Malware Without Borders
Multi-Party Response

Ziv Mador
Senior Program Manager and Response Coordinator

Jeff Williams
Principal Group Manager

Microsoft Malware Protection Center
Content

- Trend of Malware and Potentially Unwanted Software becoming more regional
- MSRT and Windows Defender telemetry collection methods
- Trends demonstrated by normalized infection rates
- The threat landscape in the selected countries
- Breakdown by OS versions
- Example of malware “without borders”
- What can we do about it?
- Q&A
Attacks are becoming more regional

Years ago, we saw major outbreaks of self-replicating worms

➤ They infected hosts regardless of language or location

These days attacks rely more often on social engineering

➤ Spread and effectiveness depend upon language and culture
**MSRT Executions**

- Malicious Software Removal Tool
- Shipped every month with Microsoft security updates

*Monthly MSRT Executions — Grand Total and Windows XP SP2*

*Monthly MSRT Executions — Other Operating Systems*
About 75% of users opt in to send reports.
Infection Rates Using MSRT Data (2H07)

2H07 Infection Ranges—
MSRT Executions per Computers Cleaned
- Insufficient data
- 0-49
- 50-99
- 100-149
- 150-199
- 200-249
- 250-299
- 300-399
- 400-500
- >500
On average, developing countries exhibit more infections than developed countries.
Non-uniform Distribution of Malware and Potentially Unwanted software

Showing the top 8 out of 24 categories (2H07)
Top Detections

China
- Spyware: CnsMin
- Browser Modifier: Baidu
- Browser Modifier: CNNIC

Korea
- Virus: Virut
- Spyware: RewardNetwork
- Backdoor: Rbot
- Virus: Parite
- Virus: Jeefo

Japan
- Spyware: CnsMin
- Trojan Downloader: Zlob
- Worm: Antinny

South Africa
- Trojan Downloader: Zlob
- PUS: Starware
- Adware: WhenU

France
- Trojan Downloader: Zlob
- Adware: Slagent
- Adware: Hotbar

Brazil
- Trojan and PWS: Banker
- Trojan Downloader: Zlob
- Adware: WhenU

Russia
- Adware: WhenU
- Virus: Jeefo
- Worm: Rjump

US:
- Trojan Downloader: Zlob
- Trojan Downloader: Renos
- Adware: Hotbar
Example 1: BrowserModifier
Win32/CNNIC

- Enables Chinese keyword searching in IE
- Sometimes installs without user consent
- Uses kernel mode driver to protect its files and registry settings
- Self-updates
Example 2: Worm: Win32/Antinny

- Spreads using the Winny Peer-to-peer file sharing application
- Copies itself to the Winny upload folder with a deceptive filename
- Targets Japanese-speaking populations
- Uses Japanese for its messages and displays additional graphics
- May copy other personal files to the shared folders
Example #2: Win32/Antinny

- 98.4% of detections occurred in Japan
- The rest: Korea, US, Taiwan, China & others

Computers Cleaned by the MSRT of the Win32/Antinny Worm
Example 3: Win32/Banker and Win32/Bancos

- Family of data-stealing trojans that capture banking credentials
- Mostly target customers of Brazilian banks
- Over 11,000 samples in 2H07, many of them use Portuguese

<table>
<thead>
<tr>
<th>Country / Region</th>
<th>% Detections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>70.5%</td>
</tr>
<tr>
<td>Portugal</td>
<td>9.0%</td>
</tr>
<tr>
<td>Spain</td>
<td>7.8%</td>
</tr>
<tr>
<td>US</td>
<td>5.9%</td>
</tr>
<tr>
<td>France</td>
<td>1.5%</td>
</tr>
<tr>
<td>Italy</td>
<td>0.9%</td>
</tr>
<tr>
<td>UK</td>
<td>1.1%</td>
</tr>
<tr>
<td>Mexico</td>
<td>0.7%</td>
</tr>
</tbody>
</table>
**OS Breakdown**

- 60% less malware and PUS detected on Vista compared to Windows XP SP2
- The higher the Service Pack level installed, the lower the rate of infection
- Server versions of Windows typically display lower infection rates than client versions

Computers cleaned by the MSRT, 2H07 (Normalized)

- Windows 2K SP4, 5.0%
- Windows 2K SP3, 12.2%
- Windows 2K SP1, 19.2%
- Windows no SP, 30.6%
- Windows XP SP2, 7.2%
- Windows XP SP1, 21.5%
- Windows Vista, 2.8%
- Windows XP SP2, 1.5%

Computers cleaned by Windows Defender, 2H07 (Normalized)

- Windows 2003, 27.5%
- Windows Vista, 28%
- Windows XP SP2, 44.5%
Uneven OS Deployment in Different Regions

Reflects on the prevalence of malware or potentially unwanted software regionally

MSRT Executions
Other Malware "Without Borders"

- There are still some threats that are spread across many different regions.
- Mostly malware that may be distributed in multiple ways.
- Either shows no UI or uses English.
Example: Malware "Without Borders"
Trojan Downloader: Win32/Zlob

- Major distribution methods:
  - Fake codec files
  - Rogue antispyware application
  - Malicious ad banners

- Telemetry:
  - Detected over 17.5 million times in 2H07
  - Detected in over 240 locales
Example: Malicious Downloader Win32/Zlob

Even though detected almost anywhere, it is by far more prevalent in the US

Computers Cleaned by the MSRT of the Win32/Zlob Downloader

- WW
- US
- UK
- Spain
- Germany
- France
So Many Threats Are Regional - What Can We do About it?...

- Expand the collaboration between industry and national response teams
- National CERTs can lead here by:
  - Identifying regional threats
  - Working with the industry to address them
    - Collecting and submitting samples
    - Sharing specific regional impact detail with vendors
  - Working with law enforcement to facilitate cases against attackers
- Recently announced program: SCPcert
Driving user education

- Apparent correlation between broad national outreach and reduction in infection rate
  - Finland
  - Japan
  - Australia

Encouraging the ISV community to adopt secure development practices
Links

Microsoft Security Intelligence Reports
  http://microsoft.com/sir
Microsoft Malware Protection Center
  http://www.microsoft.com/security/portal/
Windows Malicious Software Removal Tool
  http://www.microsoft.com/malwareremove
Windows Defender
  http://www.microsoft.com/windowsdefender
Questions?