PC infection rates rising in Canada, Microsoft warns

October 14, 2011
By Liam Lahey

Microsoft highlights the fact that some of the more common threats can be mitigated through good security best practices.

Microsoft's Bruce Cowper

It's not often we hear of current IT security practices getting it right but then that doesn't make for splashy headlines. Nevertheless, a recently released security intelligence report conducted by Microsoft has found exactly that with respect to 'zero-day' threats.

The Microsoft Security Intelligence Report volume 11 found that less than one per cent of exploits in the first half of 2011 were against zero-day vulnerabilities — software vulnerabilities that are successfully exploited before the vendor has published a security update or "patch."

In contrast, 99 per cent of all attacks during the same period distributed malware through familiar techniques, such as social engineering and unpatched vulnerabilities.

Think you're being left out Canada? Guess again. Canadians are targeted for a significant number of social engineering attacks with almost three times more phishing sites than the global average and more than three times the percentage of sites hosting drive-by downloads.

"This means that the most common malware threat in Canada is Adware, which affected 45.8 per cent of all infected computers in 2Q11, down from 57.5 per cent in 1Q11 but significantly higher than the world wide average," explained Bruce Cowper, senior security strategist for Trustworthy Computing at Microsoft. "Adware rose to become the most commonly detected category due in large part to a pair of new threat families that did not exist in 2010- Win32/OpenCandy and Win32/ShopperReports."

User interaction, typically employing social engineering techniques, is attributed to nearly half (45 per cent) of all malware propagation in the first half of 2011 globally. More than a third of all malware is spread through cybercriminal abuse of Win32/Autorun, a feature that automatically starts programs when external media, such as a CD or USB, are inserted into a computer. Ninety per cent of infections that were attributed to vulnerability exploitation had a security update available from the software vendor for more than a year.

While there's been an overall drop in the number of Canadian computers infected with malicious software (1.8 per cent), the most common types of successful exploits indicate that Canadians still have a way to go with keeping their systems up to date.

For example, worms and Trojans (downloaders and droppers) were significantly higher in Canada than the worldwide average, yet security updates have been in place to help stop these from propagating for some time, Cowper remarked.

"A key finding of the report is that a new method of analyzing malware distribution indicates that the zero-day vulnerability accounted for a very small percentage of actual infections in the first half of 2011," he said. "None of the major threat families found by the Malicious Software Removal Tool (MSRT) were propagating through the exploit of zero-day vulnerabilities."

These statistics may come as a surprise to some in the industry, he conceded. However, the key takeaway is how malware was actually propagating – social engineering, Autorun feature abuse, file-infection, and exploits (with updates available).

"Many of these attack vectors can be mitigated against through actions such as the application of fundamental good security practices, almost a sort of 'back to basics' approach."

Regarding mobile security, exploits affecting Google's Android mobile operating system (OS) and the Open Handset Alliance have been detected in significant volume beginning in early 2011. The increase in Android-based threats has been driven largely by the exploit Unix/Lotoor, the second most commonly detected OS exploit in the first half of this year.

"Lotoor is used to attack vulnerable devices by the Trojan family AndroidOS/DroidDream which often masquerades as a legitimate Android application, and is capable of allowing a remote attacker to gain access to the device. Google published a security update in March 2011 addressing this vulnerability," he said.

In the global report, Microsoft provides insight into reducing Win32/Autorun abuse with updates released earlier this year for Windows XP and Windows Vista (Windows 7 already included these updates) that prevent the Win/32Autorun feature from being enabled automatically for most media. Within four months of issuing the update, the number of infections from the most prolific Win32/Autorun-abusing malware families was reduced by almost 60 per cent on Windows XP and by 74 per cent on Windows Vista in comparison to 2010 infection rates, the company said.

Microsoft advocates a multifaceted approach to managing risk including:

- Companies should concentrate on educating employees on their responsibility to security and back that up by developing and enforcing companywide security policies in areas such as passwords.
- Upgrade to the latest products and services. Making the move to the most current products and services helps increases protection against the most prevalent online threats.
- Consider cloud services. In a cloud environment, the cloud vendor manages many of the security processes and procedures required to keep a system up to date, including the installation of security updates. Businesses and consumers constrained in managing the security of their computing environment can leverage cloud services to help offload portions of their security management.

Cowper will make a keynote speech at the SecTor 2011 conference at 12 p.m. ET on Oct. 18. His talk will focus on the importance of the relationship between customers and vendors and what businesses should be asking and expecting from a cloud service provider.

Keep up to date with what's going on in the Canadian IT channel community by subscribing to ChannelBuzz.ca's Daily Buzz e-mail newsletter or RSS feed, and following ChannelBuzz.ca on Twitter or Facebook.

More From ChannelBuzz.ca

- McAfee opens up Secure in 15 to partners
- The cloud and the Microsoft Canada/VTN connection
- VTN members welcome return of all-Canada meeting

Share the Buzz!

Tags: Android, Bruce Cowper, CIO, Cloud, Consumer, Consumers, Google, Malware, Microsoft, Microsoft Security Intelligence Report, Partnerpedia, Phishing, Security, Service Provider, Windows 7, Windows Vista, Windows XP

This entry was posted on October 14, 2011 at 12:15 pm and is filed under Security, Software. You can follow any responses to this entry through the RSS 2.0 feed.

One Response to *PC infection rates rising in Canada, Microsoft warns*

1. You Canadians are so smug, . . . « kengross144 on October 15, 2011 at 1:44 pm

   [...] Canadians are now being targeted through social media and Adware. Well here is the article: http://www.channelbuzz.ca/2011/10/pc-infection-rates-rising-in-canada-microsoft-warns-2619/ Now this kind of makes me feel better about the world situation. I mean when was the last time [...]

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment *

Post Comment

QuickVid: Markham's Newcomp gets IBM partner award