirme que Toronto disparaîtra d'Internet si elle s'oppose aux manifestants.
- À compter de 1400 hrs, le 2011 11 15, les médias annoncent que des employés de la ville de Toronto ont donné des avis d'expulsion aux démonstrateurs du mouvement d'occupation indiquant que ceux-ci doivent quitter les lieux immédiatement.
-
-

ANALYSE

1) Le 2011 11 13, le groupe international Anonymous a diffusé une vidéo sur *YouTube* dans laquelle il menace la municipalité de Toronto de cyberattaques si elle met fin pacifiquement au mouvement d'occupation comme elle entend le faire. Dans la vidéo, Anonymous affirme que Toronto disparaîtra d'Internet si elle s'oppose aux manifestants.

2) Le groupe Anonymous a réussi de nombreuses cyberattaques. Par exemple, au début de 2010, il a effectué une importante attaque par saturation contre des sites Web du gouvernement de l'Australie. De plus, selon des sources ouvertes, un pirate affirmant être membre d'Anonymous a récemment diffusé en ligne les courriels et des informations sur les bailleurs de fonds et les contacts du maire de St. Louis (Missouri) après que la municipalité a envoyé un avis d'expulsion aux participants du mouvement d'occupation. Toutefois, certaines menaces du groupe ne se sont pas réalisées, par exemple, celle de faire disparaître la Bourse de Toronto de sur Internet.

3) Au cours de l'été 2011, des dizaines de membres du groupe Anonymous ont été arrêtés dans différents pays pour avoir perpétré des attaques contre des sites Web gouvernementaux sensibles et des sites Web commerciaux. Le groupe a gagné en notoriété lorsqu'il a paralysé les systèmes de PayPal et de Visa, des entreprises qui ont cessé de faire des affaires avec *WikiLeaks* après la publication de milliers de câbles diplomatiques américains. Le groupe Anonymous a aussi paralysé le site Web de Monsanto, une importante société du secteur des biotechnologies, qu'il a qualifiée de corrompue et d'immorale et, somme toute, d'être le Mal incarné. Anonymous a juré de venger l'arrestation de ses membres.

4) Selon des informations de sources ouvertes, Anonymous recourt à l'attaque par saturation pour commettre la plupart de ses méfaits. Cette technique consiste à soudainement envoyer de grandes quantités d'informations aux serveurs d'un site Web jusqu'à ce que, saturés, ils ne puissent plus fonctionner efficacement. L'attaque par saturation peut provoquer le ralentissement et même le plantage d'un site Web, selon les ressources et la technologie sur lesquels est fondé le système. Le groupe utilise aussi une technique de piratage connue sous le nom d'injection SQL, laquelle consiste à exploiter une faille dans la programmation d'un ordinateur. Cette technique permet de contourner les mesures de sécurité, d'accéder à un réseau et de voler des informations.

5) Le National Cybersecurity and Communications Integration Center du Department of Homeland Security des États-Unis a indiqué le 2011 10 18 que les informations dont il dispose sur Anonymous donnent à penser que le groupe ne possède que des moyens limités pour effectuer des cyberattaques contre les systèmes de contrôle industriels. Toutefois, les membres habiles et chevronnés du groupe pourraient rapidement trouver des moyens d'accéder aux réseaux de ces systèmes. Qui plus est, la possibilité de s'instruire gratuitement (conférences, cours), les présentations données lors de conférences sur le piratage et les reportages des médias, entre autres, ont fait connaître la vulnérabilité des systèmes industriels et probablement raccourci le temps nécessaire pour mettre au point des tactiques, des techniques et des procédures qui permettront d'en perturber le fonctionnement.

[redacted]

7) Selon les médias sociaux, il pourrait, entre autres, être possible d'identifier les membres ou les sympathisants du groupe Anonymous par le port d'un masque à l'effigie de Guy Fawkes. [redacted]

8) Le CIET continue de surveiller la situation et fera le point au besoin. [redacted]

[redacted]

MANIPULATION DE RENSEIGNEMENTS

Le présent document est la propriété du Centre intégré d'évaluation du terrorisme (CIET) et a été préparé par celui-ci. Il s'appuie sur des informations qui proviennent de diverses sources et qui sont valables à la date de publication. Il est fourni à votre organisme ou ministère à titre confidentiel et peut être communiqué directement par votre organisme ou ministère à d'autres personnes selon le principe du besoin de savoir. Il ne doit pas être réutilisé, de quelque manière que ce soit, en tout ou en partie, sans le consentement de l'expéditeur. Pour tout commentaire, veuillez envoyer un courriel au CIET, à [redacted] ou communiquer avec la Sous-section des partenariats du CIET, au [redacted]

Le présent document peut faire l'objet d'une exception aux termes de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. On pourra également s'opposer à la communication des informations ou des renseignements qu'il contient en vertu de la *Loi sur la preuve au Canada*. Ces informations ou renseignements ne doivent être ni communiqués ni utilisés comme preuve sans consultation préalable du CIET.

Williston, Sandra

s.16(2)(c)

From: Beaudoin, Luc S
Sent: November-13-11 1:13 PM
To: 'Alain.Labossiere@ic.gc.ca'
Cc: [redacted]
Subject: U2-N2 FYI: Hacker group Anonymous threatens cyber attack if city evicts Occupy Toronto

November 13, 2011, 10:36 ET
Canadian Press
TORONTO _ The hacker group Anonymous is standing up for Toronto's Occupy movement.
In a video released on YouTube, the group threatens to launch a cyber attack on the city if officials interfere with the month-long demonstration.
The video says Toronto will be ``removed from the Internet'' unless the city promises to leave the protesters alone.
Mayor Rob Ford has asked the occupiers to dismantle their tent city in St. James Park.
A few protesters tried to set up a new base in the park behind the Ontario legislature this weekend, but their efforts cut short.
Police shut down the fledgling camp Saturday night and brought the demonstrators back to the original site.

http://www.theglobeandmail.com/news/national/toronto/anonymous-threatens-cyber-attack-if-city-interferes-with-occupy-toronto/article2234853/?from=sec431

Luc s input:

This is FYI as background if anything gets reported in the upcoming hours/days.

[redacted]

Also to consider: [redacted] (my own guess, no actual evidence of this targeting)

[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

Canadian Electricity Association (CEA) - *Security and Critical Infrastructure Protection Committee*

Chair: CEA (Francis Bradley)
Frequency: Quarterly meetings (in major Canadian cities)
Audience: Chief Security Officers of utility owners and operators

Comment: Federal officials and other external stakeholders are invited to attend a portion of the meeting to update on key areas of interest. NCSD, CIPD and the Government's ITAC participated at the September 2011 meeting in Fredericton, NB.

Next Meeting: November 15th in Ottawa

Public Safety Canada (PS) Participants: NCSD and CCRIC have been invited to participate.

Issues:

- The SCIP committee is currently brokering the NDA between the CEA and CCIRC, and will likely be looking to finalize the agreement at this meeting. Robert Pitcher from CCIRC will present on the NDA.
- Participation would provide an opportunity to propose the next-steps in the information sharing / NDA process (including a PS-wide agreement) while allowing PS to canvas for input from the CEA.
- [redacted] on November 15-17, 2011, including CCIRC, who will participate as an observer.
- Generally, participation is well received by SCIP committee members, and helps formalize bilateral relationships between PS and the various PT partners.

Energy and Utilities Sector Network (EUSN)

Chair: NRCan (Jeff Labonté; Felix Kwamena)
Frequency: Biannual meetings (in Ottawa)
Audience: Chief Security Officers of utility owners and operators; Federal stakeholders; PT Regulators and/or Operators

Next Meeting: November 16th in Ottawa (full-day).

Public Safety Canada (PS) Participants: Dorian Panchyson, NCSD; others TBD

Issues:

- This is an opportunity to network with key private sector representatives and entities, positioning NCSD as the conduit for the Government of Canada's approach to cyber security.
- [redacted]
- Discussions may also focus on the Information Sharing Document produced by CIPD.
- Certain participants may also be involved with GridEX 2011, [redacted]

Classified Briefing to the Energy Sector

Chair: NRCan (J. Labonté; F. Kwamena) but facilitated by Tim O'Neill at the RCMP

Frequency: Biannual meetings (in Ottawa)
Audience: Chief Security Officers of utility owners and operators; Federal stakeholders; PT Regulators and/or Operators

Next Meeting: November 17th (full-day) [redacted] s.19(1)

Public Safety Canada (PS) Participants: TBD

Issues:
- This is an opportunity for CCIRC to network with key operational colleagues.

Canadian Electricity Association (CEA) - *Regulatory Development Task Group*

Chair: CEA (Francis Bradley, with secretariat support from [redacted]
Frequency: Quarterly meetings (in major Canadian cities)
Audience: Executives for reliability / regulatory issues of utility owners and operators
Comment: Federal officials invite to update on files and network with committee members

Next Meeting: November 22nd, in Ottawa

Public Safety Canada (PS) Participants: NCSD, others TBD (Mike DeJong from CIPD has been invited.

Issues:
- NCSD and CIPD have been asked to participate and present. NCSD has given a "Cyber 101" to the RDTG in the past and the members are eager for NCSD to update on the Government's priorities related to cyber security.

- Given the committee's regulatory focus, this would be an opportunity to further two key areas of focus:

1. "Point of Contact" proposal

NCSD (in partnership with NRCan) had previously begun developing a proposal for the CEA to consider. This was scheduled to be discussed at a CEA meeting in April 2011, but given the timing with the federal election, neither NRCan or NCSD were able to participate.

As such, there is an appetite from RDTG members to hear more on the proposed "point of contract" idea, as FERC often expresses a desire for Canada (and the CEA) to develop a single point of contact for cyber and other reliability issues. The RDTG has informally asked if NCSD would develop a proposal for industry to consider - something that could be taken away and discussed by the RDTG committee more broadly. The issue is not so much with "information-sharing" (as provincial boards and regulators share information with one another quite regularly and with a certain degree of trust) but rather FERC's request for a "point of contact" to the Government of Canada.

2. US Cyber Legislation

The RDTG Secretariat has noted that the CEA members cannot form a consensus on the issue of US Cyber Legislation (the increase of regulatory authority for FERC). Input from CEA members into the legislative conversation is usually conducted through various trade associations in the US. As such, CEA was curious what the Federal Government's take on the proposed legislation was, and if there was any role for the Government moving forward. The CEA's perception was, given that the issue would be coordinated through provincial regulatory boards, the GoC tended to remove itself from discussions.

Williston, Sandra

From:
Sent: November-07-11 7:27 AM
To: Pitcher Robert
Subject:

s.16(2)(c)
s.19(1)
s.20(1)(b)

Follow link below for the info....if you didn t know already....;-)

Q?: are you still logging once in a while ?

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:
Sent: November 6, 2011 11:07 PM
To:
Subject: New Batch of ISO documents available 11/06/2011

Hello -

A new batch of ISO documents has been uploaded The list of documents is included below the signature block. You may download the documents from:

The FIRST ISO Home Page may be found here:

If you are interested in any of the work going on in ISO, please do not hesitate to contact Gaus (Damir Rajnovic) via his email at

Kind regards,

~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~

Pages 1880 to / à 1881

are withheld pursuant to section

sont retenues en vertu de l'article

20(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

*** FIRST restricted and confidential use mailing list. Do not Forward, Cc, Bcc, copy or summarize this email outside of the FIRST community without the express permission of the content owner(s). ***

first-teams mailing list

[redacted]

---

s.20(1)(c)

Williston, Sandra

From: Beaudoin, Luc S
Sent: November-04-11 6:22 PM
To: [redacted]
Subject: RE: Anonymous vs Los Zetas

s.16(2)(c)
s.19(1)

tx.

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: [redacted]
Sent: November 4, 2011 6:20 PM
To: [redacted]
Cc: alain.labossiere@ic.gc.ca
Subject: Anonymous vs Los Zetas

Here's some weekend or early Monday reading ☺

Some interesting analysis from Stratfor on Anonymous and the cartels in Mexico, particularly Los Zetas is worth a read. Stratfor doesn't typically do analysis on issues directly related to cybersecurity, so this is very encouraging to see.

http://www.stratfor.com/weekly/20111102-anonymous-vs-zetas-amid-mexico-cartel-violence

"Mexico's various cartels long have used the Internet to trumpet their triumphs on the battlefield and to taunt and even degrade their enemies. The cartels have posted videos of the torture, execution and desecration of the corpses of rivals. They also frequently monitor narcoblogs and sometimes even post on them. As demonstrated by the September blogger killings in Nuevo Laredo, Los Zetas appear to possess at least some rudimentary capability to trace online activity to people in the physical world. They are known to employ their own team of dedicated cyber experts and to have sources within the Mexican government. "

Some followup on the issue has been posted on Ars Technica:

http://arstechnica.com/tech-policy/news/2011/11/anonymous-calls-off-outing-of-narco-cartel-after-release-of-kidnapped-member.ars

--

[redacted]

Dincoy, Rana

From: Dincoy, Rana
Sent: November-04-11 3:56 PM
To: Anderson, Windy; Hatfield, Adam; Dvorkin, Corey; Schramm, Kent; Campbell, Tom; Maillé, Marie Anick; Labelle, Sébastien
Cc: Oldham, Craig; St-Louis, Danielle; Paquet, Alain; Coady, Therese; *
Subject: CCIRC Weekly Summary
Attachments: PS-SP-#510655-v2-WEEKLY_SUMMARY_FOR_EXECS_-_WEEK_OF_OCTOBER_24__2011.DOC

Good afternoon,

Please find attached, for your information and feedback, the Weekly Summary of noteworthy cyber events and news, accommpanied by analysis where applicable. The purpose of this product is to raise awareness of executives on current cyber threats seen by CCIRC that can impact an organization. At this point, the intended audience is a non-technical executive with security responsibilities. This product is unclassified but we anticipate producing a classified version in the future. The exact distribution list is yet to be determined.

This product is still in its pilot stage and any feedback you have would be greatly appreciated.

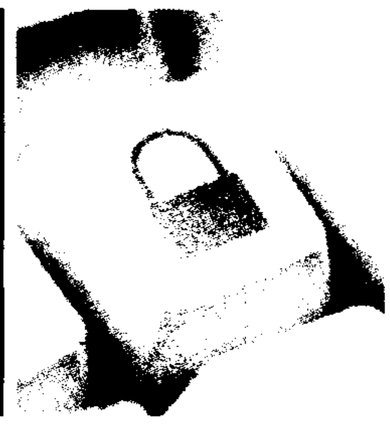
Rana Dincoy
Manager, Strategic Analysis| Gestionnaire d'analyse stratégique
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
257 Slater Street| 257 rue Slater
Ottawa, Ontario
Canada K1A 0P8
Telephone | Téléphone +1 613-991-7773
Facsimile | Télécopieur +1 613-954-3453
rana.dincoy@ps-sp.gc.ca
Government of Canada | Gouvernement du Canada

Public Safety Canada | Sécurité publique Canada

Canada

UNCLASSIFIED
DRAFT

WEEKLY SUMMARY
Canadian Cyber Incident Response Centre
Cyber Awareness Product: 11-S-002



For the Week of

22 - 28 Oct 2011

Issued: 4 Nov 2011

HIGHLIGHTS:

- **Threat Warnings:**
  - Hacker group Anonymous urged sympathizers to participate in a range of nuisance activities to coincide with Guy Fawkes Day on Nov 5 - [redacted]
- **Reported Incidents:**
  - Federal agency spammed with a suspicious e-mails referencing Gaddafi;
  - Targeted attacks on a Canadian Internet Service Provider's core infrastructure;
  - On-line recruitment of Canadian money launderers;
  - On-line posting of Canadian police personnel computer user information;
  - Computers in provincial governments, energy companies, universities and a hospital's networks compromised; and
  - Computer users lured to malicious web sites by threat actors impersonating reputable Canadian bank and airline organizations.
- **International News:** Chinese military suspected of hacking US satellites; Japanese missions around the world experienced targeted cyber attacks; Finland wants to build offensive cyber capability.

PURPOSE

UNCLASSIFIED
DRAFT

The purpose of this Weekly Summary is to inform government and critical infrastructure management about notable cyber events encountered or reported to the Canadian Cyber Incident Response Centre (CCIRC), any notable international news and any CIRC information products issued during the week.

NOTABLE INCIDENTS– 22 THROUGH 28 OCTOBER 2011:

Government Systems.

Federal Government. CCIRC received a report of employees in a federal agency receiving e-mails, with the subject line referencing Mohammed Gaddafi and Allah. CCIRC forwarded information on this incident to the Cyber Threat Evaluation Centre (CTEC), the cyber incident handler for the federal government.

Analysis: CCIRC has no information to indicate whether this federal departmental was targeted specifically by these e-mails. However, referencing popular news items and events is a common tactic used to lure internet users into opening e-mails with malicious content.

Provincial Government. CCIRC received reports on potential compromises of computers on three provincial government systems.

Analysis: CCIRC has no information to indicate that these were targeted attacks on the provinces. Reports indicated that the computers in question were infected with malicious software commonly used by cyber criminals.

Police. CCIRC discovered that user account information for a number of Canadian police organizations was posted on a hacker website. CCIRC sent information to the RCMP for evaluation and notification of the affected police agencies.

Analysis: CCIRC has no information whether police computer networks were compromised as a result of this activity. A similar incident for a Canadian provincial police force and a number of American police organizations occurred earlier in 2011.

Canadian Critical Infrastructure:

Financial Sector.

Phishing. CCIRC received nine phishing reports and actioned the one that continued to pose a threat. In this incident, a threat actor, impersonating a well-known Canadian bank, was luring computer users via e-mail, to a website hosted in Australia. CCIRC notified the bank, Google phishing, the Anti-Phishing Working Group and Microsoft, so internet users may be alerted if they encounter these websites.

Threats by Anonymous. Anonymous, the famed hacker group, urged sympathizers to hack the Toronto and Montreal Stock Exchange (TMX) computer systems on November 7 and participate in a range of nuisance activities to coincide with Guy Fawkes Day on November 5. As of the date of this writing, CCIRC learned the operation to hack the TMX computers on November 7 has been cancelled.

Analysis: Anonymous is a loosely organized hacker group that has the capacity to organize and launch a Distributed Denial of Service (DDOS) attack that could potentially bring down a website.

When Anonymous called for a November 7 attack on the TMX computers, CCIRC contacted major Canadian financial institutions. They confirmed their awareness of the potential threat from Anonymous, and that their internet service providers were prepared to mitigate any DDOS attack. As of the date of this writing, the cyber attack on TMX has been called off.

On-line recruitment for money laundering. CCIRC learned of an on-line recruitment campaign in Canada for money laundering, originating from abroad. CCIRC sent summary and technical details sent to the RCMP Anti-fraud centre as well as the RCMP High-Tech Crime Branch for possible further investigation.

Telecommunications Sector.

Intrusion attempt – Internet Service Provider Core Infrastructure: A Canadian internet service provider informed CCIRC and other Canadian telecommunication companies about recent brute force hacking attempts against their routers, at the rate of 60-100 attempts each day. The reporting internet service provider has taken mitigation measures.

Analysis: Routers of an internet service provider are used to route internet traffic of its subscribers, and possibly other internet users. Having control of a router on the Canadian telecommunication network would enable a hacker to intercept Canadians' communications and information going through that router, and use that information for a variety of malicious purposes.

Energy Sector. CCIRC received infection reports on computers of three energy sector organizations. These organizations are: A large of oil & gas producer, a service & equipment provider to the oil and gas sector, and a provincial electricity producer. CCIRC notified all three organizations of the potential infections.

Health. CCIRC received a computer infection report for a Canadian hospital and notified the organization's IT department.

Transportation. CCIRC received a report of phishing attempts in the aviation sector. Threat actors were seeking on-line customer credentials for an airline.

CCIRC Product: CCIRC released Alert AL11-501 to IT professionals and managers in its stakeholder community. This Alert informs stakeholders about the work-around solution and update released by Entrust, created when it was discovered that a Java software updated interfered with the functionality of some Entrust products.

International News

Chinese military suspected of hacking US satellites. According to a publicized portion of the draft US-China Economic and Security Review Commission annual report, computer hackers, possibly from the Chinese military, interfered with two US government satellites four times in 2007 and 2008. There is currently no public information about the nature of the hackers' interference with these satellites, which are used for earth climate and terrain observations. The report, which is to be released next month, states the interferences occurred through a ground station in Norway.

Japanese missions around the world experienced targeted cyber attacks. Open sources report that at least dozens of computers used at Japanese missions in nine countries, including Canada, have been compromised since this past summer. Many of the compromises were found to allow a remote hacker to gain access and steal confidential information. The Japanese Foreign Ministry is investigating this incident and assessing its impact.

Finland wants cyber war weapons. Open sources report Finland has joined Sweden in planning to include counter-offensive capability for cyber attacks as part of its defence strategy. The new strategy would be presented to parliament and formalized in 2013.

FEEDBACK: This is a newly developed product. Your feedback is critical to making this product useful for you. Please fill out the attached form and e-mail it to Bud Cameron, CCIRC Strategic Program Manager, at bud.cameron@ps-sp.gc.ca.

NOTES

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 Flashed marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report**: Strategic, Information or Technical
- **Operational Summary:** Daily, Weekly, or GovIRT

s.16(2)(c)

Williston, Sandra

From: Moore, Bruce
Sent: November-02-11 12:04 PM
To: 'Alain.Labossiere@ic.gc.ca'
Subject: RE: [redacted] - "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

Yes - as N2

Bruce

-----Original Message-----
From: Alain.Labossiere@ic.gc.ca [mailto:Alain.Labossiere@ic.gc.ca]
Sent: November 2, 2011 12:03 PM
To: Moore, Bruce
Subject: RE: [redacted] "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

Thanks

Can we send that to CTCP?

Alain

-----Original Message-----
From: Moore, Bruce [mailto:Bruce.Moore@ps-sp.gc.ca]
Sent: Thursday, October 27, 2011 12:16 PM
To: Labossière, Alain: DGEPS-DGGPN
Subject: FW: [redacted] "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day / Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

FYI

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

[redacted] "Anonymous" calls for nuisance activities to coincide with Guy Fawkes Day

This document is UNCLASSIFIED and is the property of the Integrated Terrorism Assessment Centre (ITAC). Prepared by ITAC, it is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to those with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed via email to ITAC at [redacted] or to ITAC Partnerships at [redacted]

ITAC is a community resource of the Canadian government's Security and Intelligence Community. It is comprised of secondees from a wide range of federal agencies and produces integrated, comprehensive and timely threat assessments for all levels of government with security responsibilities and, as appropriate, critical infrastructure stakeholders in the private sector.

ITAC would like to express its gratitude to all agencies and departments of Canada's Security and Intelligence Community for the contributions they have made to this product, and invites those agencies and departments to provide feedback on the content of this threat assessment product.

Laser 11/234 - Le groupe « Anonymous » demande à ses sympathisants de se livrer à des activités malveillantes pour souligner le Jour de Guy Fawkes

Le présent document est coté NON CLASSIFIÉ et est la propriété du Centre intégré d'évaluation du terrorisme (CIET) et a été préparé par celui-ci. Il s'appuie sur des informations qui proviennent de diverses sources et qui sont valables à la date de publication. Il est fourni à votre organisme ou ministère à titre confidentiel et peut être communiqué directement par votre organisme ou ministère à d'autres personnes selon le principe du besoin de savoir. Il ne doit pas être réutilisé, de quelque manière que ce soit, en tout ou en partie, sans le consentement de l'expéditeur. Pour tout commentaire, veuillez envoyer un courriel au CIET, à [redacted] ou communiquer avec la Sous-section des partenariats du CIET, au [redacted]

Le CIET est un membre de l'appareil canadien de la sécurité et du renseignement, composé d'employés en détachement provenant de divers organismes fédéraux. Il produit à point nommé des évaluations intégrées et détaillées de la menace pour tous les ordres de gouvernement responsables de la sécurité ainsi que pour les intervenants du secteur privé responsables de l'infrastructure essentielle.

Le CIET tient à remercier tous les organismes et les ministères de l'appareil canadien de la sécurité et du renseignement de leur contribution au présent document, et les invite à formuler des commentaires sur son contenu.

Thanks / merci,

[redacted]

ITAC

[redacted]

Williston, Sandra

From: GOC-COG
Sent: November-01-11 10:20 AM
To: _GOC Distribution List / Liste de distribution du COG
Subject: Rapport quotidien du COG - 01 novembre 2011
Attachments: 2011-11-01 Rapport quotidien du COG.pdf

(English version previously sent)

SOMMAIRE

Il n'y a pas d'addenda classifié aujourd'hui.

INCIDENTS EN COURS

Rien d'important à signaler.

À VENIR

1. Les 3 et 4 novembre 2011 : Sommet du G20 à Cannes, en France : La France accueillera le 6e Sommet du G20 les 3 et 4 novembre 2011. Le très honorable Stephen Harper, premier ministre du Canada, sera à la tête de la délégation canadienne. Le CIET estime que la menace est FAIBLE pour la délégation canadienne qui assistera au Sommet du G20 en France.

2. Le 5 novembre 2011 : appel du groupe « Anonymous » à commettre des actes de nuisance à l'occasion de la Journée Guy Fawkes : Le groupe international de cyber-pirates « Anonymous » a diffusé en ligne un message incitant ses sympathisants à participer à diverses activités de nuisance ciblant des sites Web du gouvernement et des médias le 5 novembre, pour commémorer la Journée Guy Fawkes. L'initiative, baptisée « Operation Injustice Awareness », incite les sympathisants du groupe à défigurer des sites Web et à rediriger les visiteurs de ces sites vers des messages qu'il a diffusés sur Twitter, selon sa façon de faire habituelle. Le groupe incite également ses sympathisants à descendre dans la rue, à porter des masques à l'effigie de Guy Fawkes et à défigurer leur ville en y faisant des graffitis, à affronter quiconque les interpelle et à capter des images de leurs actes pour ensuite les télécharger sur les médias sociaux. L'ACTI ignore si l'opération annoncée visera des systèmes informatiques ou des installations physiques du gouvernement du Canada ou des médias canadiens.

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

s.16(2)(c)