iSIGHTPARTNERS℠

Security beyond the edge℠

Windows 7 impact upon rogue security software

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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS℠ Security beyond the edge™

The Transition

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

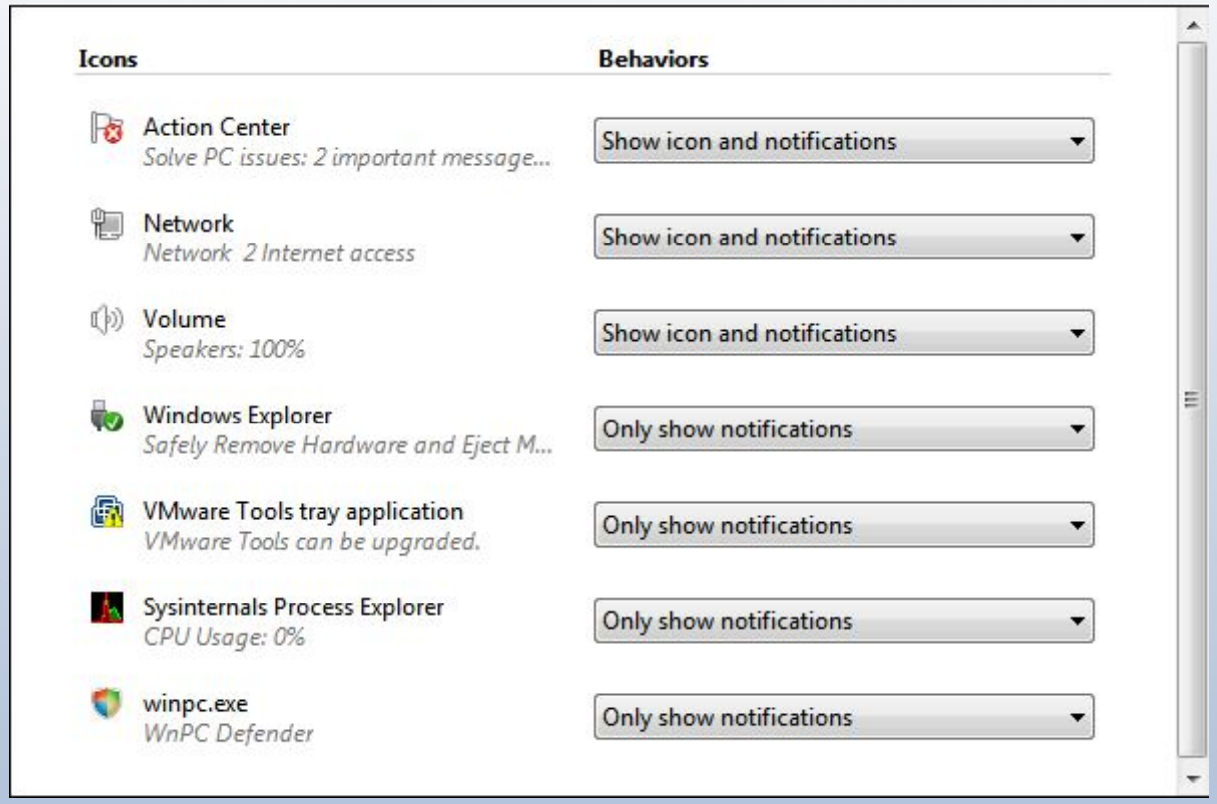
Key Security Features

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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

Notification Area Control Panel

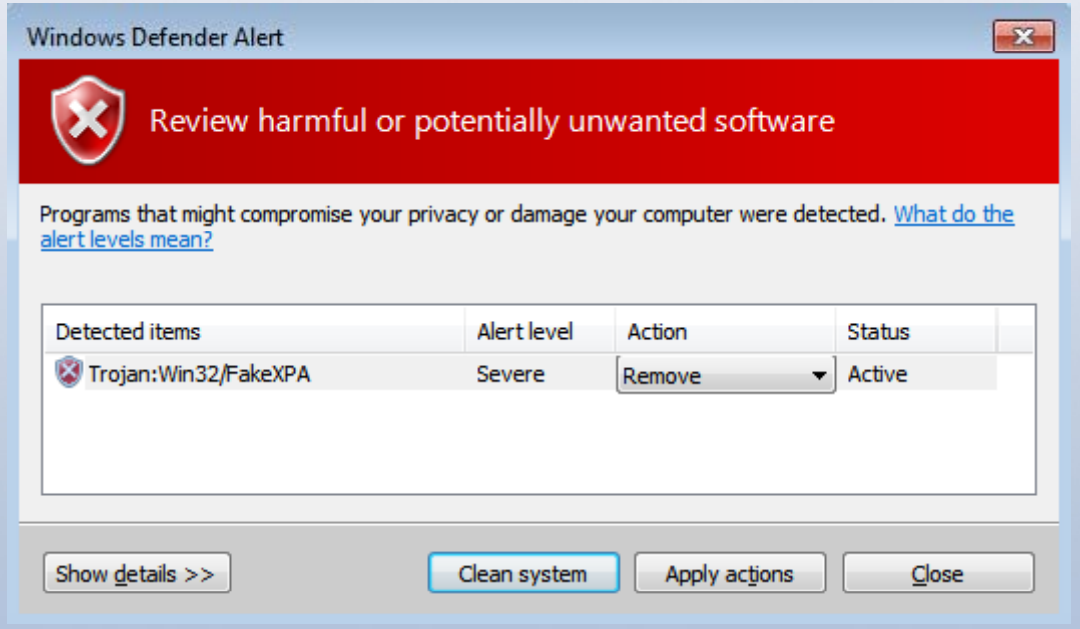
- Allows modification of taskbar icon and notification behavior



Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

Windows Defender

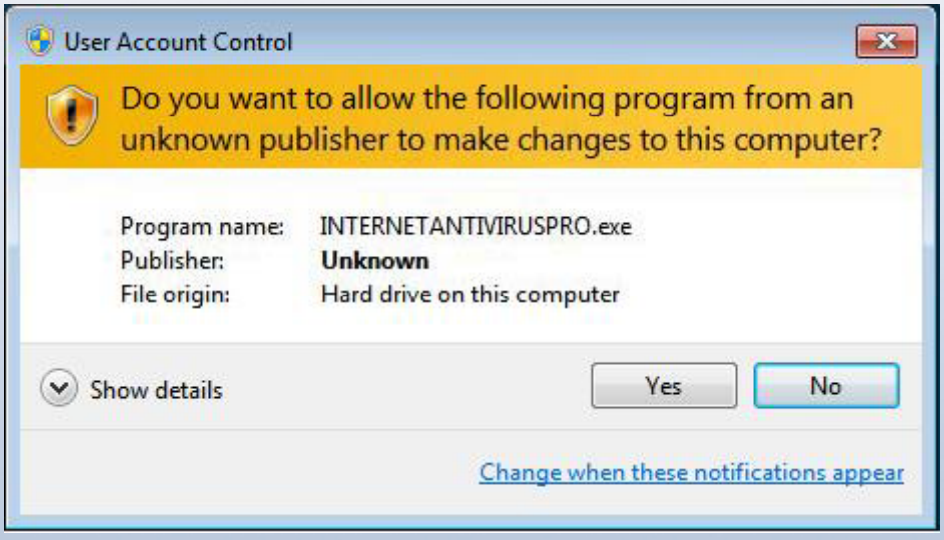
- The included spyware monitoring package for Windows Vista and Windows 7
- Can be disabled or limited by the end user
- Moderately successful at catching malicious code



Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

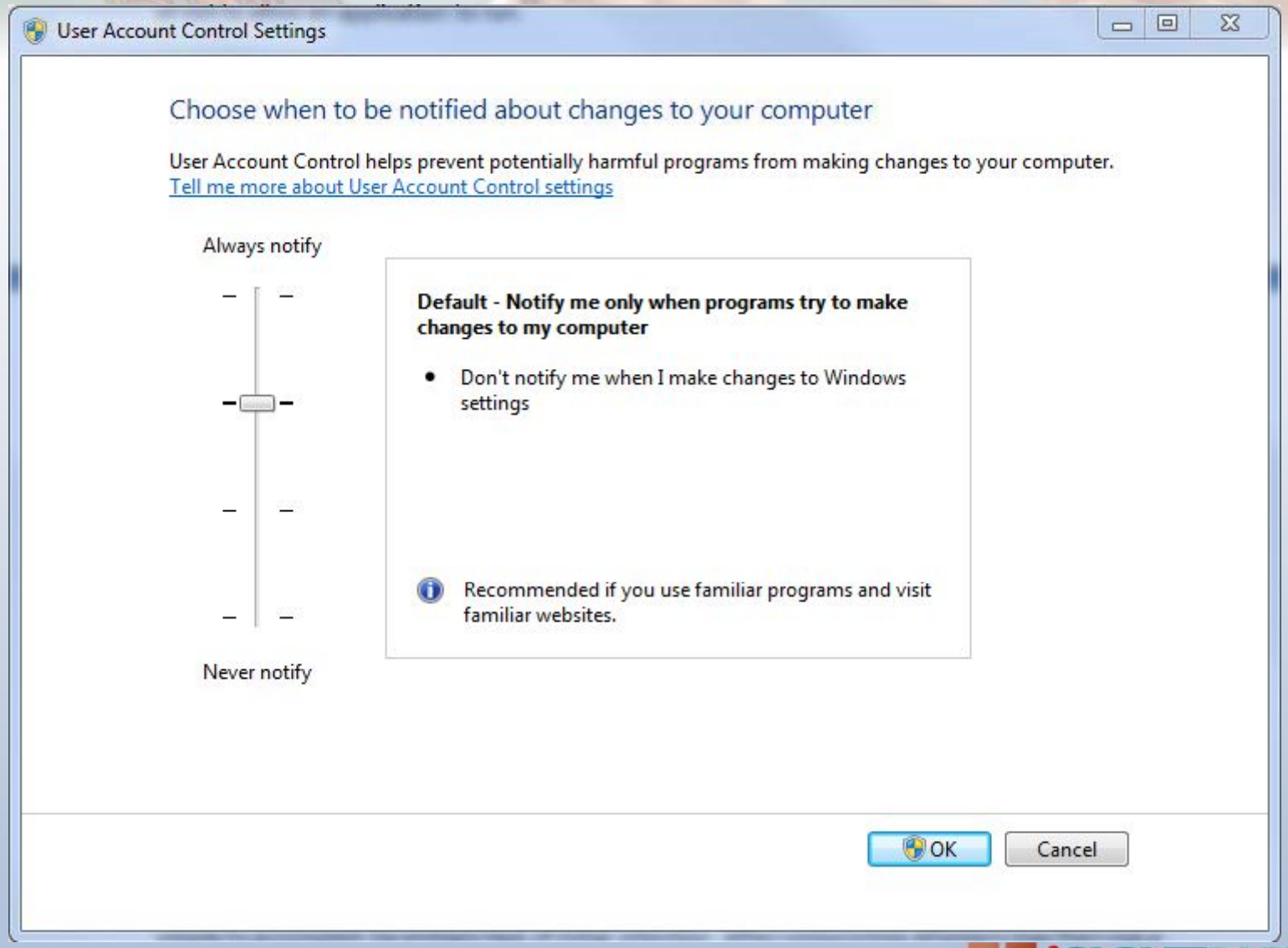
User Account Control (UAC)

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



Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

More Control



Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

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.

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS℠ Security beyond the edge™

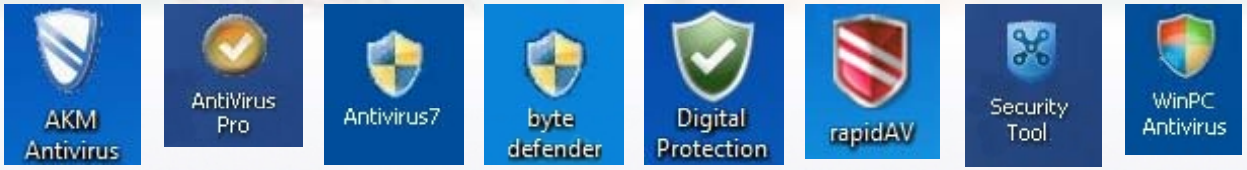
Testing Malcode in Windows 7

- 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.

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS℠ Security beyond the edge™

Rogue AV

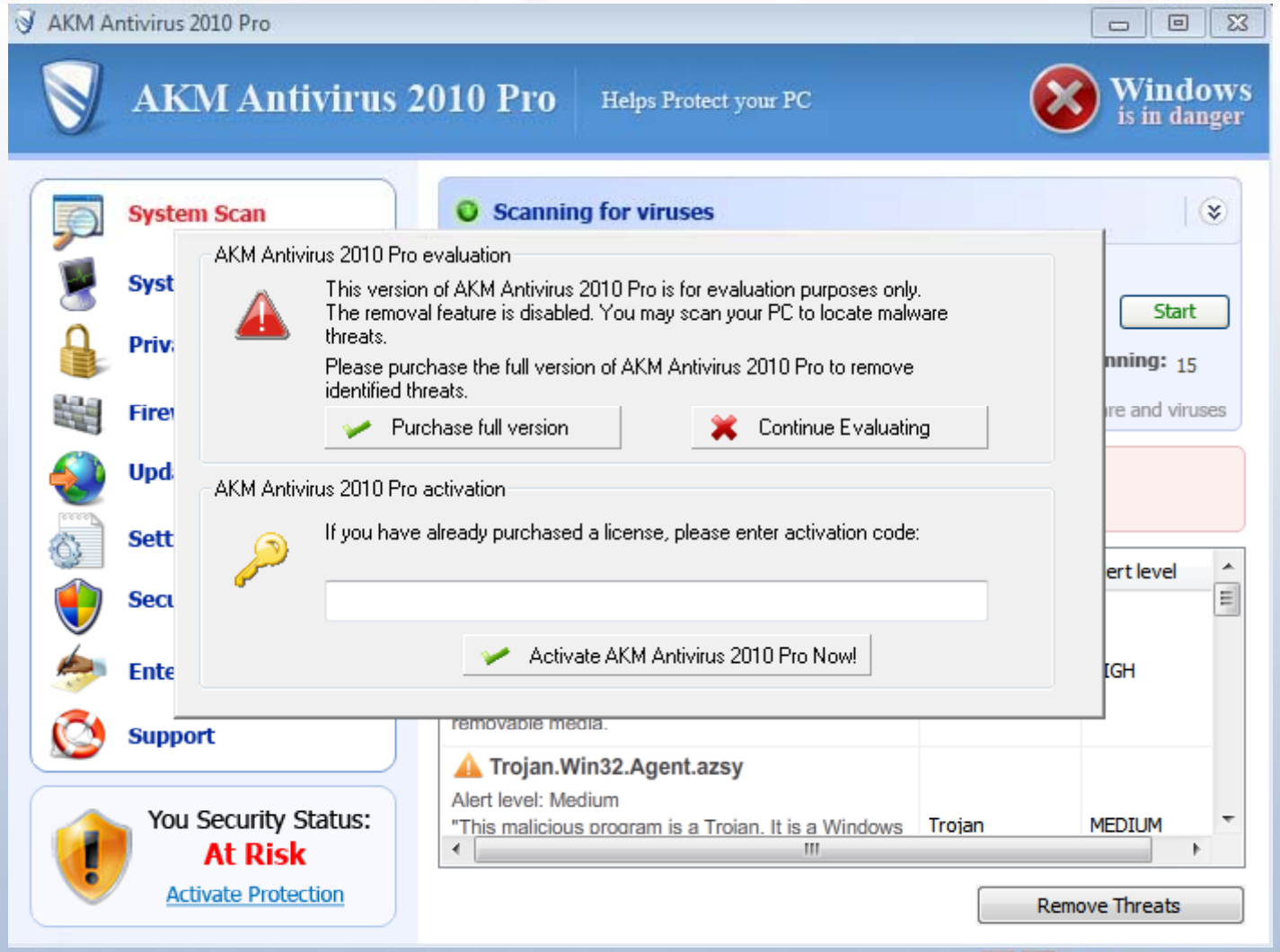


- Designed to intimidate
- Chosen for testing because of:
  - Popularity
  - Potential impact of Windows 7 security features
- Typical attack vector involves online exploitation
- The con artist of the malcode world

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS Security beyond the edge

$59.95 to ease your pain…



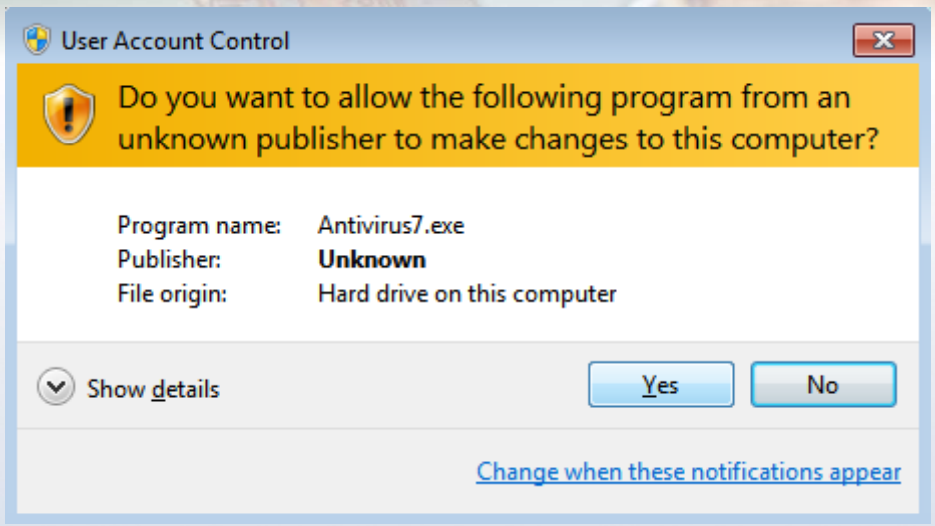
Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

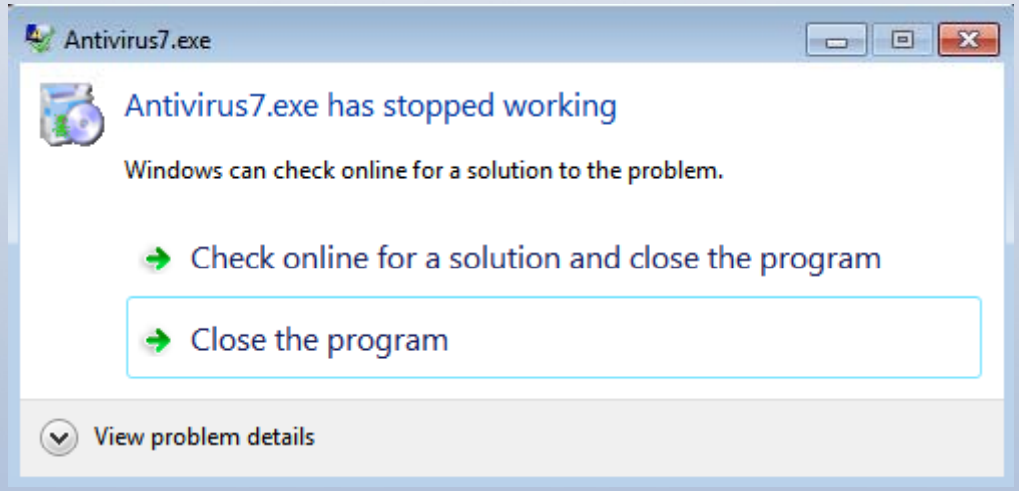
Success by Accident

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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

…Many are not





Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

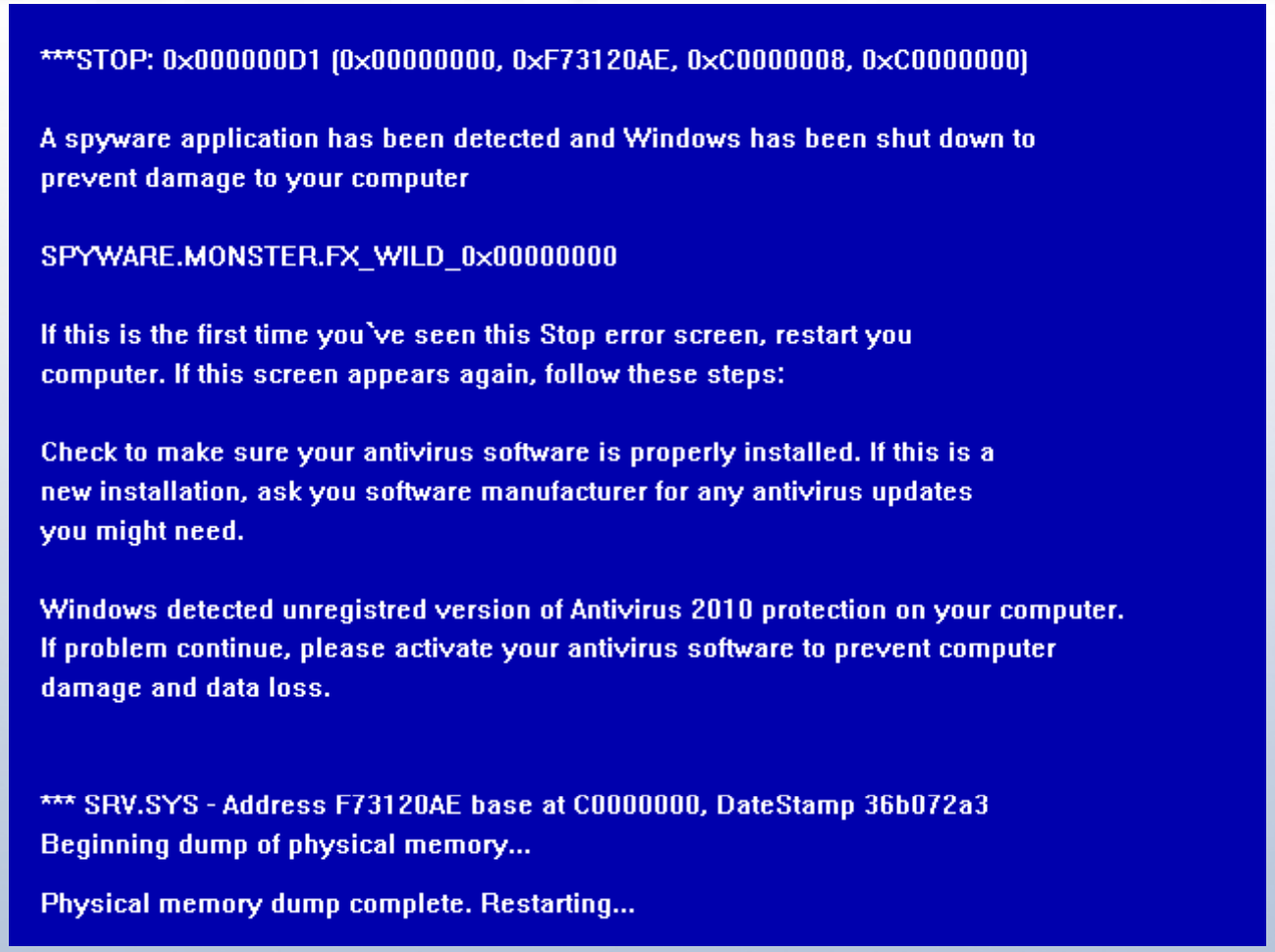
Trojans

- 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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

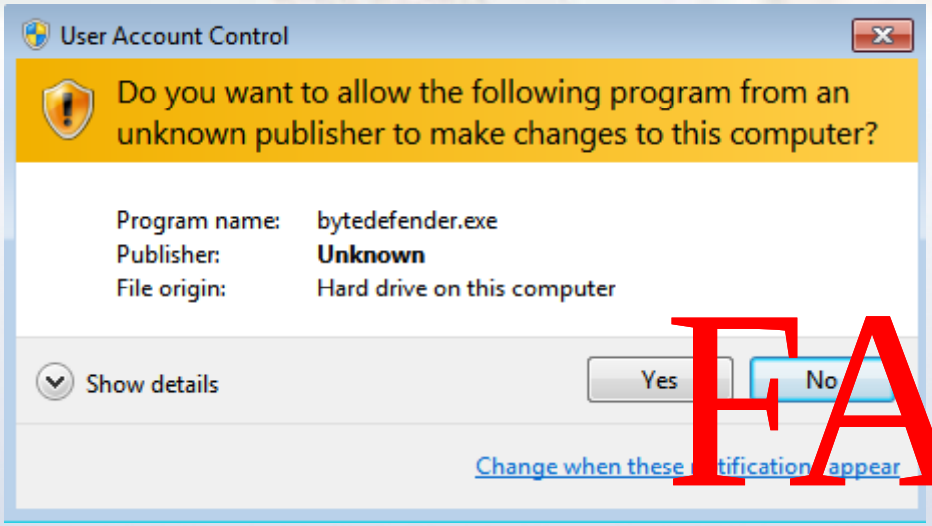
iSIGHTPARTNERS℠ Security beyond the edge™

Antivirus 2010 - Faked a "Blue Screen of Death" and restart, but was detected by Windows Defender following the fake restart

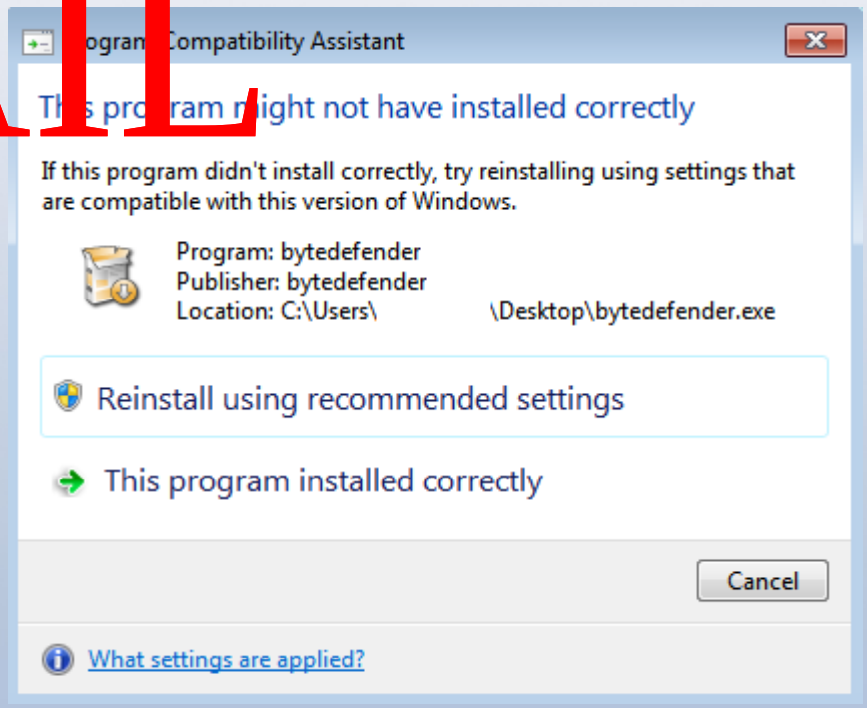


Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

ByteDefender – Generated a UAC prompt and then, even when allowed to run with full admin rights, failed to install altogether.



FAIL



Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

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

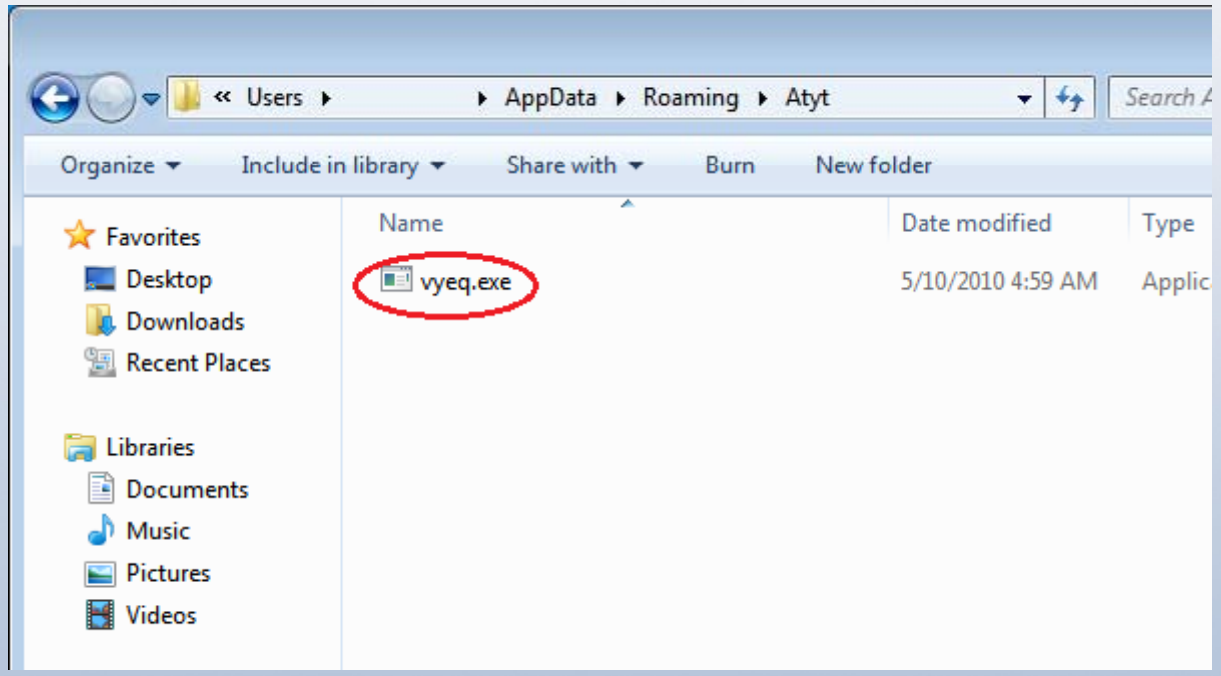
Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS℠ Security beyond the edge™

Zeus – The gold standard of banking Trojans in the underground

– Thwarted initially….

…but then adapted



Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

Trojan Test Results

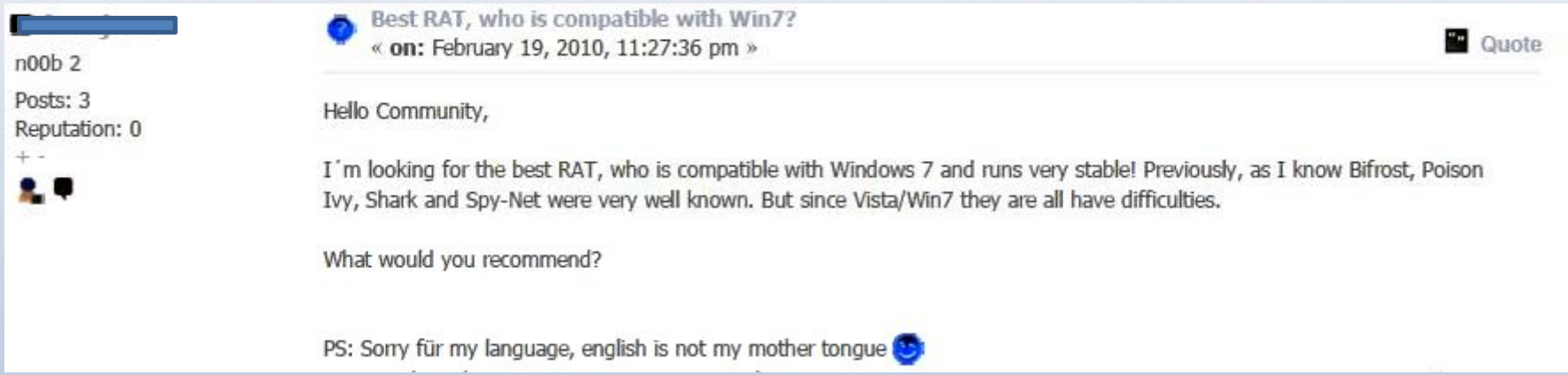
Other Malcode	
Code	**Result**
Bebloh	Failed: Unable to inject into csrss.exe.
Gumblar	Failed: Unable to access system32 - UAC protected
Mebroot	Failed: Unable to access MBR
Poison Ivy	Failed: Assumed kernel32.dll to be first DLL in list
TDL3	Failed: Unable to access system32 - UAC protected
Spy-Net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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS℠ Security beyond the edge™

Interest in the Underground

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



[redacted]
n00b 2
Posts: 3
Reputation: 0
+ -

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

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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS℠ Security beyond the edge™

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

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved

iSIGHTPARTNERS℠ Security beyond the edge™

Questions?

Proprietary and Confidential Information – Copyright© 2010 – All Rights Reserved