



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



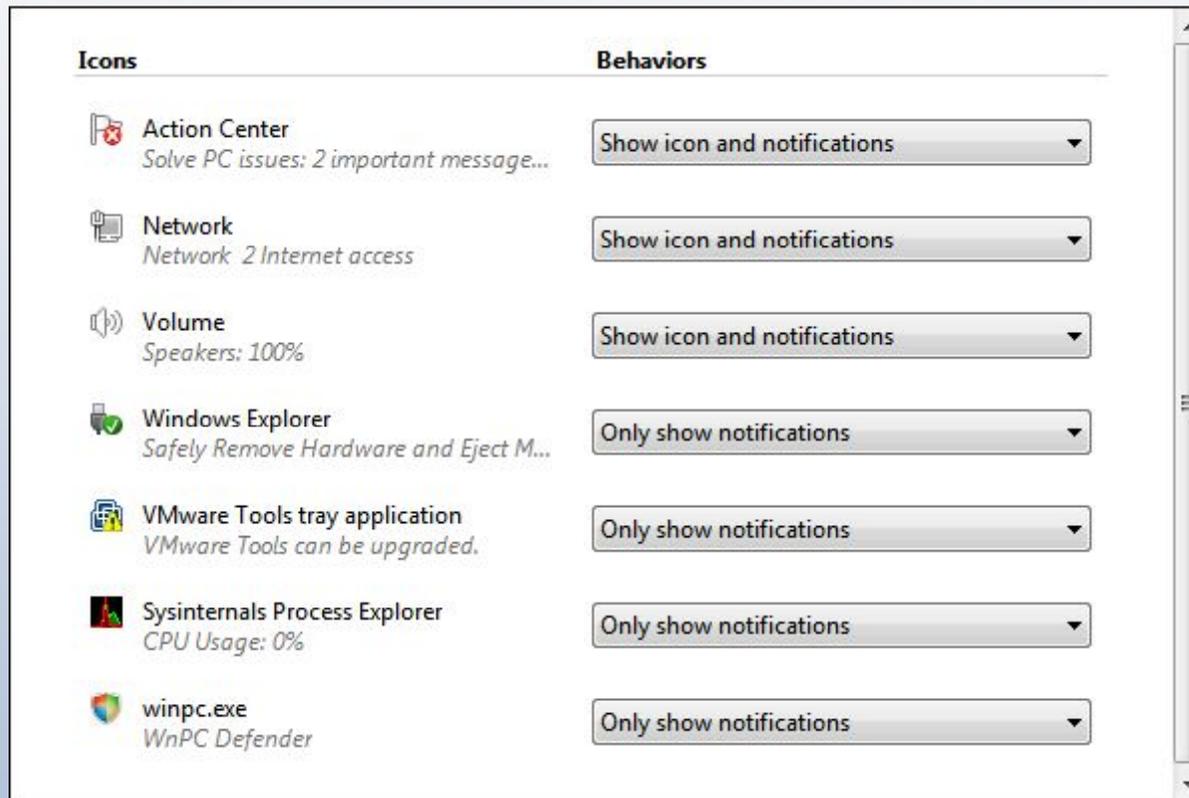


Key Security Features

- **Notification area settings Control Panel**
- **Windows Defender**
- **User Account Control (UAC)**

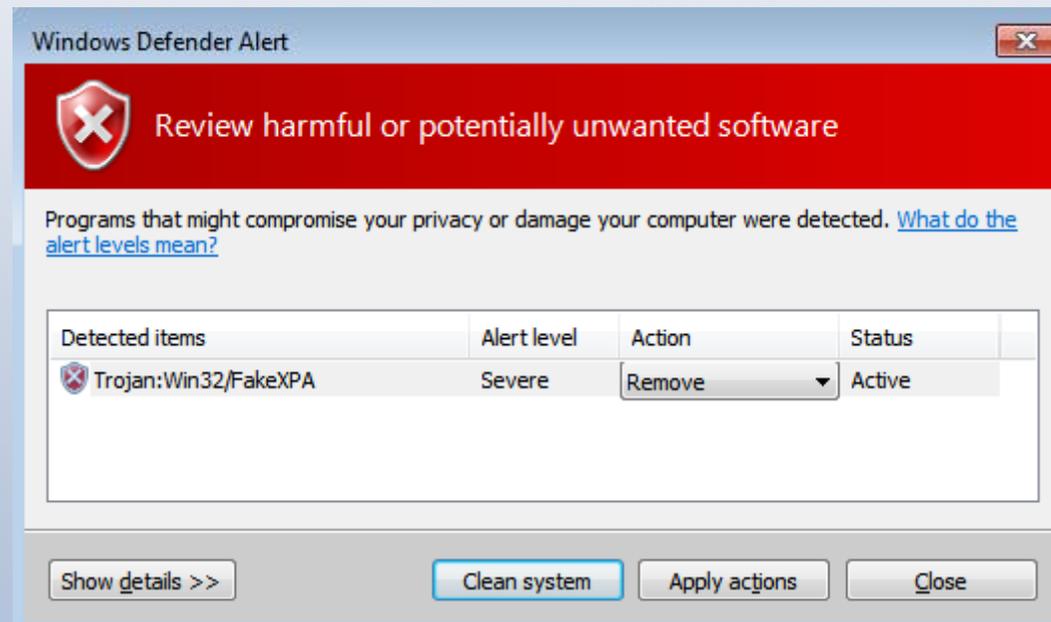
Notification Area Control Panel

- Allows modification of taskbar icon and notification behavior



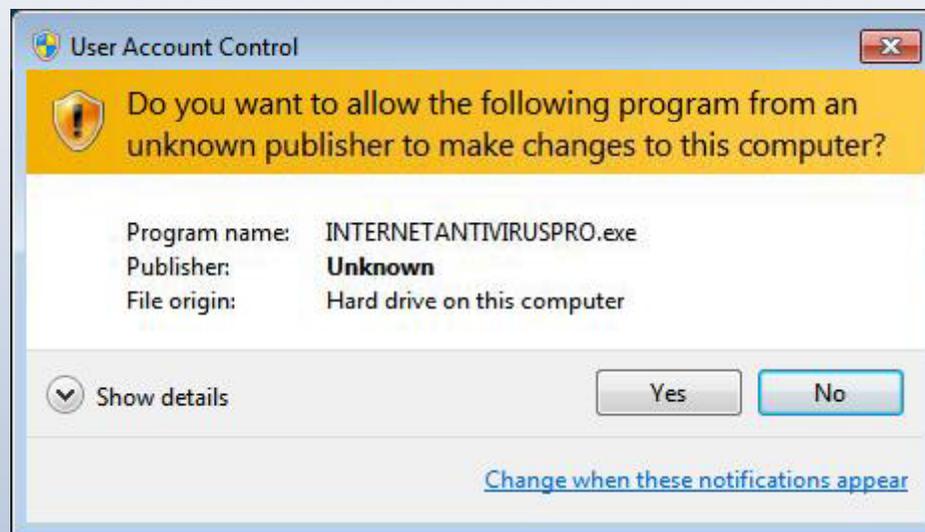
Windows Defender

- 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

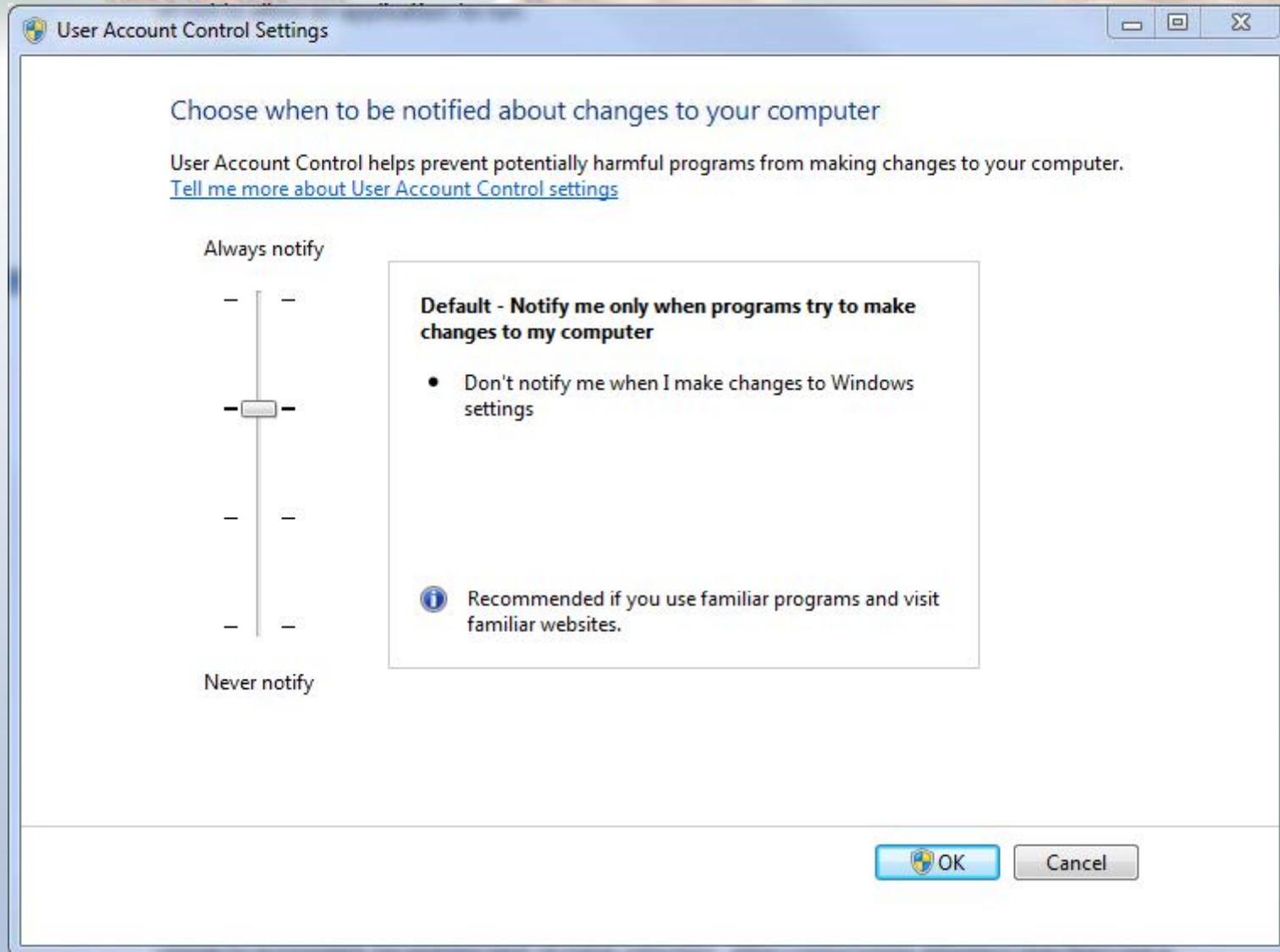


User Account Control (UAC)

- Introduced with Windows Vista
- Effective, yet perceived as an annoyance



More Control





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 malware world

\$59.95 to ease your pain...

The screenshot displays the AKM Antivirus 2010 Pro interface. At the top, the title bar reads "AKM Antivirus 2010 Pro". The main header features the product name "AKM Antivirus 2010 Pro" and the tagline "Helps Protect your PC". A prominent red warning icon with the text "Windows is in danger" is visible in the top right corner.

The interface is divided into several sections. On the left, a vertical navigation menu includes icons for "System Scan", "System", "Privacy", "Firewall", "Updates", "Settings", "Security", "Enterprise", and "Support". The "System Scan" section is active, showing a "Scanning for viruses" status with a green checkmark. A "Start" button is visible next to it.

A central dialog box is overlaid on the interface, containing two sections:

- AKM Antivirus 2010 Pro evaluation:** This section features a red warning icon and text stating: "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." Below this text are two buttons: "Purchase full version" (with a green checkmark icon) and "Continue Evaluating" (with a red X icon).
- AKM Antivirus 2010 Pro activation:** This section features a yellow key icon and text: "If you have already purchased a license, please enter activation code:". Below this is a text input field and a button labeled "Activate AKM Antivirus 2010 Pro Now!" (with a green checkmark icon).

In the background, a "You Security Status:" box shows a yellow shield with a black exclamation mark and the text "At Risk" in red, with a link to "Activate Protection".

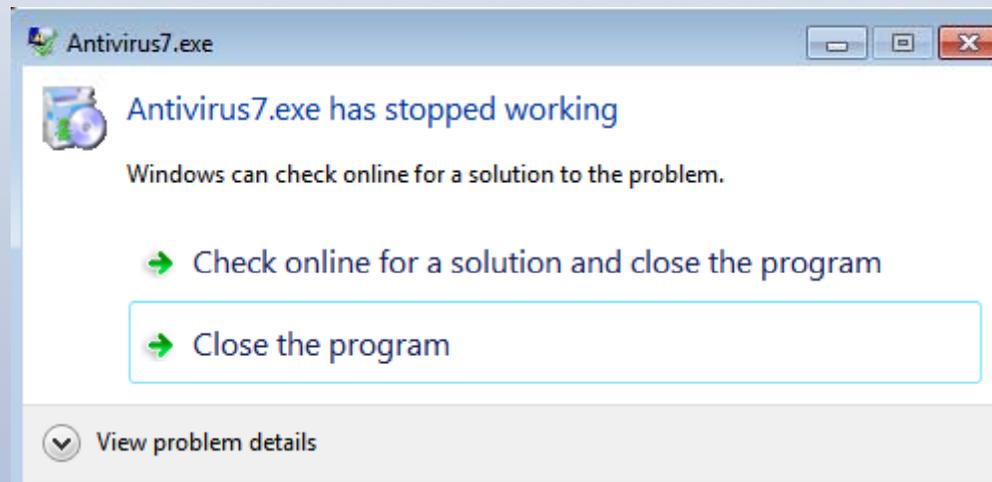
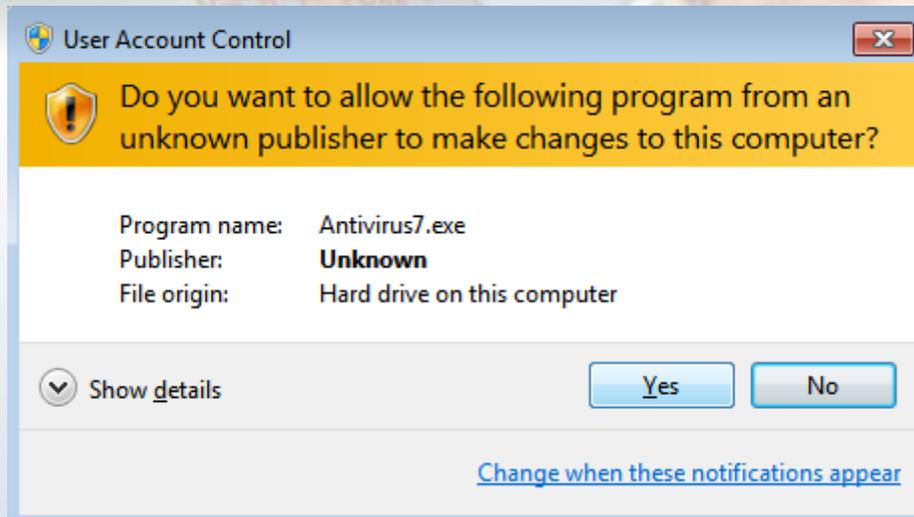
The bottom right of the interface shows a list of detected threats. The first entry is "Trojan.Win32.Agent.azsy" with an alert level of "Medium". The description reads: "This malicious program is a Trojan. It is a Windows Trojan MEDIUM". A "Remove Threats" button is located at the bottom right of the threat list.



Success by Accident

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

...Many are not



Trojans

A close-up photograph of a golden Trojan horse, a symbol of deception, resting on a wooden surface. The horse is intricately carved and has a hollow interior, as evidenced by the shadow cast inside.

- 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 (0x00000000, 0xF73120AE, 0xC0000008, 0xC0000000)

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

SPYWARE.MONSTER.FX_WILD_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:

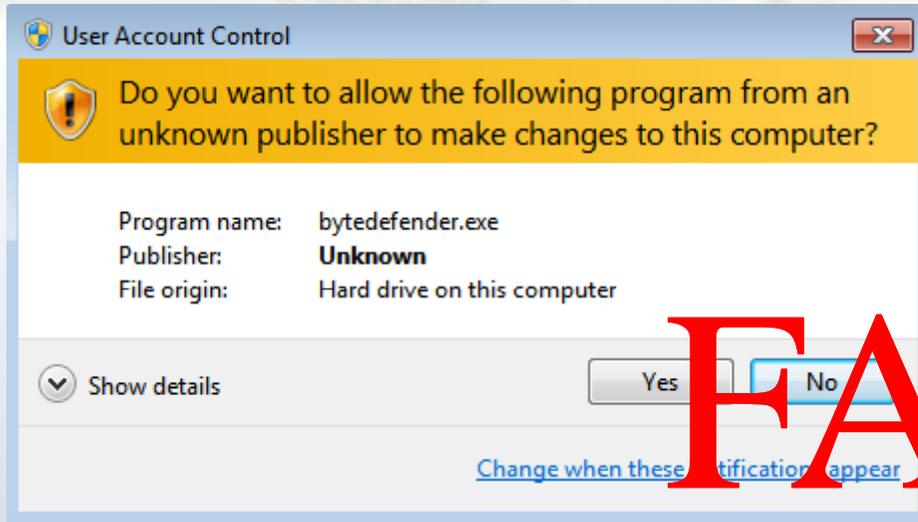
Check to make sure your antivirus software is properly installed. If this is a new installation, ask your software manufacturer for any antivirus updates you might need.

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.

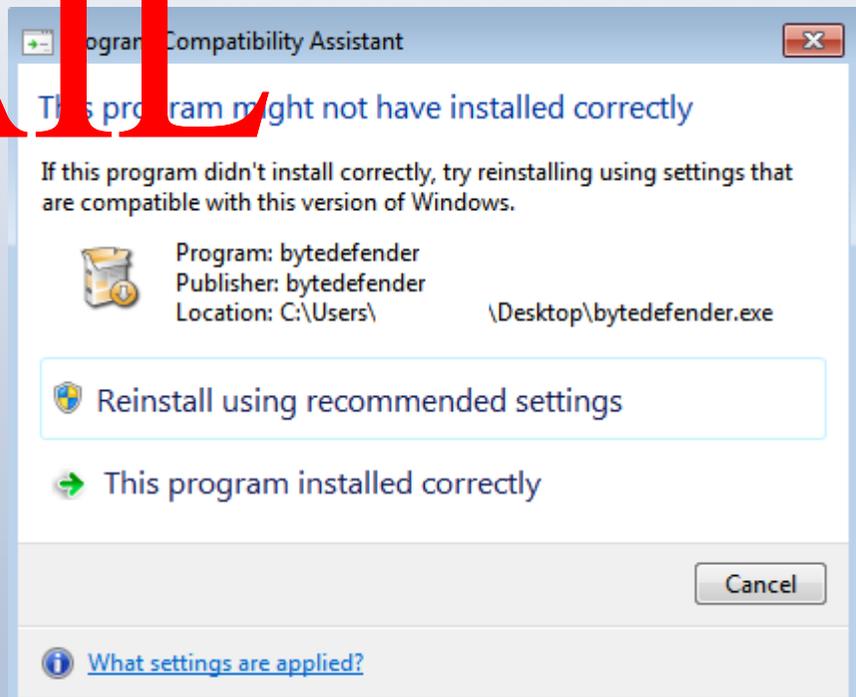
*** SRV.SYS - Address F73120AE base at C0000000, DateStamp 36b072a3
Beginning dump of physical memory...

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.



FAIL



Rogue Test Results

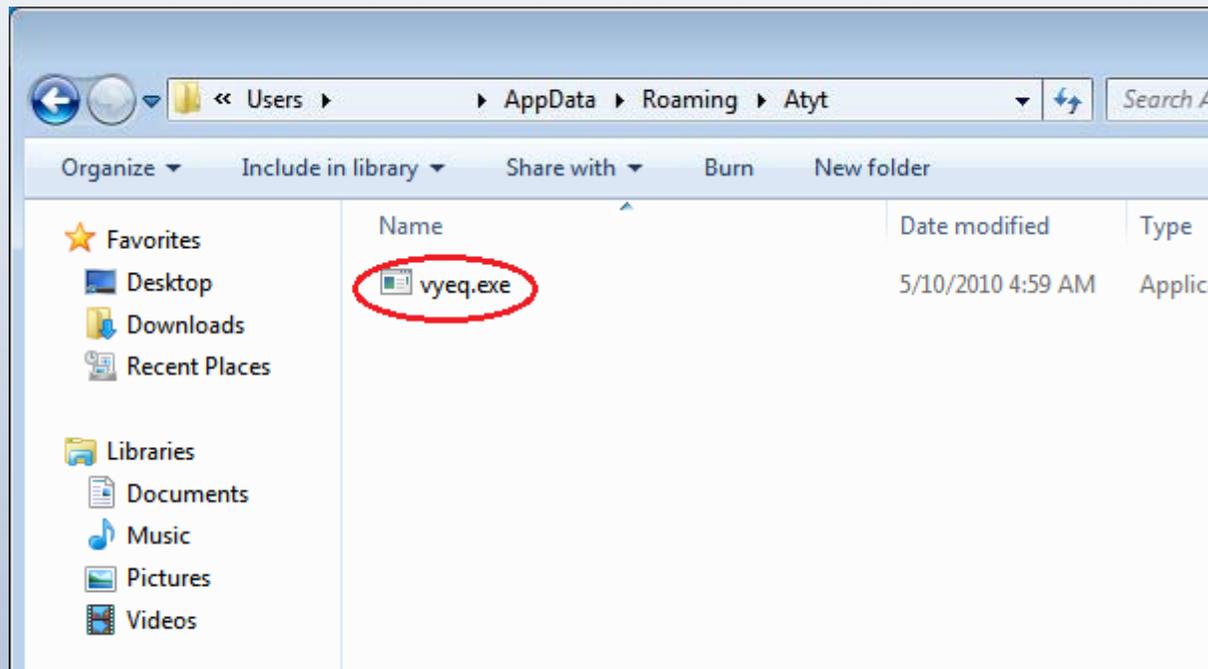
Rogue Anti-virus

Malcode	Result of Installation Attempts
AKM Antivirus 2010	Success: Installed with full functionality
Antivirus Pro	Failed: Triggered UAC prompt.
Antivirus 2010	Partial: Ran initial scare tactics; failed to install.
Antivirus 7	Failed: Triggered UAC and installation failed.
ByteDefender	Failed: Triggered UAC and installation failed.
Digital Protection	Partial: Ran initial scare tactics; failed to install.
Rapid Antivirus	Partial: Ran initial scare tactics; failed to install.
Security Tool	Success: Installed with full functionality
WinPC Antivirus	Failed: Triggered Windows Defender

Zeus – The gold standard of banking Trojans in the underground

– Thwarted initially....

...but then adapted

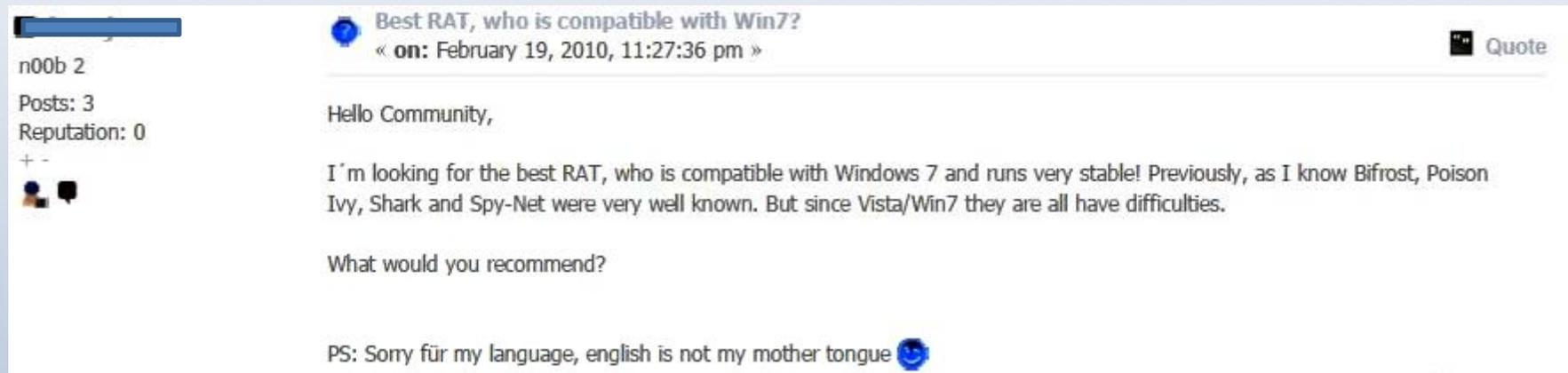


Trojan Test Results

<i>Other Malcode</i>	
Code	Result
Bebloh	Failed: Unable to inject into csrss.exe.
Gumblar	Failed: Unable to access system32 - UAC protected
Mebroot	Failed: Unable to access MBR
Poison Ivy	Failed: Assumed kernel32.dll to be first DLL in list
TDL3	Failed: Unable to access system32 - UAC protected
Spy-Net	Success: Installed with full functionality.
SpyEye	Success: Installed with full functionality.
Zeus	Success: Installed with full functionality. <i>Adapted</i>

Interest in the Underground

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



The screenshot shows a forum post with the following content:

n00b 2
Posts: 3
Reputation: 0

Best RAT, who is compatible with Win7?
« on: February 19, 2010, 11:27:36 pm »

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 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?