SciencePages

MARCH 2013

Cyber Security

Cyber security is the attempt to protect computers and networks from unauthorized access. Protecting such systems is essential for the security of public, private and online commerce, critical infrastructure and safeguarding personal information.

Canadians depend on computer networks now more than ever. But a connected society brings increasing vulnerabilities to cyber crime and espionage, so-called cyber attacks.

Cyber crime -- including identity theft, online fraud and emails scams -- directly affects the lives of Canadians. A survey estimated that from July 2011 to July 2012, 8.3 million Canadians adults were the victims of cyber crime[1], and even our government “is witnessing serious attempts to penetrate its network on a daily basis.[2]”

A 2012 global study ranked Canada third in the world for victims of cyber crime and 10th for hosting malicious websites (approx. 750,000). By contrast, the United States ranked first in both categories[3].

Cyber threats are evolving rapidly. Cyber attacks are usually perpetrated by “hackers”’ whose intent can be espionage, crime (data theft, e.g.) or activism (“hacktivism”)[4]. While Canadian research is advancing on several fronts, the government must try to keep pace with the barrage of cyber attacks[5]. In February, 2013, Richard B. Fadden, Director of CSIS, told the Senate Committee on National Security and Defence that if this growth in attacks continues, Canada may not be able to manage the cyber threat within two years[6].

[1] 2012 Norton Cybercrime Report. - http://www.newswire.ca/en/story/1030295/2012-norton-study-consumer-cybercrime-costs-canadians-c-1-4-billion; http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norto_Cybercrime_Report_Master_FINAL_050912.pdf

[2] Canadian Security Intelligence Service, 2010–2011 Public Report, Message from the Director. http://www.csis-scrs.gc.ca/pblctns/nnlrprt/2010-2011/rprt2010-2011-eng_final.asp

[3] Websense 2013 Threat Report. (p. 10, p. 11 [in infographic])http://www.websense.com/assets/reports/websense-2013-threat-report.pdf

[4] CSIS commissioned study by Angela Gendron and Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure http://www.csis-scrs.gc.ca/pblctns/cdmctrch/CyberTrheats_AO_Booklet_ENG.pdf [sic]

[5] 2012 Fall Report of the Auditor General of Canada, Chapter 3—Protecting Canadian Critical Infrastructure Against Cyber Threats. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html

[6] Testimony before the Standing Senate Committee on National Security and Defense. Ottawa, Monday, February 11, 2013.

Source:: Photos.com

klossner
"I DON'T THINK YOU UNDERSTAND THE CONCEPT of CYBERSECURITY."

Source:: Lumension

CYBER ATTACK - ECONOMIC IMPLICATIONS

The economic costs of cyber crime are difficult to gauge, in part because firms don’t want to reveal cyber security breaches and the resulting financial loss[7]. Costs can include the loss of intellectual property and damage to reputation[8]. Scientific data from objective third parties or data describing the extent of the damage is lacking, and better data on these issues is needed for further research that can ultimately inform policy. Some numbers that have been put forward:

- According to figures from anti-virus software Norton, from June 2011-2012, cyber crime had a net cost of $1.4 billion in Canada[9].
- A 2011 survey of IT security professionals in Canada found that the average annual cost of security breaches to government, public, and private enterprise was $83,000, a significant drop compared to previous years, and the average annual number of breaches was 7-8[10].
- A 2008 paper from McMaster University researchers estimated that in the previous year, identity theft cost Canadian consumers over $150 million[11].

[7] Ponemon Institute, Second Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies. http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf; CRS Report for Congress, The Economic Impact of Cyber-Attacks.http://www.cisco.com/warp public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

[8] Benjamin J. Brooker, et al., A Framework for the Evaluation of State Breach Reporting Laws, Risk Analysis. http://www.sys.virginia.edu/sieds07/papers/SIEDS07_0066_FI.pdf

[9] See fn 2. See Public Safety statement fn 1, which estimates the cost of identity theft at $1.9 billion. A few people have questioned the $1.4 billion figure, but it seems to be consistent with the government source

[10] Telus & Rotman School of Management, 2011 Executive Summary, Joint Study on Canadian IT Security Practices.http://business.telus.com/en_CA/content/pdf/whyTELUS/Security_Thought_Leadership/TELUS_Rotman_2011_Results.pdf

[11] http://merc.mcmaster.ca/working-papers/23.html

EMERGING THREAT: CYBER-ATTACKS ON MOBILE DEVICES

Today there are roughly 10 billion connected devices, or more than one for every person on the planet. Cisco’s IBSG report forecasts this number to increase to over 40 billion by the year 2020[1].

More than 11 million Canadians own smartphones and their top internet activity is using mobile apps. In 2012, German researchers reviewed 13,500 apps on the Android platform and found that eight per cent of them were vulnerable to cyber attacks that could compromise personal information. The researchers were able to capture user data from American Express, PayPal, Facebook and Google, among others.

Last year, 16 per cent of Canadian adults were victims of cyber-attacks through social media and mobile devices. 76 per cent of mobile technology users had no security software for their devices[2].

[1] http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] Sascha Fahl et al., Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security, Journal of Computer and Communications Security. http://www2.dcsec.uni-hannover.de/files/android/p50-fahl.pdf, 2012 Norton Cybercrime Report. http://www.newswire.ca/en/story/1030295/2012-norton-study-consumer-cybercrime-costs-canadians-c-1-4-billion; http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

NATIONAL SECURITY

Public Safety Minister Vic Toews has acknowledged that hackers could “disrupt the electronic controls of our power grids, water treatment plants and telecommunications networks,” physically crippling services vital to public safety and national security[1]. In 2009, the Stuxnet worm, a type of malware, infiltrated and severely damaged centrifuges at a nuclear power facility in Iran by increasing the operating speed past safe limits, causing the centrifuges to fly apart[2].

In a recent report, the security firm Mandiant attributed attacks on the Canadian branch of the industrial control systems designer Telvent to a group of Chinese hackers. Telvent develops software for controlling power grids, oil pipelines and other industrial systems across the continent. Hackers infiltrated Telvent in 2012 and stole company data related to the operation of those systems[3].

Canada has also suffered breaches of government systems, with lasting effects. In early 2011, user accounts of Treasury Board, Defense Research and Development Canada and Finance Department employees were compromised, forcing them to block staff internet access to control the data breach. It took nearly eight months for full internet service to be restored[4]. If these attacks become more common, as many predict, national security will increasingly depend on strong cyber defense.

ARAMCO VS. SHAMOON: THE COST OF A DESTRUCTIVE CYBER-ATTACK

In late 2012, hackers attacked the state-owned Saudi Arabian oil company Aramco. Saudi Arabia is the world’s largest oil producer and Aramco controls the country’s petroleum infrastructure.

A group named “The Cutting Sword of Justice” claimed responsibility for the attack, which severely damaged 30,000 computers. News reports said the hackers used malicious software (malware) called Shamoon, which rendered the computers unusable and forced the company to replace the hard drives of the affected machines[1].

Aramco said it disconnected the compromised computers from the network before its oil infrastructure was affected[2].

[1] Jim Finkle, Exclusive: Insiders suspected in Saudi cyber attack, Reuters, Sept. 7, 2012. http://www.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idUSBRE8860CR20120907

[2] Saudi Aramco, Saudi Aramco restores network services, Press Release. http://www.saudiaramco.com/content/mobile/en/home/news/latest-news/2012/saudi-aramco-restores-network.html Nicole Perlroth, In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, New York Times, October 23, 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Source: ImagesCARWTY8

MEANS USED TO COMPROMISE COMPUTER SYSTEMS

SOCIAL ENGINEERING, SPEAR PHISHING AND GHOSTNET

In 2008 and 2009, the Canadian research team Citizen Lab, Munk Centre for International Studies, University of Toronto, investigated a “cyber espionage network” it called GhostNet, which targeted Tibetan officials. The attackers manipulated individuals into revealing personal information.

The specific method was “spear phishing”’ Unlike regular phishing, which indiscriminately tries to trick users into giving up private information, “spear phishing”’crafts targeted attacks against specific people. In 2008, the perpetrators of GhostNet sent an email to campaigns@free-tibet.org with an attachment titled “Translation of Freedom Movement ID Book for Tibetans in Exile.doc”. The Word document, which appeared genuine, was infected with malware that hid on the victim’s computer when the document was opened. The malware connected to GhostNet where the computer hijackers, among other tasks, could activate webcams, view screenshots of the monitors, and access confidential information stored on the infected computers.

In its report, Citizen Lab estimated that nearly 1,300 computers, many believed to belong to diplomats and embassies around the world, were compromised by GhostNet. Investigators identified the infection by closely monitoring network traffic on the computers of the Office of the Dalai Lama[1].

[1] Ronald Deibert, et al., Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor, March 29, 2009. http://www.scribd.com/document_downloads/direct/1373

ATTACKS VIA WEB BROWSERS

Attacks through web browsers are often executed using malicious JavaScript code implanted in a web page. JavaScript is a programming language commonly used by popular news sites, online stores, educational institutions and government websites, for example.

Hackers use JavaScript to exploit vulnerabilities in web browsers and browser extensions, known as plugins. Upon visiting a compromised website, the malicious code infects the user, then downloads and installs malware on the victim’s computer. These attacks are known as “drive-by-downloads“[5].

ATTACKS VIA SOFTWARE VULNERABILITIES

Exploiting design flaws in software -- sometimes called “sloppy code” -- is another common way of gaining unauthorized access to a computer.

Hackers can take advantage of these loopholes and create programs to abuse them. They then often publish their findings online, which amplifies the problem. Once attackers access a system, they can install malware and use the infected computer for nefarious activities. Often vulnerabilities appear “in the wild” before the manufacturer has produced a patch to address them. These are called “zero day vulnerabilities” .

[1] 2012 Norton Cybercrime Report.http://www.newswire.ca/en/story/1030295/2012-norton-study-consumer-cybercrime-costs-canadians-c-1-4-billion; http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[2] Thomas M. Chen, Saeed Abu-Nimeh, Lessons from Stuxnet, IEEE Computer Society, April 2011

[3] Mandiant, APT1 Exposing One of China’s Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[4] 2012 Fall Report of the Auditor General of Canada, Chapter 3—Protecting Canadian Critical Infrastructure Against Cyber Threats. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html; Stephanie Levitz and Jim Bronskill, Hackers had head start breaking into Ottawa computers, documents show, The Globe and Mail/Canadian Press, Monday, Sep. 26 2011. http://www.theglobeandmail.com/news/politics/hackers-had-head-start-breaking-into-ottawa-computers-documents-show/article4256843/

[5] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu. The ghost in the browser: Analysis of web-based malware. In Proceedings of USENIX Workshop on Hot Topics in Understanding Botnets (HotBots), April, 2007.

WHY SHOULD WE BE CONCERNED ABOUT MALWARE AND BOTNETS?

Malware: malicious programs created to attack computers, steal sensitive information or disrupt systems. They can be Trojan horses, spyware, worms or viruses.

A malware infection is often the first step in building a botnet– a network of infected computers that can act in concert and are controlled by "botmasters". Once connected to a botnet, a botmaster can remotely instruct each compromised system, or bot, to perform various tasks. These may include stealing private information from the computer, sending out spam email or making the compromised computer part of large "distributed denial of service" (DDoS) attacks coordinated with other bots[1]. DDoS is a common tactic for overloading and crashing internet systems, and was used to attack the Estonian government and communication systems in 2007[2].

Cyber attackers design malware not only to use victims' computers for criminal activity, but to avoid detection. Hackers hide malware in system files and hardware that computers need to function, making infections difficult to detect and also sometimes impossible to remedy. In extreme cases, the only effective means of removing the malware is by replacing the entire computer[3].

[1] C. Wüest. Current advances in banking trojans. In Proceedings of 22nd Virus Bulletin International Conference September 2012.
[2] Joshua Davis, Hackers Take Down the Most Wired Country in Europe, Wired Magazine, August 21, 2007 http://www.buec.udel.edu/wraggej/MISY850-09S/Estonia.pdf
[3] Interview with José Fernandez, Assistant Professor, Department of Computer Engineering, February 14, 2013.

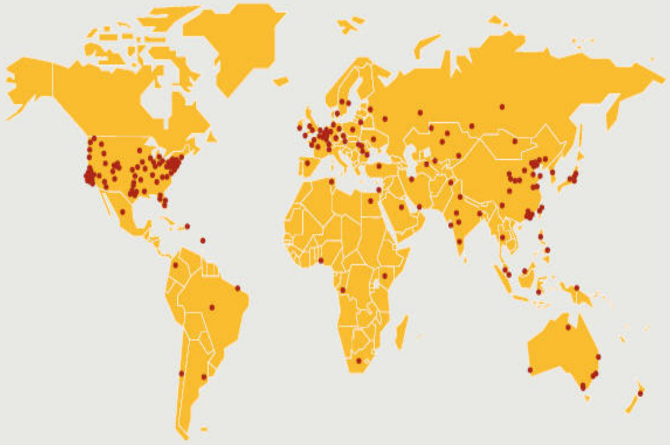
Source: CIO.com

Where Attacks Come From

Figure 5 represents the geographical distribution of attacking machines' IP addresses for all targeted attacks in 2011. It doesn't necessarily represent the location of the perpetrators.

Figure 5

Geographical Locations Of Attackers' IP Addresses



Source: Symantec

TECHNOLOGIES FOR MITIGATING CYBER-ATTACKS

Anti-virus software and network monitoring schemes can help mitigate cyber threats. However, once a defence is in place, hackers design attacks to circumvent that protection. The cat-and-mouse nature of cyber-conflicts means that methods and technologies must constantly adapt to evolving attacks[1].

CASE STUDY: BOTNET MITIGATION AND TAKING DOWN WALEDAC

Waledac was a prominent botnet which first appeared in November 2008 as a source of spam and malware.

A team of researchers at École Polytechnique de Montréal helped to discover the structure and operation of Waledac, identifying weaknesses that could help disable it. The researchers developed mitigation schemes against Waledac and re-created a live Waledac botnet on an isolated group of computers located in their laboratory. They used the re-constituted botnet to show that Waledac was vulnerable to their mitigation scheme. Microsoft used the research to disable Waledac in 2010. Unfortunately, Waledac appears to have recently resurfaced in a new form and is again being used for cyber crime[1].

[1] IJoan Calvet, et al., The case for in-the-lab botnet experimentation: creating and taking down a 3000-node botnet, Proceedings of Annual Computer Security Applications Conference (ACSAC 2010), December 2010. Fahmida Y. Rashid, Waledac Botnet Reappears as New Password Stealing Variant, eWeek, February 15, 2012. http://www.eweek.com/c/a/Security/Waledac-Botnet-Reappears-as-New-Password-Stealing-Variant-882729/

[1] Interview with José Fernandez, Assistant Professor, Department of Computer Engineering, February 14, 2013.

SciencePages

POLICY TO ENSURE CYBER SECURITY

The following laws can help protect personal information in the case of cyber attacks or theft of equipment and loss of mobile media[1].Protection against cyber-attacks will require a combination of citizen education, technological development and regulation that establishes security protocols for industry and government. Canada is a signatory to The Council of Europe's Convention on Cybercrime, or the Budapest Convention. It provides a framework for legislation to investigate and prosecute cyber criminals, including requirements that countries establish "24/7 Network[s]" operating at all times so any other party can contact them to share information about cyber crimes[2].

To address systemic problems both the European Union (EU) and the United States, in February 2013, released strategies to improve cyber security. The EU recommended forcing the private sector to share information about cyber attacks with government agencies, while the US addressed the same problem in an executive order to encourage critical infrastructure owners to participate in the development of best practices for cyber security[3]. Both emphasized that sharing information was important to understanding cyber threats. Countries like Finland, Israel and Sweden, who have been praised for their cyber security, all have close collaboration between government, military, academia and the private sector[4].

[1] Ross Fraser, comments on document.
[2] Convention on Cybercrime CETS No.: 185, Signatorieshttp://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG Convention on Cybercrime, Budapest, November 21, 2001 (Art. 35) http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[3] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, February 7, 2013. http://op.bna.com/pl.nsf/id/dapn-94pmql/$File/eucyber1.pdf Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, February 7, 2013.http://op.bna.com/pl.nsf/id/dapn-94pmqy/$File/eucyber2.pdf White House, The Office of the Press Secretary, Executive Order Improving Critical Infrastructure Cybersecurity, February 12, 2013.http://www.ft.com/intl/cms/370fb006-7586-11e2-a9f3-00144feabdc0.pdf

[4] Brigid Grauman, Cyber-security: The vexed question of global rules, Security & Defence Agenda, February, 2012. http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.

CYBER SECURITY LEGISLATION AND PRIVACY

Some legislative efforts to address cyber security and cyber crime have emerged recently in Canada, but have come under strong criticism. Bill C-30 failed in February after public outcry over granting authorities the power to access internet subscriber information and monitor online communications without a warrant. It has since been replaced by Bill C-55, which would grant similar powers in situations deemed emergencies[1]. The federal government is currently reviewing the regulations applicable to the *2010 Canadian Anti-Spam Legislation.* The law will in part govern the ability of third parties to install software on a person's computer without consent[2].

Canada's Privacy Commissioner Jennifer Stoddart has criticized Bill C-12, a law concerning the responsibilities of private firms when customer data breaches occur, for not going far enough to protect the data of individuals. She said the current state of private data legislation is "unacceptable[3]." Notably, Canada has no law requiring that personal information be encrypted when stored on mobile devices or transmitted through open networks, unlike Massachusetts, for example.

[1] Michael Geist, Lawful Access is Dead (For Now): Government Kills Bill C-30, michaelgeist.ca, February 12, 2013. http://www.michaelgeist.ca/content/view/6782/125/
[2] Canada's Anti-Spam Legislation, Fast Facts, http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html
[3] Jennifer Stoddart, Testimony before Information & Ethics Committee, Ottawa, December 11th, 2012 http://openparliament.ca/committees/ethics/41-1/59/jennifer-stoddart-34/

Public Safety Canada has made similar proposals for sharing information between government and private sector and developing standards for cyber security but many have not yet been fully implemented, according to the Auditor General[1].

Cyber security policy is in its infancy and requires a nuanced approach. For example, industrial systems face very different challenges than commercial or government networks, though public safety can be jeopardized by damage to either. Dialogue between all sectors will help identify and respond to the problem[2].

Experts stress that these initiatives are necessary to respond to national -- and sometimes global -- threats, but common criticisms are that these policies lack concrete direction and that without expanding international collaboration, cyber criminals will operate outside the bounds of these agreements[3].

At the individual level, both researchers and government underscore the importance of education. In September 2012, the federal government launched Cyber Security Awareness Month[4] with an accompanying website[5] offering helpful advice for groups at high risk, including seniors, students and children. Practical information helps all Internet users safeguard not only themselves, but strengthens cyber security for everyone by protecting the larger networks to which they connect.

FURTHER RESOURCES:

- Ron Deibert, Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace, Canadian Defence & Foreign Affairs Institute, August 2012. https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pd
- Canada's Cyber Security Strategy: http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx
- Assessing Cyber Threats to Canadian Infrastructure, report prepared for CSIS, Angela Gendron and Martin Rudner, March 2012, http://www.csis-scrs.gc.ca/pblctns/cdmctrch/CyberTrheats_AO_Booklet_ENG.pdf

[1] Testimony before the Standing Senate Committee on National Security and Defense. Ottawa, Monday, February 11, 2013
[2] Interview with Eric Byres, CTO and VP Engineering, Tofino Security, February 14, 2013
[3] Marc Hall, Storm cloud emerges from EU cybersecurity strategy, EurActv.com, February 8, 2013 http://www.euractiv.com/infosociety/stormcloud-emerges-cloud-safety-news-517658
Lisa Vaas, Infosec pros give verdict on EU's new cybersecurity strategy: "Nice try", NakedSecurity, February 8, 2013 http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/
Chengxi Wang, Obama's Cybersecurity Executive Order: Heart In The Right Place But There Is Little Teeth, Forbes.Com, February 14, 2013. Lisa Vaas, Infosec pros give verdict on EU's new cybersecurity strategy: "Nice try", NakedSecurity, February 8, 2013 http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/
Chengxi Wang, Obama's Cybersecurity Executive Order: Heart In The Right Place But There Is Little Teeth, Forbes.Com, February 14, 2013. http://www.forbes.com/sites/forrester/2013/02/14/obamas-cybersecurity-executive-order-heart-in-the-right-place-but-there-is-little-teeth/
Gerry Smith, Obama's Cybersecurity Order Weaker Than Previous Proposals, HuffingtonPost.com, February 12, 2013. http://www.huffingtonpost.com/2013/02/12/obama-cybersecurity-state-of-the-union_n_2669941.html Ron Deibert, Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace, Canadian Defence & Foreign Affairs Institute, August 2012. https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf

[4] Ministry of Public Safety, Government of Canada Launches Cyber Security Awareness Month with New Public Awareness Campaign Partnership, September 27, 2012. http://www.publicsafety.gc.ca/media/nr/2012/nr20120927-1-eng.aspx
[5] Get Cyber Safe. http://www.getcybersafe.gc.ca/index-eng.aspx

About SciencePages

SciencePages (www.sciencepages.ca) is an initiative of the Partnership Group for Science and Engineering (www.pagse.org) in collaboration with the Science Media Centre of Canada (www.sciencemediacentre.ca).

SciencePages aims to increase discussion on topical issues that have science and engineering at their core, by summarizing the current state of knowledge and policy landscape.

Each issue is prepared and reviewed by a multi-disciplinary team and is published regularly, free of charge.

This issue is made possible thanks to the Natural Sciences and Engineering Research Council of Canada (NSERC) the Canada Foundation for Innovation (CFI) and Federal S&T Community Secretariat.

It was prepared by Carlton Davis, Tomas Urbina, and Simon Liem.

For more information please write to us at: info@sciencepages.ca.

A fully referenced version of the SciencePages is available at www.sciencepages.ca