Windows 7 impact upon rogue security software

Josh Norris, Threat Discovery Analyst • jnorris@isightpartners.com
Ken Dunham, Director of Global Response • kdunham@isightpartners.com
Overview

- Windows 7 Impact Upon Rogue AV?
- Key Security Features Examined
  - User Account Control (UAC)
  - Windows Defender
- Win7 Tests of Rogue AV & Malcode
- Legacy Code and Adapted Codes for Win7
- Key Takeaways of Anecdotal Research
The Transition
Key Security Features

• Notification area settings Control Panel
• Windows Defender
• User Account Control (UAC)
Notification Area Control Panel

- Allows modification of taskbar icon and notification behavior

<table>
<thead>
<tr>
<th>Icons</th>
<th>Behaviors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Center</td>
<td>Show icon and notifications</td>
</tr>
<tr>
<td></td>
<td>Solve PC issues: 2 important message...</td>
</tr>
<tr>
<td>Network</td>
<td>Show icon and notifications</td>
</tr>
<tr>
<td></td>
<td>Network: 2 internet access</td>
</tr>
<tr>
<td>Volume</td>
<td>Show icon and notifications</td>
</tr>
<tr>
<td></td>
<td>Speakers: 100%</td>
</tr>
<tr>
<td>Windows Explorer</td>
<td>Only show notifications</td>
</tr>
<tr>
<td></td>
<td>Safely Remove Hardware and Eject M...</td>
</tr>
<tr>
<td>VMware Tools tray application</td>
<td>Only show notifications</td>
</tr>
<tr>
<td></td>
<td>VMware Tools can be upgraded.</td>
</tr>
<tr>
<td>Sysinternals Process Explorer</td>
<td>Only show notifications</td>
</tr>
<tr>
<td></td>
<td>CPU Usage: 0%</td>
</tr>
<tr>
<td>winpc.exe</td>
<td>Only show notifications</td>
</tr>
<tr>
<td></td>
<td>WinPC Defender</td>
</tr>
</tbody>
</table>
Windows Defender

• The included spyware monitoring package for Windows Vista and Windows 7
• Can be disabled or limited by the end user
• Moderately successful at catching malicious code
User Account Control (UAC)

- Introduced with Windows Vista
- Effective, yet perceived as an annoyance
Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

- Default - Notify me only when programs try to make changes to my computer
  - Don't notify me when I make changes to Windows settings
  - Recommended if you use familiar programs and visit familiar websites.

Never notify

OK Cancel
The Purpose of UAC

• NOT a security boundary but rather a convenience.
• An attempt to take advantage of the fact that most Malcode requires admin rights to function properly.
• Prevents modification of key directories and registry hives.
• Prevents full compromise, not necessarily full functionality.
Testing Malcode in Windows 7

- Codes tested in a Windows 7 environment fall into two main categories:
  - Rogue AV
  - Trojans
- Tested with UAC at “Always Notify”, Windows Defender on and updated, and no traditional AV.
Rogue AV

• Designed to intimidate
• Chosen for testing because of:
  – Popularity
  – Potential impact of Windows 7 security features
• Typical attack vector involves online exploitation
• The con artist of the malcode world
$59.95 to ease your pain...

AKM Antivirus 2010 Pro

You Security Status: **At Risk**

**AKM Antivirus 2010 Pro** helps protect your PC.

**Scanning for viruses**

AKM Antivirus 2010 Pro evaluation

This version of AKM Antivirus 2010 Pro is for evaluation purposes only. The removal feature is disabled. You may scan your PC to locate malware threats. Please purchase the full version of AKM Antivirus 2010 Pro to remove identified threats.

- Purchase full version
- Continue Evaluating

AKM Antivirus 2010 Pro activation

If you have already purchased a license, please enter activation code:

- Activate AKM Antivirus 2010 Pro Now!

**Trojan.Win32.Agent.azsy**

Alert level: Medium

This malicious program is a Trojan, it is a Windows Trojan.
Success by Accident

• Rogue AV does not typically need extensive control or rights
• Many are unintentionally successful...
...Many are not
Trojans

- Often a secondary payload
- Extremely varied, but usually designed to control and/or glean data
  - Via: Keylogging, DDoS, form injection, webcam control, and more
- Not more malicious than Rogue AV but typically more harmful and difficult to remove
- Typically need admin access
Antivirus 2010 - Faked a "Blue Screen of Death" and restart, but was detected by Windows Defender following the fake restart

***STOP: 0x000000D1 (0x0000000, 0xF73120AE, 0xC0000008, 0xC0000000)

A spyware application has been detected and Windows has been shut down to prevent damage to your computer

SPYWARE.MONSTFR.FX_WII D_0x00000000

If this is the first time you’ve seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure your antivirus software is properly installed. If this is a new installation, ask your software manufacturer for any antivirus updates you might need.

Windows detected unregistered version of Antivirus 2010 protection on your computer. If problem continue, please activate your antivirus software to prevent computer damage and data loss.

*** SRV.SYS - Address F73120AE base at C0000000, DateStamp 36b072a3
Beginning dump of physical memory...
Physical memory dump complete. Restarting...
ByteDefender – Generated a UAC prompt and then, even when allowed to run with full admin rights, failed to install altogether.
## Rogue Anti-virus

<table>
<thead>
<tr>
<th>Malcode</th>
<th>Result of Installation Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>AKM Antivirus 2010</td>
<td>Success: Installed with full functionality</td>
</tr>
<tr>
<td>Antivirus Pro</td>
<td>Failed: Triggered UAC prompt.</td>
</tr>
<tr>
<td>Antivirus 2010</td>
<td>Partial: Ran initial scare tactics; failed to install.</td>
</tr>
<tr>
<td>Antivirus 7</td>
<td>Failed: Triggered UAC and installation failed.</td>
</tr>
<tr>
<td>ByteDefender</td>
<td>Failed: Triggered UAC and installation failed.</td>
</tr>
<tr>
<td>Digital Protection</td>
<td>Partial: Ran initial scare tactics; failed to install.</td>
</tr>
<tr>
<td>Rapid Antivirus</td>
<td>Partial: Ran initial scare tactics; failed to install.</td>
</tr>
<tr>
<td>Security Tool</td>
<td>Success: Installed with full functionality</td>
</tr>
<tr>
<td>WinPC Antivirus</td>
<td>Failed: Triggered Windows Defender</td>
</tr>
</tbody>
</table>
Zeus – The gold standard of banking Trojans in the underground
– Thwarted initially....
...but then adapted
## Trojan Test Results

### Other Malcode

<table>
<thead>
<tr>
<th>Code</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bebloh</td>
<td>Failed: Unable to inject into csrss.exe.</td>
</tr>
<tr>
<td>Gumblar</td>
<td>Failed: Unable to access system32 - UAC protected</td>
</tr>
<tr>
<td>Mebroot</td>
<td>Failed: Unable to access MBR</td>
</tr>
<tr>
<td>Poison Ivy</td>
<td>Failed: Assumed kernel32.dll to be first DLL in list</td>
</tr>
<tr>
<td>TDL3</td>
<td>Failed: Unable to access system32 - UAC protected</td>
</tr>
<tr>
<td>Spy-Net</td>
<td>Success: Installed with full functionality.</td>
</tr>
<tr>
<td>SpyEye</td>
<td>Success: Installed with full functionality.</td>
</tr>
<tr>
<td>Zeus</td>
<td>Success: Installed with full functionality. Adapted</td>
</tr>
</tbody>
</table>
Interest in the Underground

• Common questions, Easily answered
• Actors adapt: Following the money

Best RAT, who is compatible with Win7?

Hello Community,

I'm looking for the best RAT, who is compatible with Windows 7 and runs very stable! Previously, as I know Bifrost, Poison Ivy, Shark and Spy-Net were very well known. But since Vista/Win7 they are all have difficulties.

What would you recommend?

PS: Sorry für my language, english is not my mother tongue 😊
Key Takeaways

• Rogue AV: From accidental success to trendsetter
• Kernel level access difficult to obtain
• Zeus: A microcosm of the Malcode community
• UAC is a big step in the right direction
• Additional defenses are recommended
  – Data Execution Prevention (DEP)
  – Network level filtering
  – Patching
  – Traditional AV
Questions?