CCIRC
Canadian Cyber Incident Response Centre

BUILDING A **SAFE** AND **RESILIENT CANADA**

CCIRC CYBER OPERATIONAL SUMMARY

REPORTING PERIOD: FEBRUARY 16, 2014 – MARCH 1, 2014
CCIRC CYBER AWARENESS PRODUCT: 14-S-006

PURPOSE

This report is intended to provide cyber information to owners and operators of Canada's critical infrastructure in order to support operational and security decision-making in these organizations. It is based on information reported to and researched by the Canadian Cyber Incident Response Centre (CCIRC), and may not be indicative of the cyber environment in Canada. Additional reporting by partners would help CCIRC contribute to a more accurate Canadian picture.

Highlights

- Canadian energy and utilities sector targeted in watering hole attacks

- Canadian Internet protocol addresses used in distributed denial of service attacks

In the news:

- Credential breach affects more than one million subscribers of an online publication

- Fake Secure Socket Layer (SSL) certificates could be used for man-in-the-middle attacks

OVERVIEW

During this reporting period, CCIRC handled 58 incidents, including:

- Malware targeting Canadian financial institutions;
- Spread of ransomware continues;
- Analysis of 67 malware samples provided by partners in the financial sector and federal government, including phishing emails containing malicious attachments; and
- 3,601 victim notifications were sent to public and private sector partners infected with various malware, including ZeroAccess, Citadel, Conficker and Zeus.

PRODUCTS RELEASED

CCIRC regularly issues information products to notify its public and private sector partners of potential, imminent or actual cyber threats. During the reporting period, CCIRC issued seven cyber awareness products.

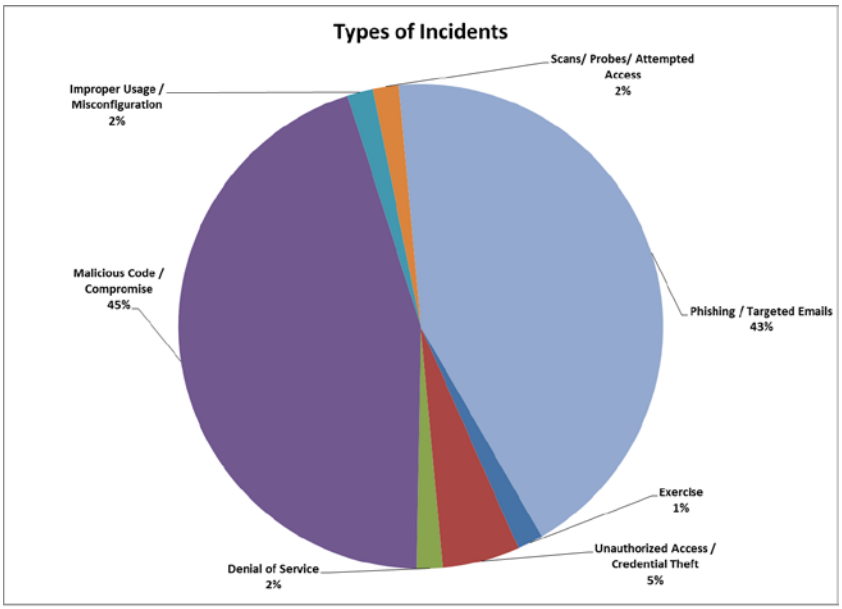
CCIRC issued Cyber Flash CF14-005 to inform stakeholders about spear phishing activity targeting Canadian critical infrastructure organizations. CCIRC released two Advisories to draw attention to security updates for Adobe Flash Player (AV14-011) and multiple vulnerabilities in Cisco intrusion prevention system software (AV14-012). CCIRC also released an Alert AL14-003 to bring attention to a use-after-free vulnerability in Microsoft Internet Explorer versions 9 and 10 and AL14-504

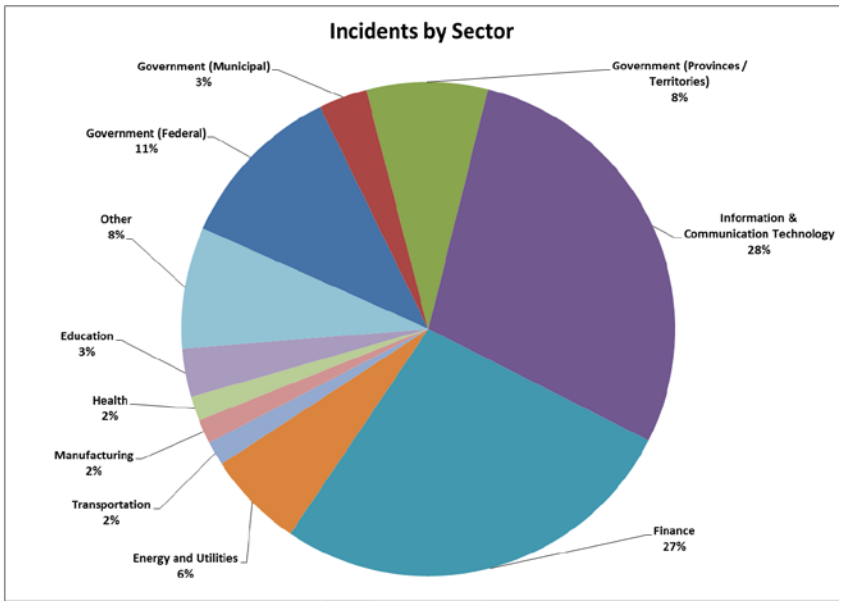
along with two subsequent updates to bring attention to a Canadian energy and utilties company website used in a watering hole attack and share indicators of compromise (IOC).

NEW INCIDENTS

PRIVATE SECTOR

Targeted attacks against Canadian energy sector – CCIRC became aware of targeted attacks against organizations in the Canadian energy and utilities sector using watering hole techniques. CCIRC was first alerted to this incident by a trusted financial sector partner when their intrusion detection system (IDS) alert was triggered on an energy and utilties sector organization's website which was found to be hosting a malicious iframe. Upon further analysis, CCIRC was able to determine that users were being redirected to a compromised website that was serving the Lightsout Exploit kit and Havex remote access Trojan (RAT). CCIRC notified the website owner that was hosting the malicious iframe and released Alert AL14-504 with IOCs to inform the broader critical infrastructure community.





In the days following this incident, a trusted security researcher reported to CCIRC that three energy and utilities sector organizations and one municipality may have been compromised through the same watering hole attack. CCIRC notified the affected organizations and provided mitigation advice. Two of these organizations had confirmed infections and removed the devices from their networks.

CCIRC obtained additional IOC's and released alert AL14-504, as well as two updates. As a result, a large energy and utilities sector organization reported to CCIRC that they were seeing beaconing to three of the command and control domains identified in the Alert. CCIRC provided mitigation advice to the organization.

Comment: An iframe, or inline frame, is a way to load one web page inside another, usually from a different server. Attackers can insert iframe code into the saved search results of legitimate websites and when a visitor clicks on a link, they are redirected to a malicious

website. The unsuspecting user's computer would then be at risk from the automatic download of malware.

In watering hole attacks, the attacker poisons a legitimate website likely to be visited by employees from an organization. In many cases, a redirect is injected into the legitimate website (the watering hole) which will redirect victim browsers when they visit the site. The malicious redirect will often install a backdoor or other malware on a victim machine. The attacks mentioned exploited the following vulnerabilities in Microsoft, Java, and Mozilla products: CVE-2013-1347, CVE-2013-2471, CVE-2013-2465, CVE-2013-1690, and CVE-2012-1723.

Exploit kits use application or system vulnerabilities to install malware and allow malicious entities to gain access to infected computing machines. RATs can be used to carry out a variety of malicious activities including monitoring user behaviour, stealing personal information, installing or distributing other malware, attacking other computers, and deleting, downloading, or altering files and file systems. For more information, including mitigation strategies, please see CCIRC's TR11-002 Mitigation Guidelines for Advanced Persistent Threats.

Distributed denial of service (DDoS) attacks launched from Canadian Internet protocol (IP) addresses – CCIRC continues to observe incidents of Canadian IP addresses being used to perpetrate DDoS activity. In this incident, the DDoS attacks were believed to be associated with Brobot malware and exploited a vulnerability in an out-of date Joomla! BlueStork content management system (CMS) for the majority of reported infections; however, other infections exploited vulnerabilities in other types of CMS. CCIRC notified the IP hosts, provided mitigation advice and requested the removal of the malware in order to prevent further DDoS attacks.

Comment: Brobot is a hypertext preprocessor (PHP) script dropped on websites having web application vulnerabilities. This tool is known to have a variety of DDoS functionalities and maintains persistence on the infected servers.

DDoS attacks occur when multiple systems simultaneously flood networked computer resources, potentially rendering them inaccessible. The use of compromised CMS is a common attack vector due to the number of exploitable vulnerabilities associated with this software and the increased networking and computing capacity of web servers running CMS. CCIRC issued IN13-001 Content Management Systems Security and Associated Risks and Alert AL14-501 to raise awareness of vulnerabilities in CMS and web hosting control panels that can be exploited to carry out DDoS attacks. For more information on DDoS including tips to defend against DDoS attacks, please see CCIRC's TR12-001: Mitigation Guidelines for Denial of Service Attacks.

Ransomware – A Canadian organization reported to CCIRC that one of their computers was infected with Howdecrypt ransomware, also known as CryptorBit. While the infection method and number of files encrypted is not known, the organization was able to restore the majority of their files from backups. CCIRC provided additional mitigation advice to the affected organization.

Comment: Howdecrypt (or CryptorBit) is a ransomware program that was first seen in December 2013. Howdecrypt targets all versions of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8. When infected, this ransomware will scan a computer and encrypt any file it finds regardless of the file type or extension. It will then demand a ransom

payable in bitcoin. While no dropper for this infection has been actively seen in the wild, some reports indicate that files became corrupted after installing a fake Adobe Flash update or after being infected by a fake anti-virus program.

CCIRC suggests that organizations have backups in place and that in a situation like this you do not pay the ransom, contact your local law enforcement and also report this event to the Canadian Anti-Fraud Centre. For more information on ransomware, please see CCIRC's IN13-004 Ransomware.

Credential leaks – CCIRC received a report from a trusted partner regarding email addresses and password hashes belonging to users at two Canadian universities being posted to a website. CCIRC notified the affected organizations and provided mitigation advice.

Comment: Credential theft may be leveraged to carry out a variety of malicious campaigns. CCIRC recommends that affected individuals change the passwords of all affected and non-affected accounts. Victims of credential theft should be aware that they are at risk of further attacks and should contact their respective IT security teams if they believe they are being targeted.

Virus targeting Canadian financial institutions - CCIRC received a report from a trusted partner that identified two Canadian banks that have been infected with the Win32/Expiro virus. CCIRC notified the affected organizations and provided mitigation advice.

Comment: The Win32/Expiro virus is able to connect to a server to receive commands remotely from a malicious actor. It steals sensitive information, allows backdoor access and control, lowers Internet Explorer security, and sends information about your computer every time it connects to the server.

Best Practices

Canada Revenue Agency Phishing Schemes

CCIRC continues to observe incidents of Canada Revenue Agency (CRA) phishing emails. There tends to be an increase in reported instances of CRA phishing emails during tax season. CCIRC reminds Canadians to be cautious and that these phishing emails are fraudulent and do not represent the CRA. Anyone receiving such emails should not respond or comply with any instructions, click on any links, or provide any personal information. These phishing scams can result in identity theft or the infection of your computer with malware. The CRA does not email Canadians to request personal information of any kind. Reminder:

- The CRA does not request information pertaining to a passport, health card, or driver's license.
- The CRA does not divulge taxpayer information to another party unless formally authorized to do so by the taxpayer.
- The CRA does not leave any personal information on answering machines or voice mail.

Anyone receiving suspicious emails should contact the Canadian Anti-Fraud Centre.

PUBLIC SECTOR

Compromised provincial government email accounts – CCIRC received a report from a trusted source indicating that two provincial government email accounts have sent more than 400 spam messages over the course of a week. The spam messages asked recipients to make a donation to a

charitable institution and contained an email address to do so. CCIRC notified the affected organization and provided mitigation advice.

VICTIM NOTIFICATIONS, PHISHING AND MALWARE ANALYSIS

Victim notifications – CCIRC sent 3,601 notifications to partners in public and private sector organizations whose computers were potentially infected with malware. ZeroAccess, Citadel, Downadup, also known as Conficker, and Zeus were the most prevalent observed malware types. These notifications accounted for 827,954 infected IP addresses and contained detection indicators and mitigation advice. The majority of notifications were sent to partners in the information and communications technology (ICT) sector, to organizations in the energy and utilities sector, to education institutions and to provincial and territorial government organizations.

> *Comment: The relatively high number of notifications sent to the ICT sector is largely due to the fact that most critical infrastructure operators rely upon the services of an ICT organization, and is not solely indicative of the state of security within the ICT sector itself. Partners who would like more information on CCIRC's automated National Cyber Threat Notification System are encouraged to email cyber-incident@ps-sp.gc.ca.*

Phishing attempts – Partners reported to CCIRC that malicious actors had impersonated a number of organizations, including federal government agencies and major Canadian and international banks in order to solicit personal and financial information from users. In all instances of observed phishing attempts, CCIRC notified the impersonated institutions and the affected organizations' phishing intake filters.

Malware samples submitted to CCIRC – A number of CCIRC's partners submitted malware samples for analysis. CCIRC analyzes the samples it receives, and shares the results of this analysis with those who submitted them. During the reporting period, 67 malware samples were submitted, including phishing emails with malicious attachments. Most of these emails were impersonating federal government agencies, Canadian banks, and telecommunications organizations. Partners are encouraged to submit suspicious or seemingly malicious emails and files to CCIRC at: malware@ccirc-ccric.gc.ca using the password "infected". Indicators derived from the samples provided are shared with partners through CCIRC's Weekly Technical Report.

NOTEWORTHY ITEMS IN THE NEWS

Syrian Electronic Army Leaks Details of over 1 Million Forbes Readers – Forbes confirmed that its publishing platform was breached by the Syrian Electronic Army (SEA) allowing the attackers to gain access to the company's readers' credentials, WordPress administration console, and some Twitter accounts. Forbes stated that user passwords are encrypted, but advised their subscribers to change their passwords as a precaution. Forbes also warned readers to be wary of any emails sent from Forbes, saying the possibility is high that they could receive phishing emails from the SEA spoofing Forbes. The SEA claimed that they attacked Forbes because of the publication's reports about the hacker group and Syria.

Fake SSL certificates deployed across the internet – A security firm has found fake Secure Socket Layer (SSL) certificates impersonating financial institutions, e-commerce sites, Internet service providers and social media sites. Some of these certificates can be used to carry out man-in-the-middle attacks, allowing the attackers to decrypt legitimate online banking traffic and re-encrypt it

before forwarding it to the banks. The fake certificates have similar names as the hostnames of their targets, but are not signed by trusted certificate authorities.

The simple way to stop serious Microsoft software flaws? Take away 'admin' rights – An international privilege management software company reported that 90% of risk posed by critical vulnerabilities in Microsoft products in 2013 could have been removed if users ran Windows with 'standard' instead of 'administrator' rights.. The company also reported that 96% of critical flaws in 2013 were mitigated by removing administrator rights on all versions of Windows, 100% for Internet Explorer, 91% for Office, and 96% in Windows Server products. More than 50% of the vulnerabilities involved Remote Code Execution.

Erasing SSDs: Security is an issue – A paper published by an American university states that sanitizing or removing data from hard drives is a fairly well understood process; however, solid state disks (SSDs) have a different internal architecture, so it is not clear if hard drive sanitization techniques will work for SSDs. Hard drives use magnetic storage platters, so digital sanitization techniques, such as overwriting, are sufficient. SSDs use flash memory technology making overwriting not possible.

UPS Malware Spam Using Fake SPF Headers – A security research and education organization reports fake Sender Policy Framework (SPF) headers are being used by spammers to bypass spam filters. SPF is a system that identifies which mail servers are allowed to send emails from a domain. Poorly configured mail gateways and spam filters can be fooled by adding a header that the e-mail passed the SPF validation. These emails can contain malicious attachments.

PUBLISHED INTERNET THREAT REPORTS

FireEye: Advanced Threat Report 2013 – FireEye reports that the top three countries most frequently targeted by advanced persistent threats (APT), which FireEye defines as attackers associated with a nation-state, were the United States, South Korea, and Canada. FireEye observed the widespread use of Internet Explorer (IE) "zero day" watering holes, and that Java exploits were the most widely used by hackers in the first half of 2013.

> *Comment: In 2013, CCIRC observed the widespread use of IE "zero day" watering holes by sophisticated attackers, as highlighted in Cyber Flash* CF13-007 Internet Explorer 8 Zero-day Vulnerability Used in Watering Hole Type Attacks (CVE-2013-1347). *CCIRC also observed the widespread exploitation of Java, as detailed in its* Spotlight On… Java, *which is available to partners via CCIRC's Community Portal. For more information on APT, please see CCIRC's TR12-001: Mitigation Guidelines for Denial of Service Attacks.*

Secunia Vulnerability Review 2014 – In 2013, three quarters of the software vulnerabilities analyzed by Secunia affected third-party programs, which highlights how resource-intensive it can be to patch promptly. According to Secunia, 86.1% of all vulnerabilities discovered in 2013 had a patch available on the day of disclosure.

> *Comment: This report underscores that timely patching of software vulnerabilities and operating systems are essential mitigation strategies, and as such are two of the Top 4 Strategies to Mitigate Targeted Cyber Intrusions.*

SANS: Healthcare Report 2014 – Based on the *2014 SANS Securing the Internet of Things Survey*, this report points out that medical devices are increasingly being networked and connected to the Internet, thereby exposing these devices to a higher level of cyber risk. A compromised medical device, such as an MRI machine, has the potential to adversely impact patients' health, among other costs.

Trend Micro - Point-of-Sale System Breaches – Point of Sales (PoS) systems are difficult to secure due to their role and location in a network. Small businesses tend to use a simple form of cellular data connection, but large businesses may want more functionality out of their system which requires internal server connections which in most cases are management remotely. Most PoS systems used an embedded version of Microsoft Windows, and attackers can gain access, bypass and defeat any running security solutions present. Hackers can attack PoS systems directly, network communications or target specific servers.

FEEDBACK

Your feedback is appreciated and critical to making this product useful for you. Please email any feedback you have to the Operational Analysis and Support Section at CCIRC-CCRIC@ps-sp.gc.ca.

MANDATE

In support of Public Safety Canada'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 security incident response team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber events. It does this by providing authoritative advice and support, and coordinating information sharing and event response.

REPORTING CYBER INCIDENTS

Canadian critical infrastructure operators who wish to report cyber incidents may send associated email reports to cyber-incident@ps-sp.gc.ca, using the CCIRC Cyber Duty Officer PGP encryption key.