SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Did Patriot Hackers Attack the Canadian Government?

By Terry Cutler on Mar 21, 2011

Like Confirm Buzz Tweet 16 0 Digg Share RSS

It appears that **Canada's Finance, Defense Research and Development departments, as well as the Treasury Board, were hacked** in February by what the Canadian government is calling an "unprecedented" and "significant" cyber attack. Although confirmation is pending, the attack seems to be the work of patriot hackers, using computer servers based in China.

The Canadian government admitted that if the hackers went all the way they would have accessed the financial information of private citizens.

This attack is hard to pull off, on one hand, and dangerously simple, on the other. Although seven months prior, CSIS, Canada's Spy agency, warned in a **CBC report** that this attack was coming, the Canadian government still fell victim to it. This could happen to anyone. Someone could be at a conference and send you an email with a link to a picture. You click on it, and your system is infiltrated by malware that hackers can leverage. You have been phished.

On a larger scale, with a specialized form of executive **spear-phishing**, big businesses, trading companies and as we have seen in February, the federal departments of big governments are at risk. It all starts with a simple everyday e-mail. When someone sends an e-mail that says "I am the CEO and I forgot my password, could you please reset it to doug123 so that I can change it later?" many employees don't even question that before resetting the password. At this point, the hacker usually has access to the inside network but doesn't want to set off intruder lockout alarms. Having the admin reset the password for him is much easier.

This is called executive spear-fishing and it's different from a typical phishing attack. In the basic attack, you tend to receive a bi-weekly 65 percent off Cialis pills. You click and you get attacked. Executive spear-phishing is a more sophisticated and convincing e-mail and is targeted at certain people in government or big business.

It happens all the time, and is very difficult to defend against. We are naturally trusting, and it is our human nature to help others. However in doing so we are putting the security of the company at risk.

One of the biggest problems is that most departments in many large companies have their own security policy. If you do not have some form of hierarchy group, or an outsourced firm for your company that specializes in Internet security, the problem will never be fixed, no matter how much money you throw at it.

Security awareness training for employees is very low on the priority list. The reasons for this could be high staff turnover, a lack of allotted funds for training, or no security defense plan to begin with it.

Most of the systems I've encountered are out-dated. Having worked with the government for ten years through a large software vendor, I noticed that the systems are not up to date with the latest and greatest

Google™ Custom Search Search ×

SUBSCRIBE TO SECURITYWEEK

Enter Your Email Address Subscribe

Most Read Most Recent

- Survey Reveals How Stupid People are With Their Passwords
- New Tool Reveals Internet Passwords
- Hacker Uses XSS and Google Street View Data to Determine Physical Location
- Snoop Dogg Joins the War on Cybercrime
- Study Reveals 75 Percent of Individuals Use Same Password for Social Networking and Email
- The Rise of the Small Botnet
- An Inside Look at Hacker Business Models
- IT Salary Guide Shows Increase in Salaries for IT Security Professionals
- Nevercookie Eats Evercookie With New Firefox Plugin
- Defense Department's Cyberwar Credibility Gap
- The Commodities of Underground Markets
- Commercial Software Harnesses Amazon Cloud to Crack Passwords Faster
- McAfee to Acquire Database Security Firm Sentrigo
- Behind Bars: The Hospital Guard Hacker Who Posted His Crime on YouTube
- BreakingPoint Provides War Game Training Using its Network-Crushing Appliance
- Data Security at the Point of Sale: Back to the Basics
- NetQin Mobile Launches Anti-virus for BlackBerry
- Google Sponsors Cybersecurity Seminar Series at the University of Maryland
- Cisco Solution Extends Corporate Wireless Network Control and Security to Remote Workers
- AVG Technologies Arranges $235 Million in Financing

patches or firmware. Furthermore, there's just so much red tape to get through before it can be turned into a project.

Even more frustrating, most government staff work 9-5; they are overworked and underpaid. Companies could bring in extra shifts, but more than likely it would be better to outsource it to a company that specifically deals with these problems.

I often notice that once a breech or attack unfolds, company officials panic and start shutting things down. Once they go off the grid, they delete critical log files, rather than preserve the evidence so forensic investigations can trace the hacker.

Finding the origin of the attack is also difficult. A hacker could go through several proxy servers which makes the hacker appear that he's attacking from other countries such as China. By hiding their tracks, there's a high probability that this happened to the Canadian government. This is why, when it finally gets pieced together, the government thinks it came from China instead of next door.

To track the attacker means getting a search warrant to investigate the server. The server is most likely is in another country, and is part of multi-proxy servers which, in all probability, has the logs deleted.

This consumes time and money, often causing the investigation to stall or come to a dead end.

So what can we do?

The first line of defense is right in the e-mail. When you receive a link all you have to do is pass the cursor over it to see a link to a website. Remember to always click on links that come from social networks in their respective inboxes -- never click an e-mail from Facebook or Linkedin in your Hotmail account. If links are unfamiliar, suspicious activity should be considered. An employee should report it to security, or the person delegated to receive these reports.

SIEM (Security Information Event Management) software can pull logs on a routine basis from all the systems in the company. SIEM, if properly deployed, will **report suspicious activity**. In addition, other software can help, like identity & access management. If there was a critical server in the system, and we know that no one in the department should be accessing it at a certain hour of the night, we would easily detect foul play. In some situations, unauthorized late night cleaning crews have been found checking personal e-mails.

Cyber attacks have replaced bank robberies. It's important to get defense knowledge. A hacker is always on the cutting-edge. The recent events should be a wake-up call to governments and business, especially since the "**Anonymous Group**" wants blood. They need to get their cyber defenses up to stop events like this from happening. Otherwise, one day soon, they'll be just another victim.

See Also: How to Protect Your Organization Against Advanced Persistent Threats

Like Confirm Buzz Tweet 16 0 Digg Share RSS

Terry Cutler is a co-founder of Digital Locksmiths, Inc., an IT security and data defense firm based in Montreal and serves as the company's Chief Security Evangelist and Certified Ethical Hacker. Prior to joining Digital Locksmiths, he was a Premium Support Engineer for Novell in Canada where he analyzed network vulnerabilities and transitioned security technologies into production. In addition to being a licensed private investigator in Canada, Terry is an internationally known author, trainer, speaker, and security consultant, Terry has appeared in numerous national television and radio programs and is very active on the conference circuit. Follow Terry on Twitter at @TerryPCutler

Previous Columns by Terry Cutler:

- Did Patriot Hackers Attack the Canadian Government?
- A Compliance with a Complex Problem
- Beating Back the Botnets
- Enterprise Security Priorities for 2011
- Mobile Security: It's Time to Get Serious

- **Security Focus on Consumer Electronics w/ BONUS Free Software Trial**
- **Introduction to Security for Smart Object Networks Devices w/ BONUS Free Software Trial**
- **Best Practices for Testing Secure Applications for Embedded Devices**
- **Mitigation of Security Vulnerabilities on Android & Other Open Handset Platforms**

Tags: Cyberwarfare INDUSTRY INSIGHTS Virus & Threats

Like DISQUS

Showing 0 comments

Sort by Best rating **Subscribe by email** **Subscribe by RSS**

Add New Comment

Type your comment here.

Post as ...

Trackback URL http://disqus.com/forums/securityweek/was_c

Popular Topics

- Information Security News
- IT Security News
- Risk Management
- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community

- IT Security Newsletters
- Events
- Comments
- Most Read

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Stuxnet Group on LinkedIn
- RSS Feed
- Submit Tip

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media