Microsoft Security Intelligence Report
The Threat Landscape in Canada

Tim Rains
Director, Trustworthy Computing
Microsoft Corporation

TwC Next
Marking a Milestone.
Continuing Our Commitment.
Source of Threat Intelligence

Over 280 million active Hotmail accounts with billions of emails scanned.

Microsoft Security Essentials—operating globally in more than 30 languages.

Malicious Software Removal Tool—downloaded and executed almost 3.9 billion times in the first half of 2012.

Billions of web pages scanned by Bing each day.

Microsoft Security Intelligence Report:
Threat intelligence from over **600 million systems** in **100+ countries/regions**.
Infection Rate Since 2009

The graph illustrates the infection rate per thousand scanned computers from 3Q09 to 2Q12. The data is categorized into two groups: CCM (admin specified) and CCM (IP). The graph shows a decrease in infection rates over time, with the CCM (IP) group consistently lower than the CCM (admin specified) group. The infection rates for Canada and Worldwide are also shown, with Canada having lower infection rates compared to Worldwide.
Threat Categories in Canada

The chart illustrates the percentage of computers with detections of various threat categories in Canada compared to worldwide. The categories include:

- Misc. Trojans
- Exploits
- Adware
- Trojan Down loaders & Droggers
- Worms
- Password Stealers & Monitoring Tools
- Backdoors
- Viruses
- Spyware

The chart uses blue bars to represent Canada and orange bars to represent worldwide. The y-axis indicates the percent of computers with detections, ranging from 0% to 50%.
## Threat Families in Canada 2Q12

<table>
<thead>
<tr>
<th>Family</th>
<th>Most Significant Category</th>
<th>% of Computers Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 JS/Blacole</td>
<td>Exploits</td>
<td>10.1%</td>
</tr>
<tr>
<td>2 HTML/IframeRef</td>
<td>Exploits</td>
<td>9.2%</td>
</tr>
<tr>
<td>3 Win32/FakePAV</td>
<td>Misc. Trojans</td>
<td>8.8%</td>
</tr>
<tr>
<td>4 Win32/Hotbar</td>
<td>Adware</td>
<td>8.6%</td>
</tr>
<tr>
<td>5 JS/Pornpop</td>
<td>Adware</td>
<td>8.0%</td>
</tr>
<tr>
<td>6 ASX/Wimad</td>
<td>Trojan Downloaders &amp; Droppers</td>
<td>7.7%</td>
</tr>
<tr>
<td>7 CVE-2012-0507</td>
<td>Exploits</td>
<td>7.5%</td>
</tr>
<tr>
<td>8 Win32/Keygen</td>
<td>Misc. Potentially Unwanted Software</td>
<td>7.1%</td>
</tr>
<tr>
<td>9 Win32/Winwebsec</td>
<td>Misc. Trojans</td>
<td>6.9%</td>
</tr>
<tr>
<td>10 Win32/Sirefef</td>
<td>Misc. Trojans</td>
<td>6.8%</td>
</tr>
</tbody>
</table>
Exploit Trends

- The number of systems reporting exploits delivered through HTML or JavaScript increased steeply in the second half of 2011, due primarily to the emergence of JS/Blacole.

![Graph showing exploit trends from 1Q11 to 4Q11 with categories such as HTML/JavaScript, Java, Documents, Operating System, Adobe Flash (SWF), Shellcode and Heapspray, and Other.]
Java Exploits

- Many of the more commonly exploited Java vulnerabilities are more than 10 years old, as are the security updates that have been released to address them.
- The CVE-2010-840 vulnerability is exploited by JS/Blackhole and is only seen in Canada.

Top exploit in Canada 1H11-2H12 (detected 9.2+ million times)

2nd most detected exploit in Canada 1H11-2H12 (detected 6+ million times)

3rd most detected exploit in Canada 1H11-2H12 (detected 3.5 million times)

4th most detected exploit in Canada 1H11-2H12 (detected 2+ million times)
Blacole Example

Example email containing a malicious link

The antimalware software installed on the system detected a component of the Blacole exploit kit
Threat Categories in Canada

- Adware
- Exploits
- Misc. Trojans
- Spyware
- Viruses
- Backdoors
- Misc. Potentially Unwanted Software
- PWS and Monitoring Tools
- Trojan Downloaders and Droppers
- Worms

Charts show trends from 1Q11 to 2Q12 for various threat categories.
FakePAV Example

Fake Security Essentials Alert Dialog

FakePAV claims that it can't remove the threat and prompts you to "scan online".

Current versions of FakePAV claim that you need to install AV software and that "ThinkPoint" will be installed as soon as the machine is rebooted.

The affected machine is now even more difficult to use; in addition to stopping explorer.exe from running, it terminates task manager, leaving no easy way to run any other programs.
## Malicious Websites in Canada

<table>
<thead>
<tr>
<th>Metric</th>
<th>1Q12</th>
<th>2Q12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing sites per 1000 hosts (Worldwide)</td>
<td>1.35 (1.54)</td>
<td>1.50 (1.62)</td>
</tr>
<tr>
<td>Malware hosting sites per 1000 hosts (Worldwide)</td>
<td>2.52 (2.66)</td>
<td>2.62 (3.01)</td>
</tr>
<tr>
<td>Percentage of sites hosting drive-by downloads (Worldwide)</td>
<td>0.088% (0.072%)</td>
<td>0.091% (0.154%)</td>
</tr>
</tbody>
</table>
Update Service Usage

PERCENT OF 2008 TOTAL USAGE

- Microsoft Update - Worldwide
- Windows Update - Worldwide
- Windows Update - Canada
- Microsoft Update - Canada
Infection Rates by OS and Service Pack

- Normalized numbers
- Infection rates for more recently released operating systems and service packs are consistently lower than earlier ones, for both client and server platforms
- Infection rates for 64-bit editions of Windows Vista and Windows 7 have increased
## Protect Your Environment

| ✔ | Keep all software on your systems updated |
| ✔ | Run anti-virus software from a trusted vendor |
| ✔ | Use caution when clicking on links (webpages, attachments and file transfers) |
| ✔ | Protect yourself from social engineering attacks |
Resources

**Website**
http://microsoft.com/sir

**Blog**
http://blogs.technet.com/b/security/
http://blogs.technet.com/b/mmpc/

**Twitter**
@MSFTSecurity
@MSFTmmpc