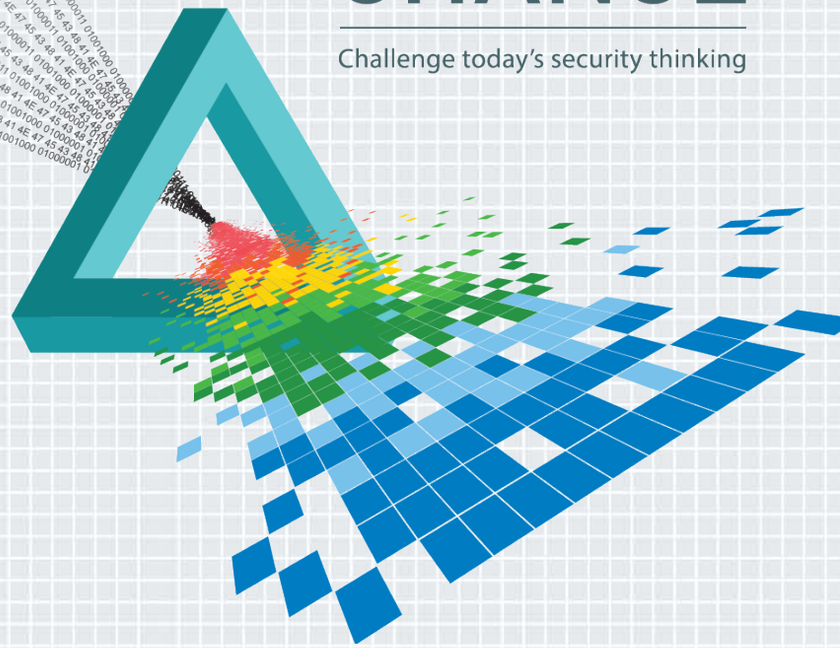
RSAConference2015
San Francisco | April 20-24 | Moscone Center



CHANGE
Challenge today's security thinking

SESSION ID: HTA-T07R

Malware Hunting with the Sysinternals Tools

Mark Russinovich

CTO, Microsoft Azure
Microsoft
@markrussinovich

THE WALL STREET JOURNAL. | TECH

TECHNOLOGY

Symantec Develops New Attack on Cyberhac

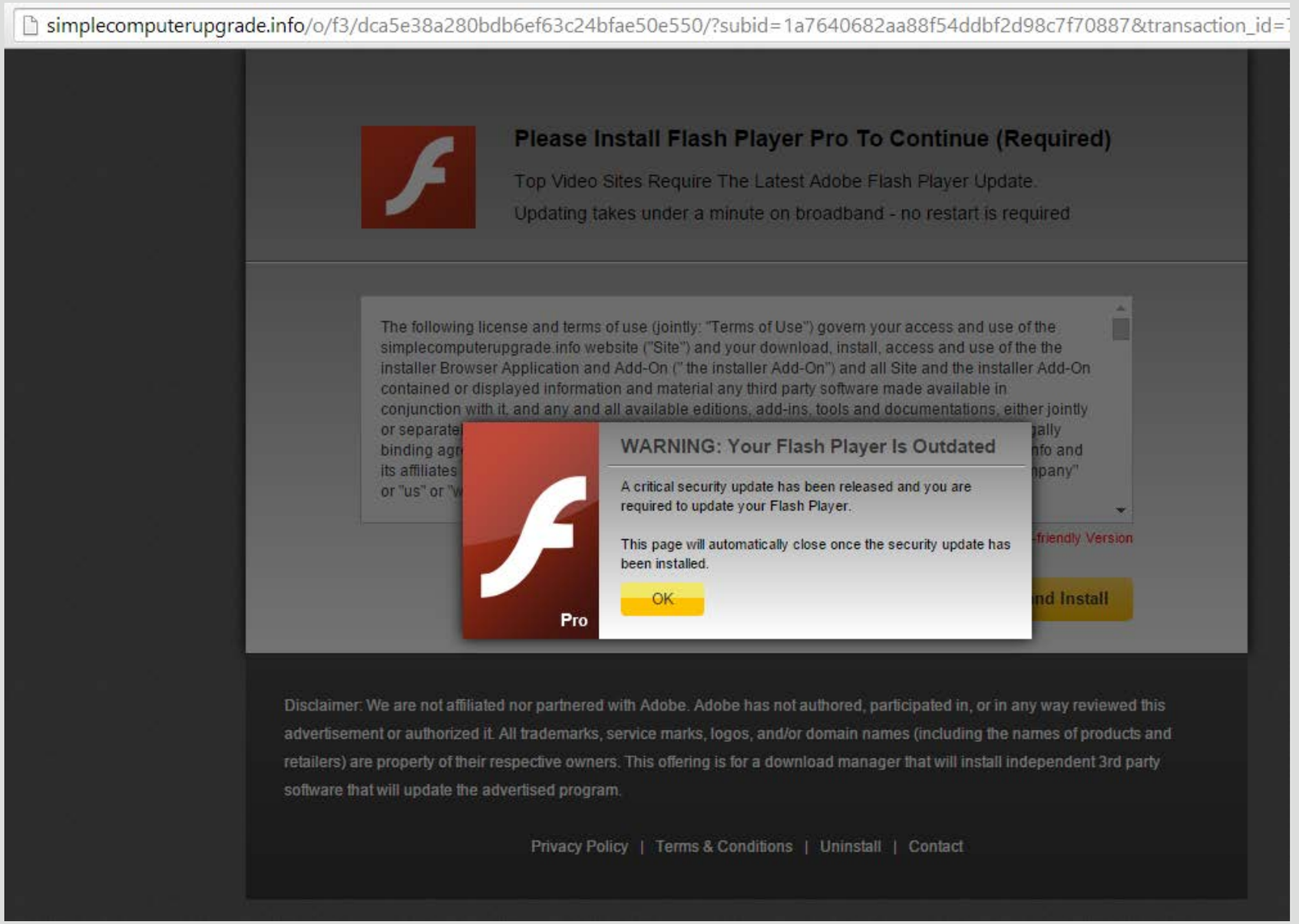
Declaring Antivirus Software Dead, Firm Turns to Minimizing Damage Fro

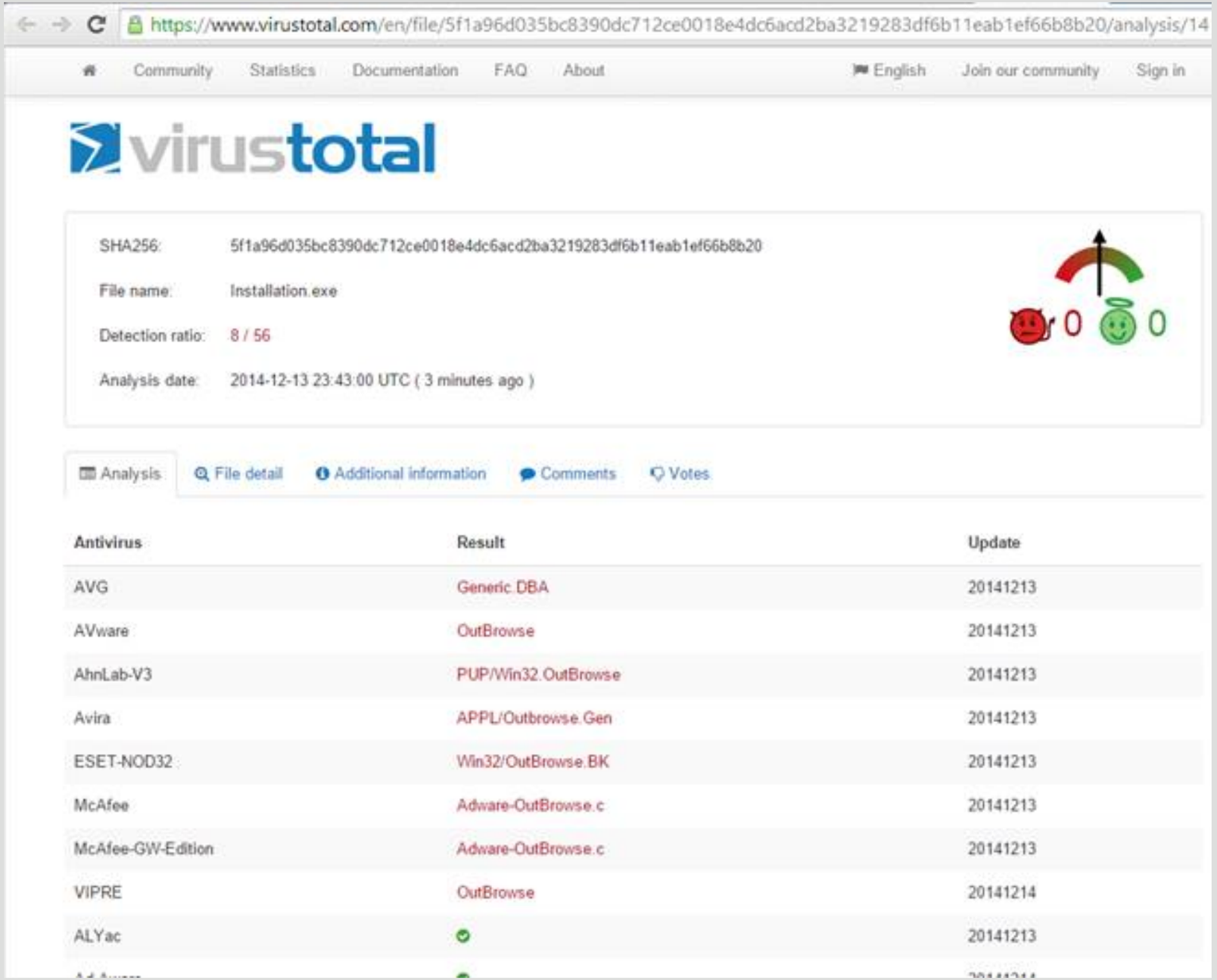
By DANNY YADRON CONNECT

Updated May 4, 2014 10:41 p.m. ET

Symantec Corp. invented commercial antivirus software to protect computers from hackers a quarter-century ago. Now the company says such tactics are doomed to failure.

Antivirus "is dead," says Brian Dye, Symantec's senior vice president for information security. "We don't think of antivirus as a moneymaker in any way."


simplecomputerupgrade.info/o/f3/dca5e38a280bdb6ef63c24bfae50e550/?subid=1a7640682aa88f54ddbf2d98c7f70887&transaction_id=
Please Install Flash Player Pro To Continue (Required)
Top Video Sites Require The Latest Adobe Flash Player Update.
Updating takes under a minute on broadband - no restart is required
The following license and terms of use (jointly: "Terms of Use") govern your access and use of the simplecomputerupgrade.info website ("Site") and your download, install, access and use of the the installer Browser Application and Add-On (" the installer Add-On") and all Site and the installer Add-On contained or displayed information and material any third party software made available in conjunction with it, and any and all available editions, add-ins, tools and documentations, either jointly
WARNING: Your Flash Player Is Outdated
A critical security update has been released and you are required to update your Flash Player.
This page will automatically close once the security update has been installed.
OK
Pro
Disclaimer: We are not affiliated nor partnered with Adobe. Adobe has not authored, participated in, or in any way reviewed this advertisement or authorized it. All trademarks, service marks, logos, and/or domain names (including the names of products and retailers) are property of their respective owners. This offering is for a download manager that will install independent 3rd party software that will update the advertised program.
Privacy Policy | Terms & Conditions | Uninstall | Contact


https://www.virustotal.com/en/file/5f1a96d035bc8390dc712ce0018e4dc6acd2ba3219283df6b11eab1ef66b8b20/analysis/14
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal
SHA256: 5f1a96d035bc8390dc712ce0018e4dc6acd2ba3219283df6b11eab1ef66b8b20
File name: Installation.exe
Detection ratio: 8 / 56
Analysis date: 2014-12-13 23:43:00 UTC (3 minutes ago)
0
0
Analysis
File detail
Additional information
Comments
Votes
Antivirus
Result
Update
AVG
Generic.DBA
20141213
AVware
OutBrowse
20141213
AhnLab-V3
PUP/Win32.OutBrowse
20141213
Avira
APPL/Outbrowse.Gen
20141213
ESET-NOD32
Win32/OutBrowse.BK
20141213
McAfee
Adware-OutBrowse.c
20141213
McAfee-GW-Edition
Adware-OutBrowse.c
20141213
VIPRE
OutBrowse
20141214
ALYac
20141213

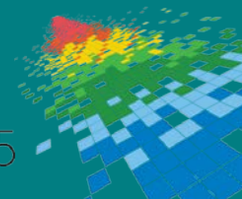
About this Talk

- Learn about Sysinternals tools and techniques for analyzing and cleaning malware
  - Professional antimalware analysis requires years of deep training
  - But even for professionals, Sysinternals tools can prove useful
- Analyzing:
  - Understanding the impact of malware
  - Can be used to understand malware operation
  - Generates road map for cleaning infestations
- Cleaning:
  - Removing an infestation of a compromised system
  - Attempting a clean can also reveal more information about malware's operation

Malware Cleaning Steps

- Disconnect from network
- Identify malicious processes and drivers
- Terminate identified processes
- Identify and delete malware autostarts
- Delete malware files
- Reboot and repeat

Identifying Malware Processes

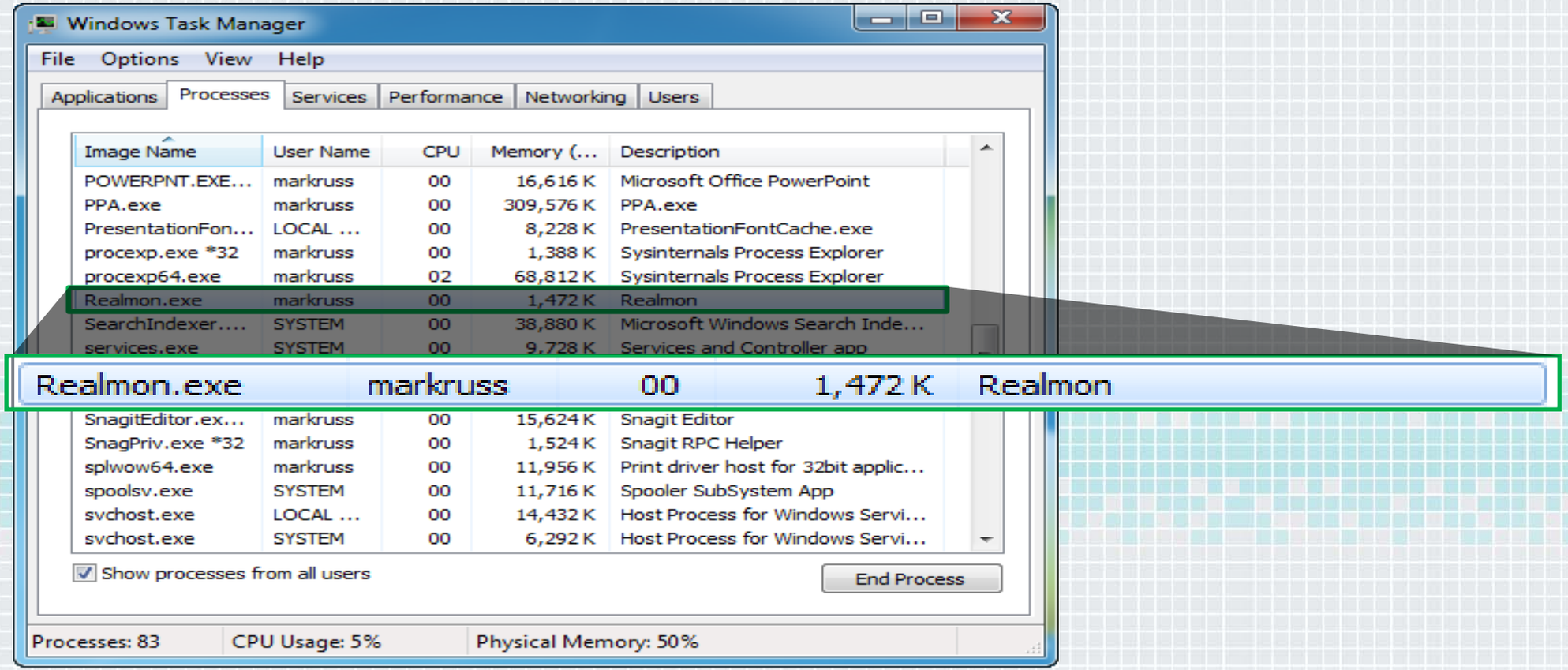


What Are You Looking For?

- Investigate processes that…
- …have no icon
- …have no description or company name
- …unsigned Microsoft images
- …live in Windows directory or user profile
- …are packed
- …include strange URLs in their strings
- …have open TCP/IP endpoints
- …host suspicious DLLs or services

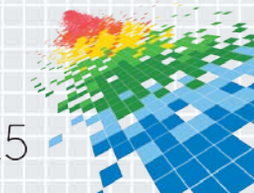
What About Task Manager?

- Task Manager provides little information about images that are running



Process Explorer

- Process Explorer is “Super Task Manager”
- Has lots of general troubleshooting capabilities:
  - DLL versioning problems
  - Handle leaks and locked files
  - Performance troubleshooting
  - Hung processes
- We’re going to focus on its malware cleaning capabilities



The Process View

- The process tree shows parent-child relationships
- Icon, description, and company name are pulled from image version information
  - Most malware doesn't have version information
  - What about malware pretending to be from Microsoft?
    - We'll deal with that shortly…
- Use the Window Finder (in the toolbar) to associate a window with its owning process
- Use the Search Online menu entry to lookup unknown processes
  - But malware often uses totally random or pseudo-random names

Refresh Highlighting

- Refresh highlighting highlights changes
  - Red: process exited
  - Green: new process
- Change duration (default 1 second) in Options
- Press space bar to pause and F5 to refresh
- Cause display to scroll to make new processes visible with Show New Processes option
- We'll see how to spot short-lived processes later…

Process-type Highlights

- Blue processes are running in the same security context as Process Explorer
- Pink processes host Windows services
- Purple highlighting indicates an image is “packed”
  - Packed can mean compressed or encrypted
  - Malware commonly uses packing (e.g. UPX) to make antivirus signature matching more difficult
  - Packing and encryption also hide strings from view
- There are a few other colors, but they’re not important for malware hunting

Tooltips

- Process tooltips show the full path to the process image
- Malware more often hides behind Svchost, Rundll32, Dllhost and WMIPrsve
  - Tooltip for Rundll32 processes shows hosted DLL
  - Dllhost tooltip shows hosted COM server
  - WMI provider tooltip shows WMI servers
  - Tooltip for service processes shows hosted services

Detailed Process Information

- Double-click on a process to see more information
- Pages relevant to malware analysis:
  - Image: signing status, start time, version, autostart location
  - TCP/IP: open endpoints
  - Strings: printable strings in main executable

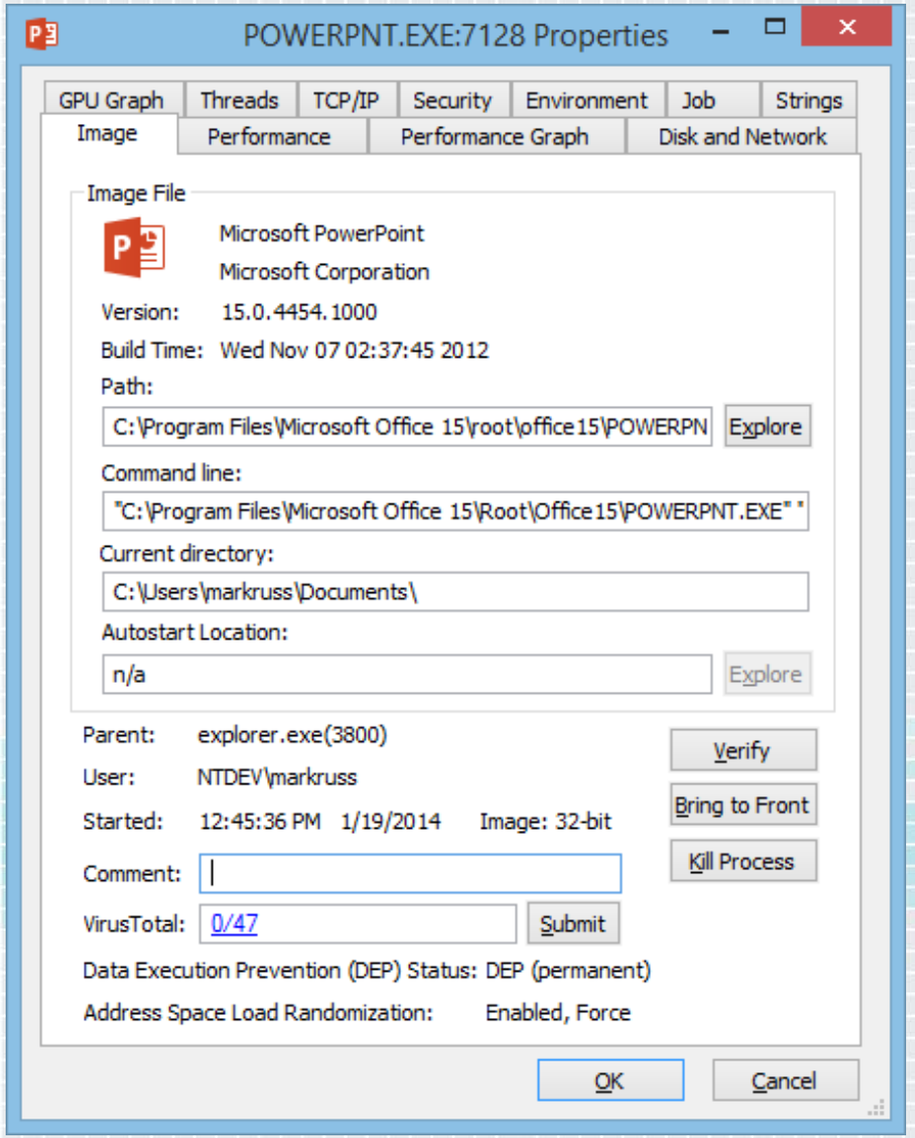
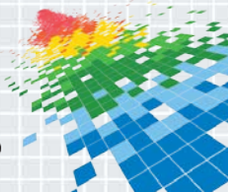


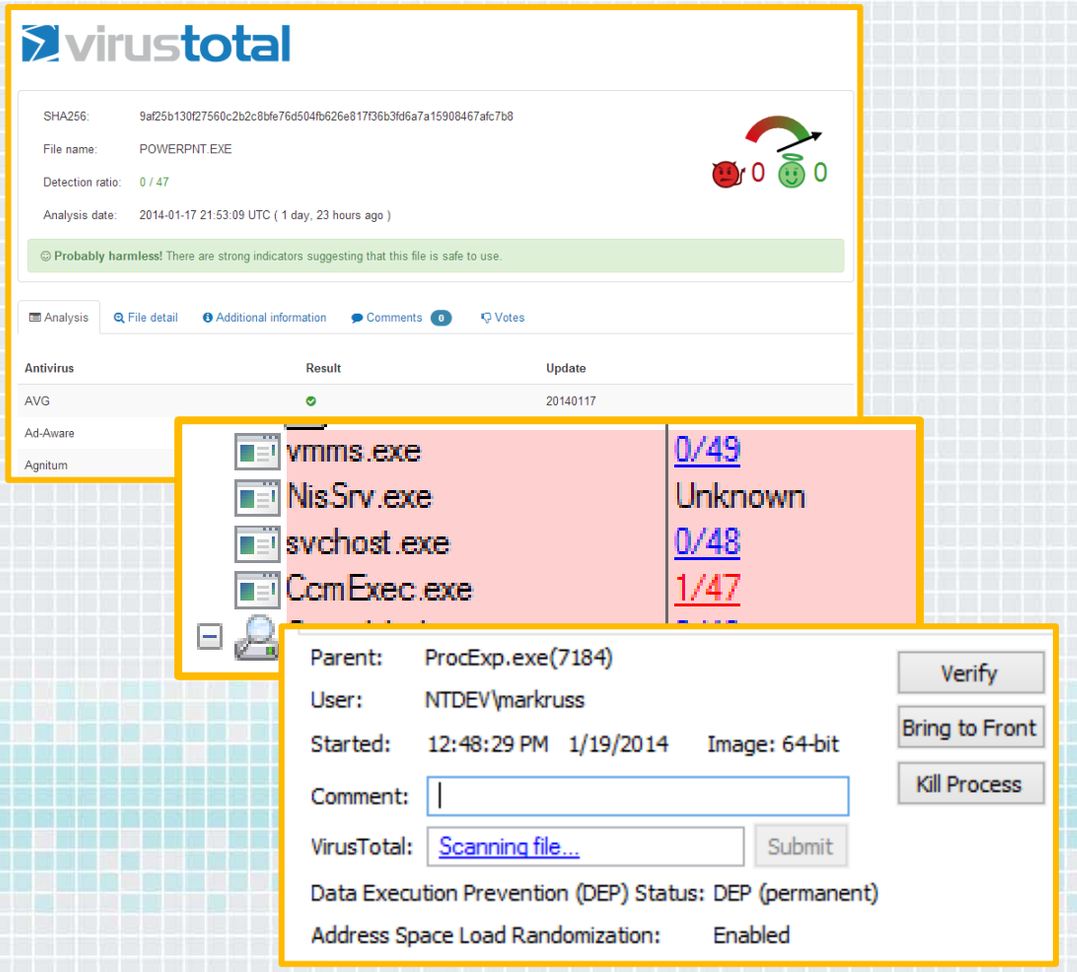
Image Verification

- All (well, most) Microsoft code is digitally signed
  - Hash of file is signed with Microsoft's private key
  - Signature is checked by decrypting signed hash with the public key
- You can selectively check for signatures with the Verify button on the process image tab
  - Select the Verify Image Signatures option to check all
  - Add the Verified Signer column to see all
- Note that verification will connect to the Internet to check Certificate Revocation List (CRL) servers



VirusTotal Integration

- VirusTotal.com is Antivirus-as-a-Service (AaaS)
- You can have Process Explorer check file hashes
  - Check all displayed files with Options->Check VirusTotal
  - Results reported in VirusTotal column as well as DLL and process properties
  - Uploads hashes
  - Reports results as positive detection rate or “Unknown”
- You can submit unknown files for scanning
  - Options->Submit Unknown Executables submits all portable executable (PE) images < 32 MB in size
  - Can submit on-demand with context menu or properties dialog



Sigcheck

- Scan the system for suspicious executable images

```
sigcheck -e –vs -vr -u -s c:\
```

- Use –v to check VirusTotal:
  - -v to submit hashes (-vs to submit files for scanning)
  - -vr to open the VirusTotal report
- Look for same characteristics as suspicious processes
  - Be especially wary of items in the \Windows directory and the \Users\<username>\Appdata directories
  - Investigate all unsigned images
  - Examine images with high entropy (> 7)

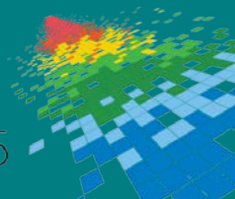
The DLL View

- Malware can hide as a DLL inside a legitimate process
  - We've already seen this with Rundll32 and Svchost
  - Typically loads via an autostart
  - Can load through "dll injection"
  - Packing highlight shows in DLL view as well
- Open the DLL view by clicking on the DLL icon in the toolbar
  - Shows more than just loaded DLLs
  - Includes .EXE and any "memory mapped files"
- Can search for a DLL with the Find dialog
- DLL strings are also viewable on the DLL properties

Terminating Malicious Processes

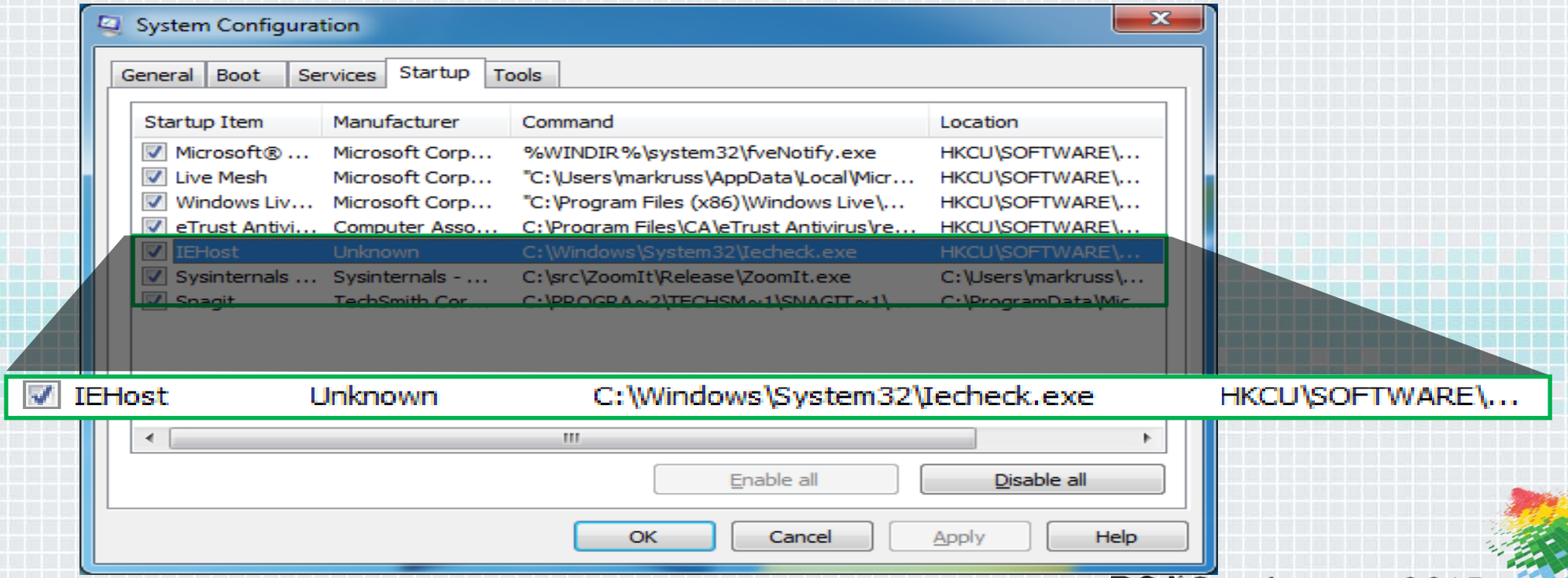
- Don’t kill the processes
  - Malware processes are often restarted by watchdogs
- Instead, suspend them
  - Note that this might cause a system hang for Svchost processes
  - Record the full path to each malicious EXE and DLL
- After they are all asleep then kill them
  - Watch for restarts with new names…

Cleaning Autostarts



Investigating Autostarts

- Windows Msconfig (Start->Run->Msconfig) falls short
  - It knows about few locations
  - It provides little information



Autoruns

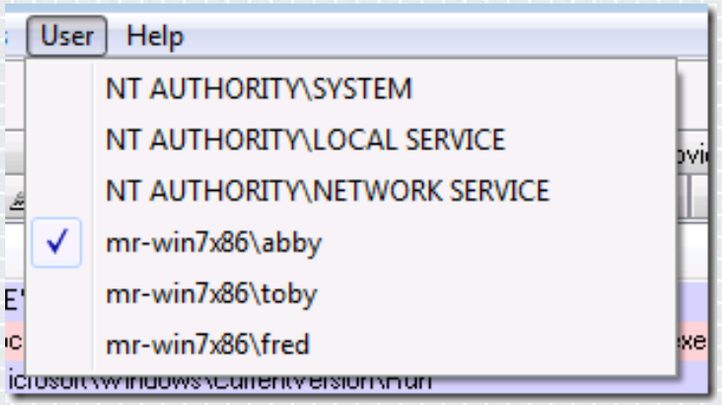
- Shows every place in the system that can be configured to run something at boot & logon
  - Standard Run keys and Startup folders
  - Shell, userinit
  - Services and drivers
  - Tasks
  - Winlogon notifications
  - Explorer and IE addins (toolbars, Browser Helper Objects, …)
  - More and ever growing…
- Each startup category has its own tab and all items display on the Everything tab
  - Startup name, image description, company and path

Identifying Malware Autostarts

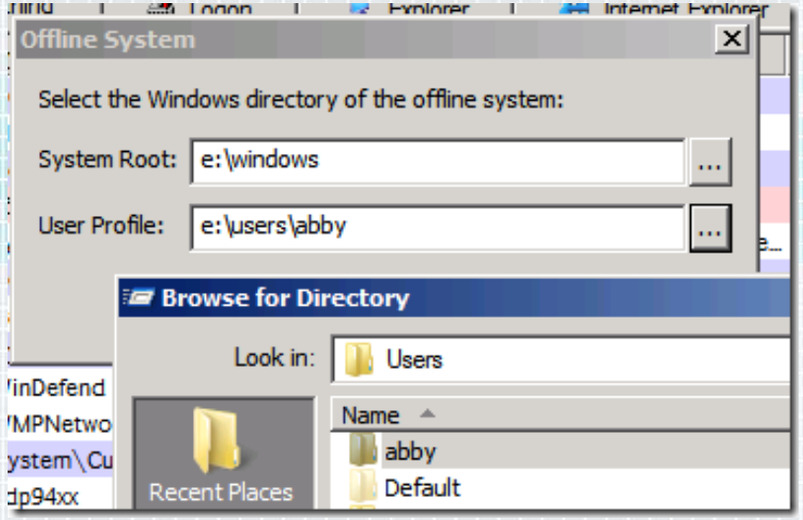
- Zoom-in on add-ons (including malware) by selecting these filter options:
  - Verify Code Signatures
  - Hide Microsoft Entries
- Select an item to see more in the lower window
  - Online search unknown images
  - Double-click on an item to look at where its configured in the Registry or file system
- Has other features:
  - Can also show empty locations (informational only)
  - Includes compare functionality
  - Includes equivalent command-line version, Autorunsc.exe

Alternate Profiles and Offline Scanning

- If a specific account is infected, you can use Autoruns from another:

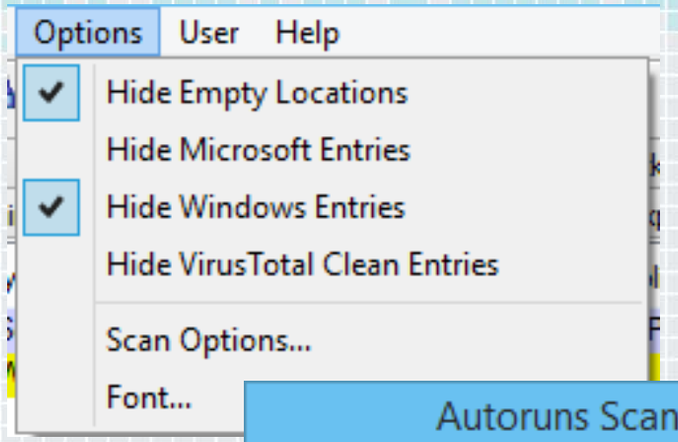


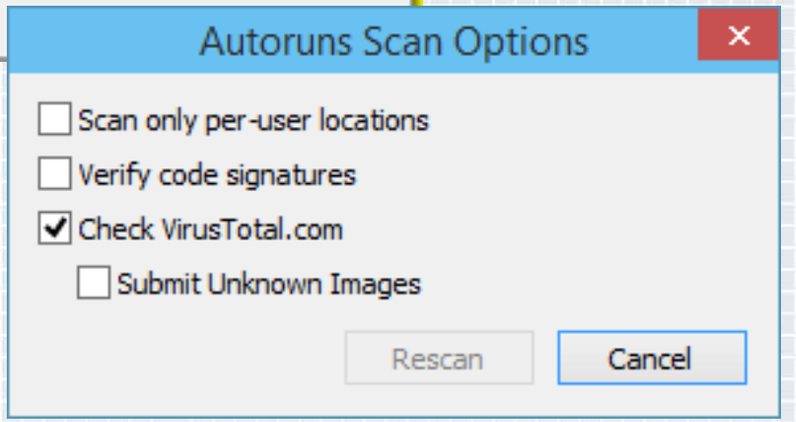
- If the system can't be cleaned online, Autoruns can be used offline:

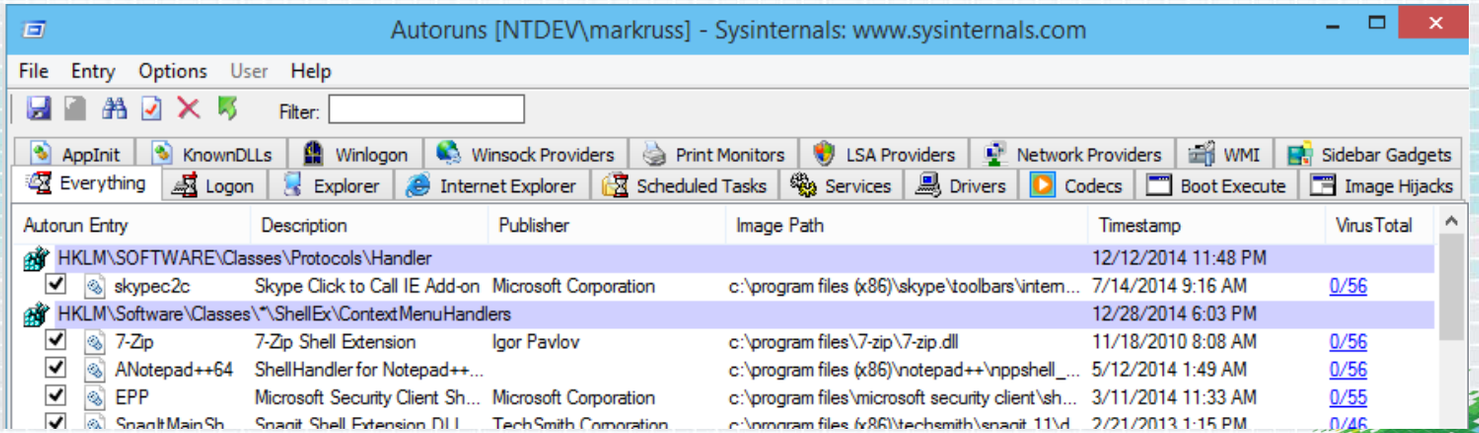


New: Autoruns v13

- Dynamic filtering
- More detailed progress updates
- Full scan save-to-file
- File compare deleted/new
- VirusTotal Integration
  - You can have Autoruns check VirusTotal for hashes
  - Option to submit files for scanning



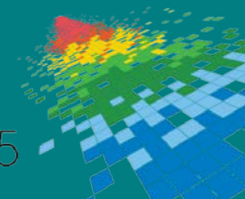




Deleting Autostarts

- Delete suspicious autostarts
  - You can disable them if you're not sure
- After you're done do a full refresh
- If they come back, run Process Monitor to see who's putting them back
  - You might have misidentified a malware process
  - It might be a hidden, system, or legitimate process

Tracing Malware Activity



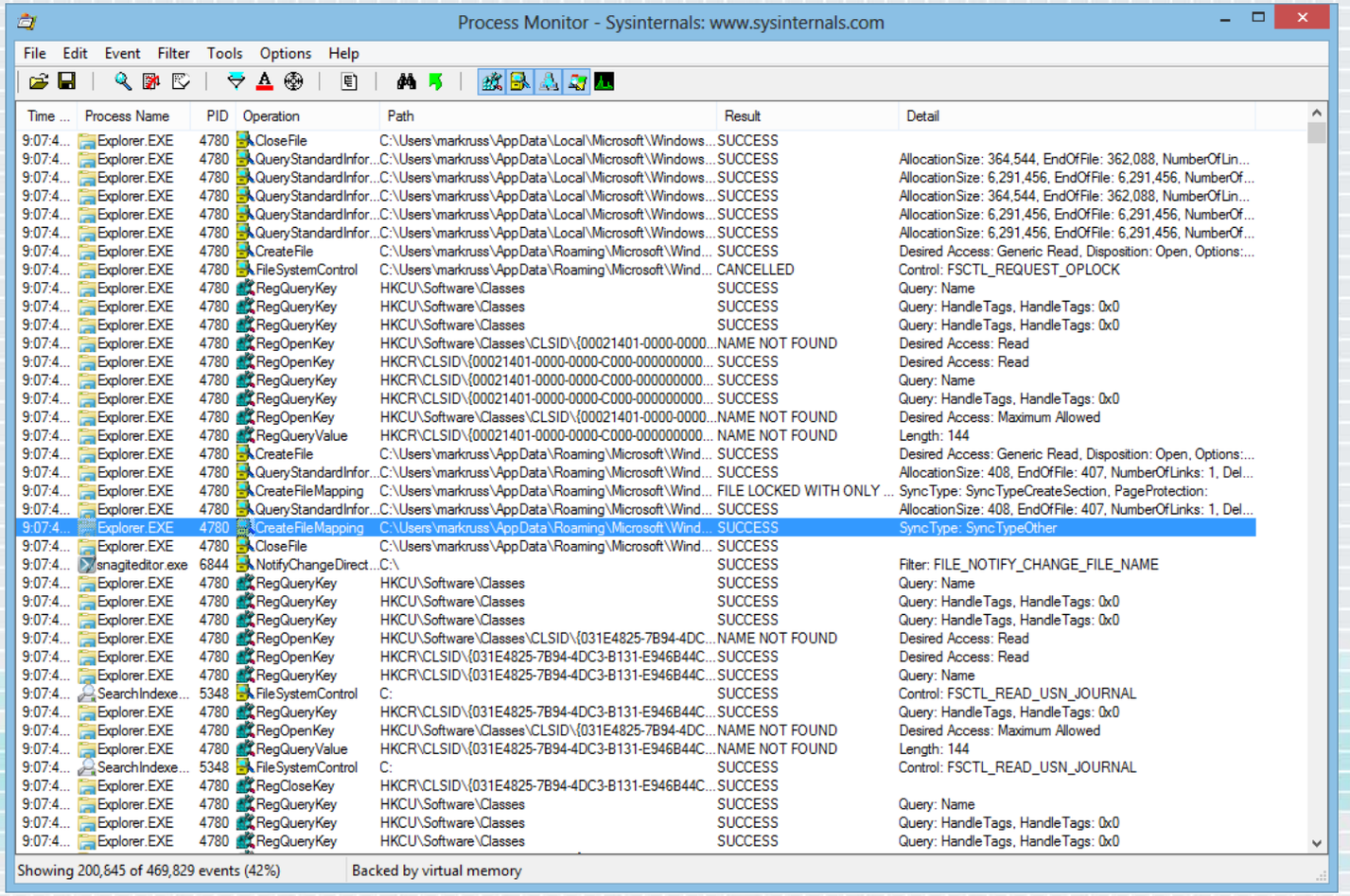
Tracing Malware

- Tracing activity can reveal the system impact of malware
  - Tracing shows initial infection, before cloaking is applied
  - Can reveal the internals of “buddy system” and other infection-protection mechanisms
- Process Monitor makes tracing easy
  - A simple filter can identify all system modifications
  - Investigating stacks can distinguish legitimate activity from malicious activity
  - It will often show you the cause for error messages
  - It many times tells you what is causing sluggish performance

When in doubt, run Process Monitor!

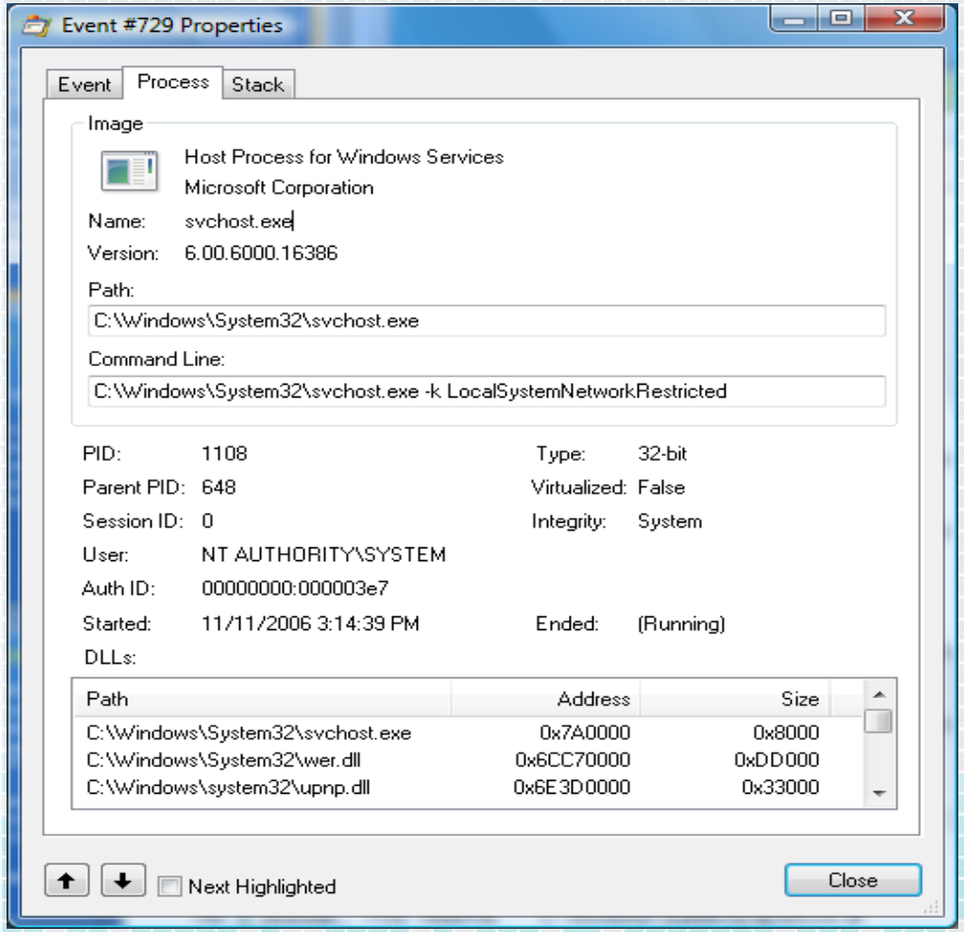
Event Classes

- File system (Filemon)
  - Includes I/O command input and output details
- Registry (Regmon)
  - Includes all data
- Process
  - Process create and exit
  - Thread create and exit
  - Image loads, including drivers
- Network
  - ETW network tracing
- Profiling
  - Thread stack snapshots



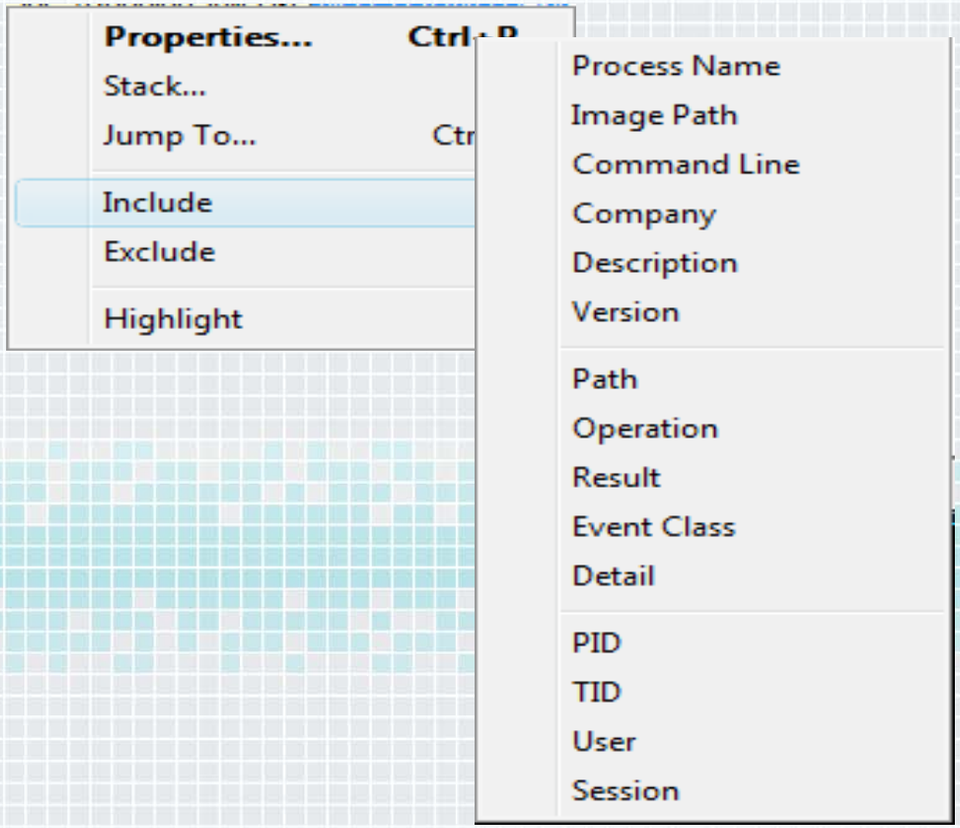
Event Properties

- Event details
  - Duration, process, thread, details, etc.
- Process information
  - Command line
  - User
  - Session and logon session
  - Image information
  - Start time
- Thread stack at time of event



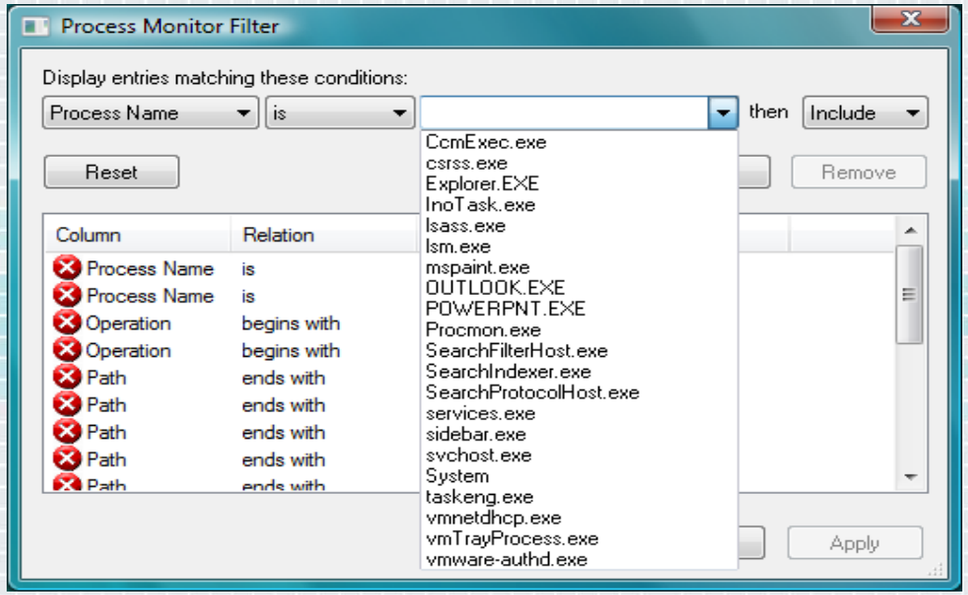
Filtering

- To filter on a value, right-click on the line and select the attribute from the Include, Exclude or Highlight submenus
- When you set a highlight filter you can move through highlighted event properties



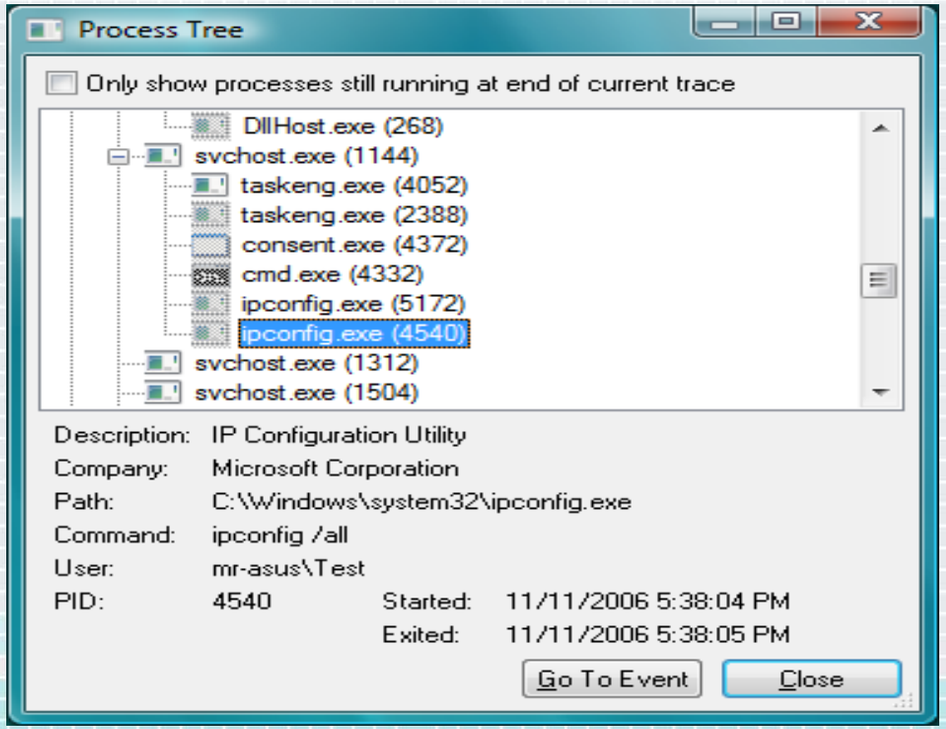
Advanced Filters

- Multiple-filter behavior:
  - Values from different attributes are AND'd
  - Values for the same attribute are OR'd
- Use Edit Filter context menu for quick configuration
- More complex filtering is available in the Filter dialog
  - Outlook-style rule definition
- You can save and restore filters
- Filter for watching malware impact:
  "Category is Write"

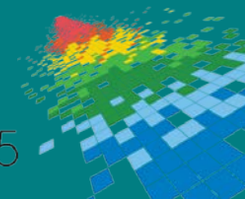


The Process Tree

- Tools->Process Tree
  - Shows all processes that have been seen in the trace (including parents)
  - Can toggle on and off terminated processes
- The process tree provides an easy way to see process relationships
  - Short-lived processes
  - Command lines
  - User names



Malware Forensics



System Monitor (Sysmon)

- Background system monitoring utility
  - Record system events to the Windows event log
  - Can be used for system anomaly detection
  - Forensics can trace intruder activity across the network
- Written for use in Microsoft corporate network
  - To understand attacker behavior and tools
  - Significant contributions by Thomas Garnier
  - Public version has reduced functionality
- Installs as service/driver
  - No reboot required
  - Captures events from early in the boot process

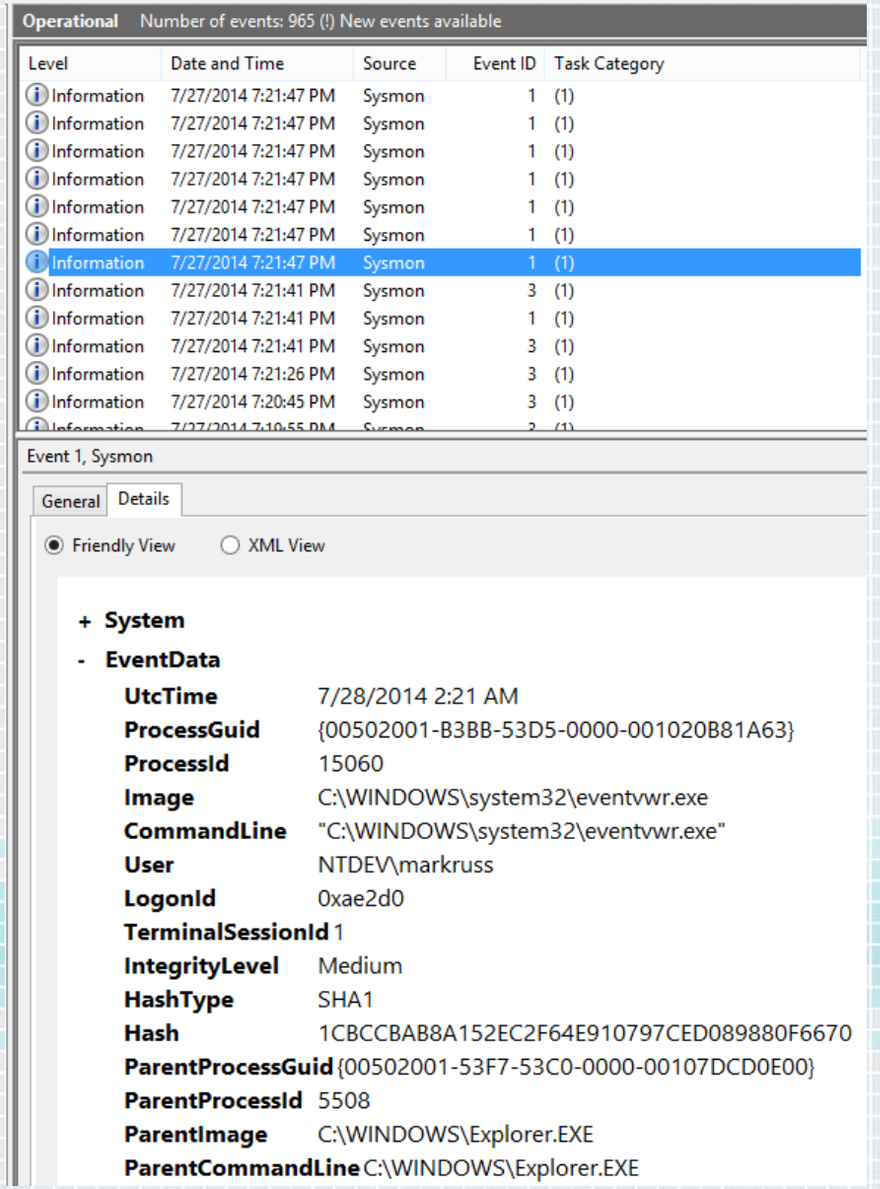
```
C:\sysint\Sysmon\Public_Release>sysmon -c

Sysinternals Sysmon v1.0 - System activity monitor
Copyright (C) 2014 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Current configuration:
 - Service name:                   Sysmon
 - Driver name:                    SysmonDrv
 - HashingAlgorithm:               SHA1
 - Network connection:             enabled
```

Sysmon Events

- Process create (new: process terminate process):
  - Image file and image file hash
  - Command line
  - Parent image and command line
  - GUID for process ID-independent tracking
- Driver load and unload:
  - Image file and image file hash
- Network connections:
  - Process name
  - IP addresses and ports
  - Host and port names
- File create timestamp change
  - Process responsible
  - Original and new timestamp
- New: CreateRemoteThread
  - Source process
  - Target process

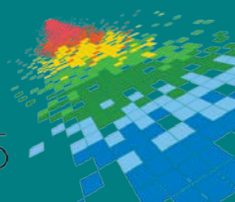


Sysmon Configuration

- Supports filters on the command-line
  - Processes to include or exclude
  - Process network activity
  - Hash types to collect
- Configuration file offers full filtering
  - Include/exclude on any event type
  - Conditionals on any event field
- Default:
  - Process create and terminate, file timestamp change

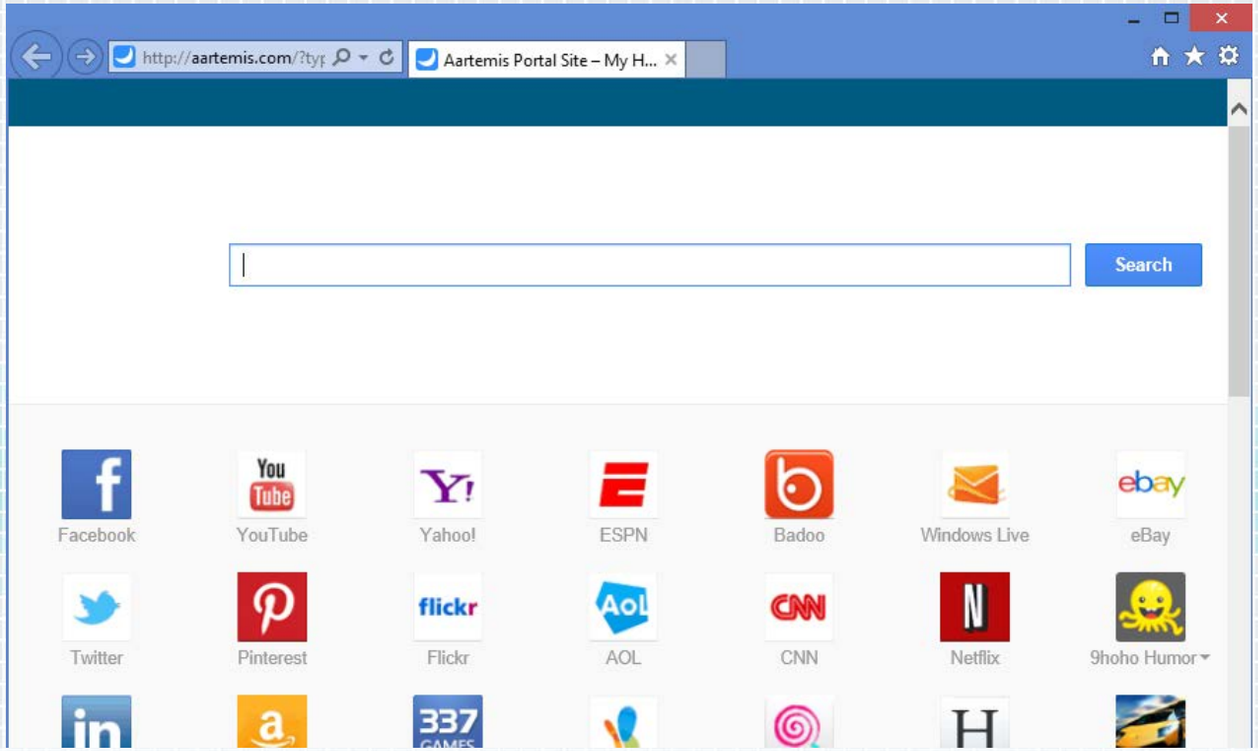
```
<Sysmon schemaversion="2.0">
  <!-- Capture all hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <ProcessCreate onmatch="include">
      <Image condition="contains">notepad</Image>
    </ProcessCreate>
    <FileCreateTime onmatch="include"/>
    <ImageLoad onmatch="include"/>
    <CreateRemoteThread onmatch="include"/>
    <ProcessTerminate onmatch="include">
      <Image condition="contains">notepad</Image>
    </ProcessTerminate>
    <DriverLoad onmatch="exclude"/>
    <NetworkConnect onmatch="include"/>
  </EventFiltering>
</Sysmon>
```

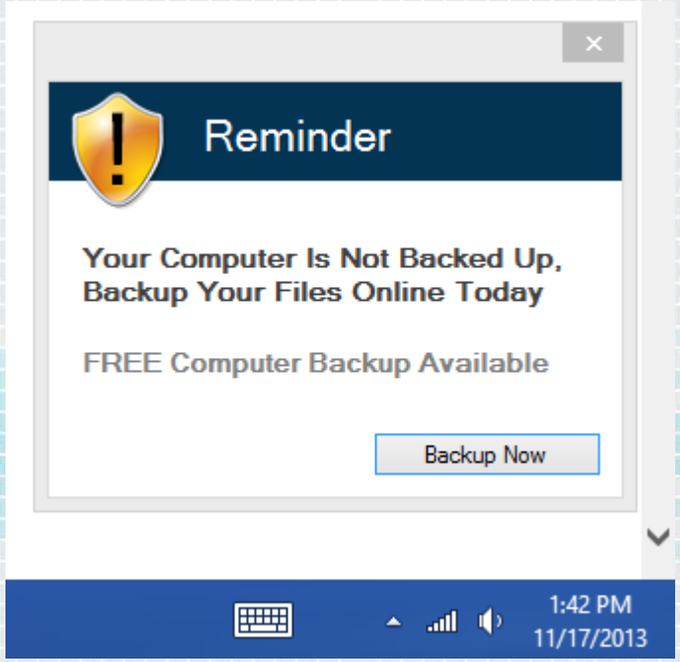
Unwanted Software



The Case of the Unwanted Software

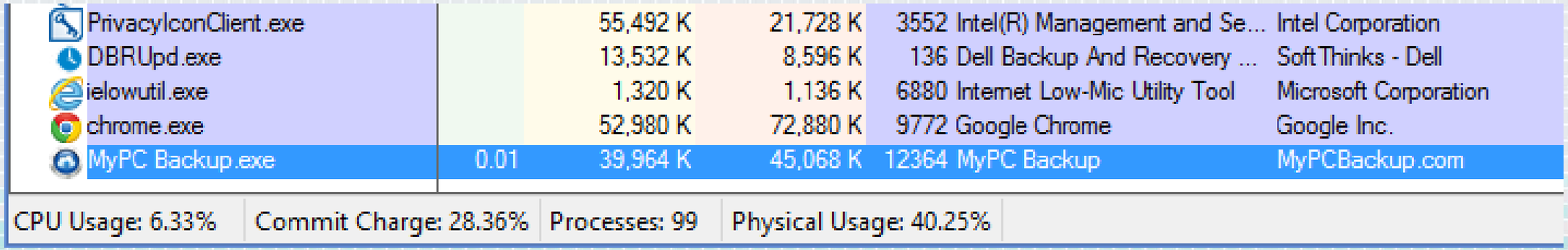
- Mom complained about two symptoms:
  - Her IE home page was hijacked
  - She got toast from a backup program





The Case of the Unwanted Software (Cont)

- I went after the backup toast first
- Launched Process Explorer and used window finder to identify offending process:

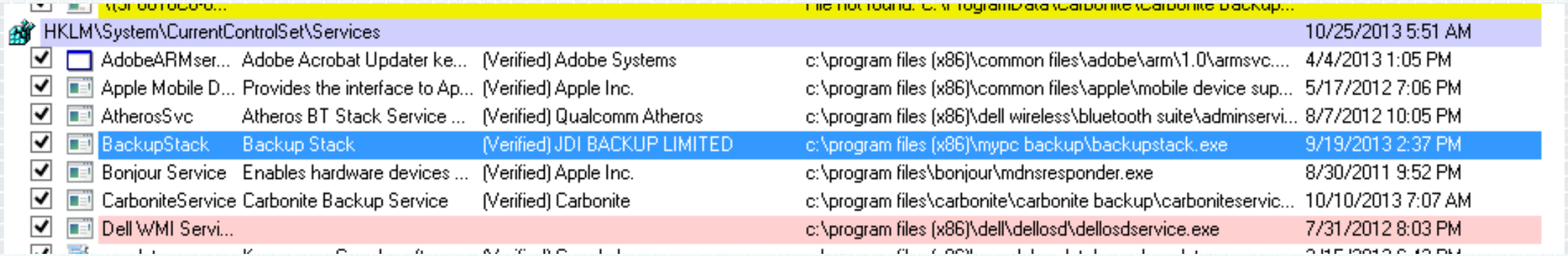


PrivacyIconClient.exe		55,492 K	21,728 K	3552	Intel(R) Management and Se...	Intel Corporation
DBRUpd.exe		13,532 K	8,596 K	136	Dell Backup And Recovery ...	Soft Thinks - Dell
ielowutil.exe		1,320 K	1,136 K	6880	Internet Low-Mic Utility Tool	Microsoft Corporation
chrome.exe		52,980 K	72,880 K	9772	Google Chrome	Google Inc.
MyPC Backup.exe	0.01	39,964 K	45,068 K	12364	MyPC Backup	MyPCBackup.com

CPU Usage: 6.33% | Commit Charge: 28.36% | Processes: 99 | Physical Usage: 40.25%

The Case of the Unwanted Software (Cont)

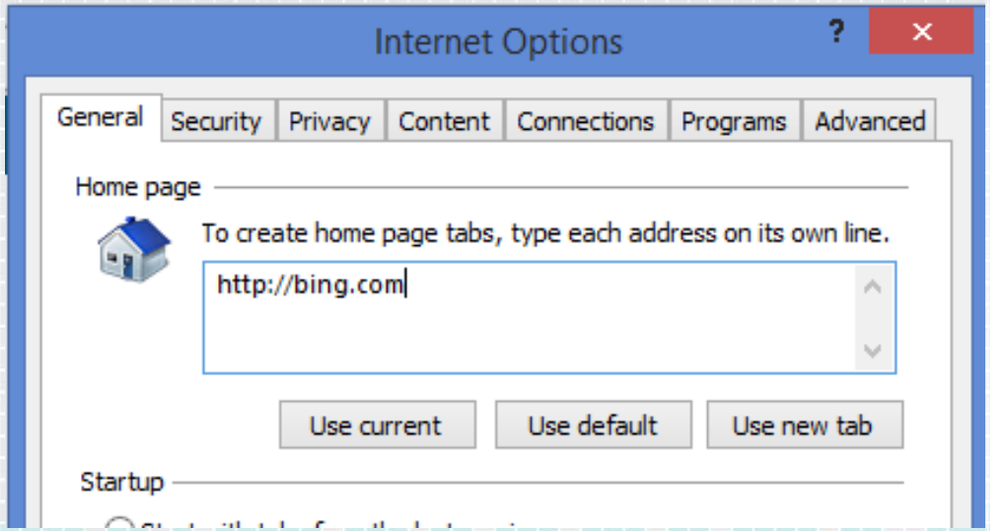
- Launched Autoruns and disabled related processes:



HKLM\System\CurrentControlSet\Services				10/25/2013 5:51 AM
AdobeARMser...	Adobe Acrobat Updater ke...	(Verified) Adobe Systems	c:\program files (x86)\common files\adobe\arm\1.0\armsvc....	4/4/2013 1:05 PM
Apple Mobile D...	Provides the interface to Ap...	(Verified) Apple Inc.	c:\program files (x86)\common files\apple\mobile device sup...	5/17/2012 7:06 PM
AtherosSvc	Atheros BT Stack Service ...	(Verified) Qualcomm Atheros	c:\program files (x86)\dell wireless\bluetooth suite\adminservi...	8/7/2012 10:05 PM
BackupStack	Backup Stack	(Verified) JDI BACKUP LIMITED	c:\program files (x86)\mypc backup\backupstack.exe	9/19/2013 2:37 PM
Bonjour Service	Enables hardware devices ...	(Verified) Apple Inc.	c:\program files\bonjour\mdnsresponder.exe	8/30/2011 9:52 PM
CarboniteService	Carbonite Backup Service	(Verified) Carbonite	c:\program files\carbonite\carbonite backup\carboniteservic...	10/10/2013 7:07 AM
Dell WMI Servi...			c:\program files (x86)\dell\dellosd\dellosdservice.exe	7/31/2012 8:03 PM

The Case of the Unwanted Software (Cont)

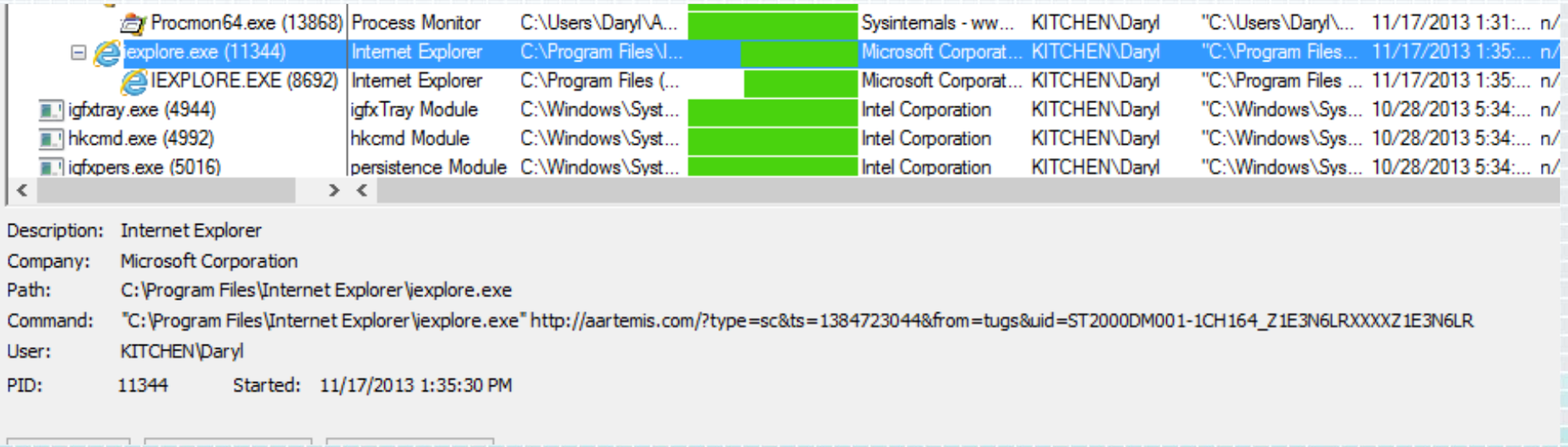
- To find home page hijack, first looked at home page setting
  - Saw that it was Bing:



- But IE launched a different page, so captured an IE startup trace with Procmon…

The Case of the Unwanted Software: Solved

- Looked at IE command line and saw parameter:

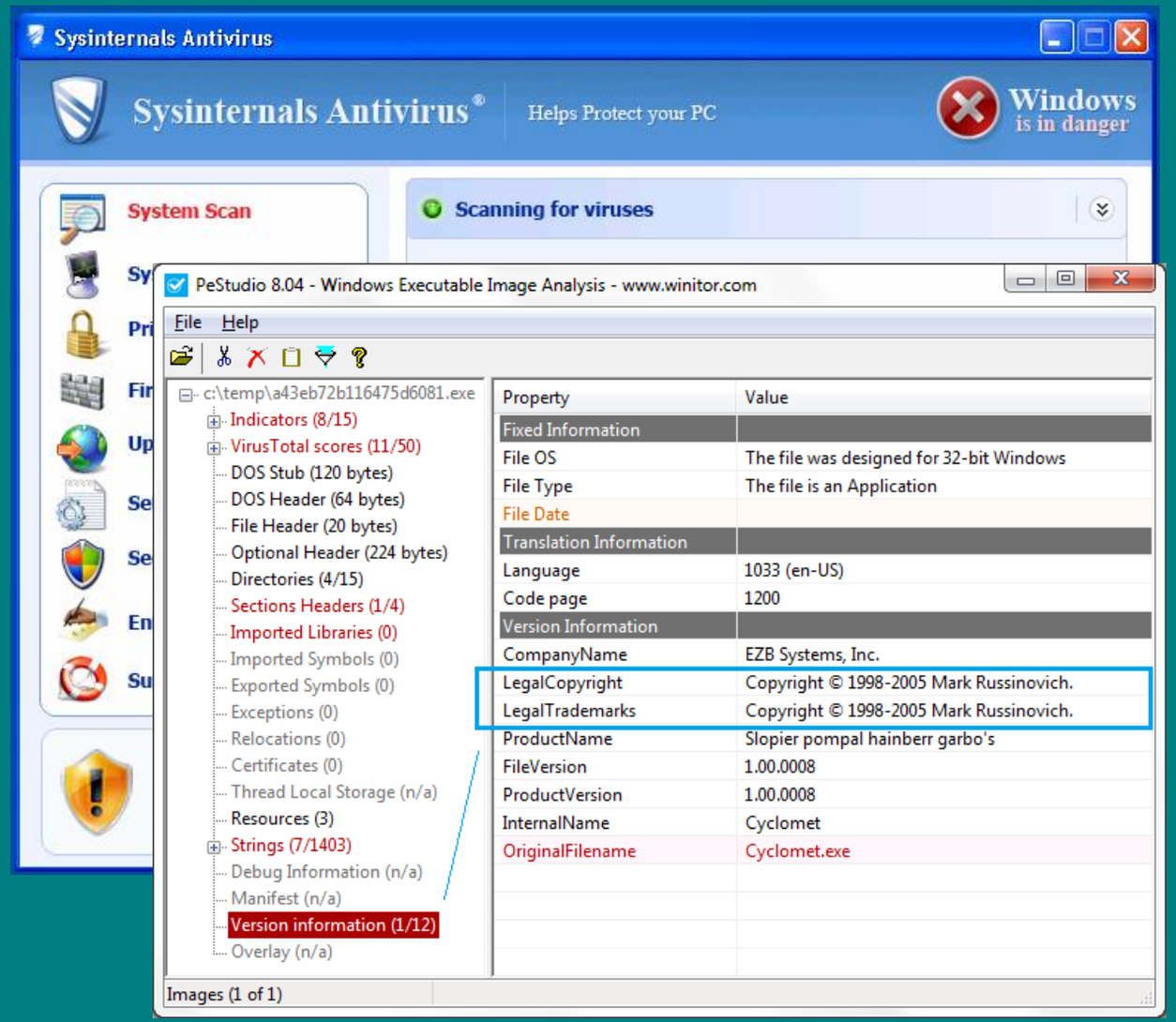


Procmon64.exe (13868)	Process Monitor	C:\Users\Daryl\A...	Sysinternals - ww...	KITCHEN\Daryl	"C:\Users\Daryl\...	11/17/2013 1:31:...	n/
explore.exe (11344)	Internet Explorer	C:\Program Files\I...	Microsoft Corporat...	KITCHEN\Daryl	"C:\Program Files...	11/17/2013 1:35:...	n/
IEXPLORE.EXE (8692)	Internet Explorer	C:\Program Files (...	Microsoft Corporat...	KITCHEN\Daryl	"C:\Program Files ...	11/17/2013 1:35:...	n/
igfxtray.exe (4944)	igfxTray Module	C:\Windows\Syst...	Intel Corporation	KITCHEN\Daryl	"C:\Windows\Sys...	10/28/2013 5:34:...	n/
hkcmd.exe (4992)	hkcmd Module	C:\Windows\Syst...	Intel Corporation	KITCHEN\Daryl	"C:\Windows\Sys...	10/28/2013 5:34:...	n/
igfxpers.exe (5016)	persistence Module	C:\Windows\Syst...	Intel Corporation	KITCHEN\Daryl	"C:\Windows\Sys...	10/28/2013 5:34:...	n/

Description: Internet Explorer
Company: Microsoft Corporation
Path: C:\Program Files\Internet Explorer\iexplore.exe
Command: "C:\Program Files\Internet Explorer\iexplore.exe" http://aartemis.com/?type=sc&ts=1384723044&from=tugs&uid=ST2000DM001-1CH164_Z1E3N6LRXXXXZ1E3N6LR
User: KITCHEN\Daryl
PID: 11344 Started: 11/17/2013 1:35:30 PM

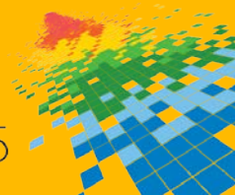
- Opened IE shortcut link and deleted command line: problem solved

Scareware

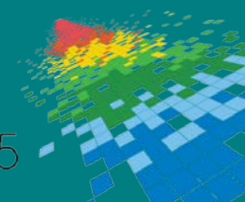

Sysinternals Antivirus
Sysinternals Antivirus®
Helps Protect your PC
Windows is in danger
System Scan
Scanning for viruses
PeStudio 8.04 - Windows Executable Image Analysis - www.winitor.com
File Help
c:\temp\a43eb72b116475d6081.exe
Indicators (8/15)
VirusTotal scores (11/50)
DOS Stub (120 bytes)
DOS Header (64 bytes)
File Header (20 bytes)
Optional Header (224 bytes)
Directories (4/15)
Sections Headers (1/4)
Imported Libraries (0)
Imported Symbols (0)
Exported Symbols (0)
Exceptions (0)
Relocations (0)
Certificates (0)
Thread Local Storage (n/a)
Resources (3)
Strings (7/1403)
Debug Information (n/a)
Manifest (n/a)
Version information (1/12)
Overlay (n/a)
Property
Value
Fixed Information
File OS
The file was designed for 32-bit Windows
File Type
The file is an Application
File Date
Translation Information
Language
1033 (en-US)
Code page
1200
Version Information
CompanyName
EZB Systems, Inc.
LegalCopyright
Copyright © 1998-2005 Mark Russinovich.
LegalTrademarks
Copyright © 1998-2005 Mark Russinovich.
ProductName
Slopier pompal hainberr garbo's
FileVersion
1.00.0008
ProductVersion
1.00.0008
InternalName
Cyclomet
OriginalFilename
Cyclomet.exe
Images (1 of 1)

Analyzing FakeRean

http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Win32/fakerean



Detonation Chambers

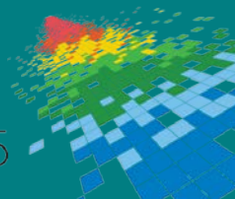


SONAR

- Microsoft's operating system group runs an IE zero-day sandbox detection detonation chamber
  - Sysmon logs detect malware escape from IE's low-integrity sandbox
  - Sysmon log analysis can lead researchers to escape vulnerability
- Previous zero-day RDP Active-X sandbox escape with UAC bypass:

Image	Command Line	Parent	IL
C:\Windows\System32\TSWbPrxy.exe	C:\Windows\system32\TSWbPrxy.exe -Embedding	C:\Windows\System32\svchost.exe	Medium
C:\Windows\System32\regsvr32.exe	-i:fhhefkjdhenkceklildhe -s "C:\Users\Abby\AppData\LocalLow\{55F7E274-C610-4FAE-95AA-59612F07CF73}\api-ms-win-system-secproc-l1-1-0.dll"	C:\Windows\System32\TSWbPrxy.exe	Medium
C:\Windows\explorer.exe	C:\Windows\explorer.exe	C:\Windows\System32\regsvr32.exe	Medium
Bypass UAC			
C:\Windows\System32\migwiz\migwiz.exe	"C:\Windows\System32\migwiz\migwiz.exe"	C:\Windows\explorer.exe	High

Summary



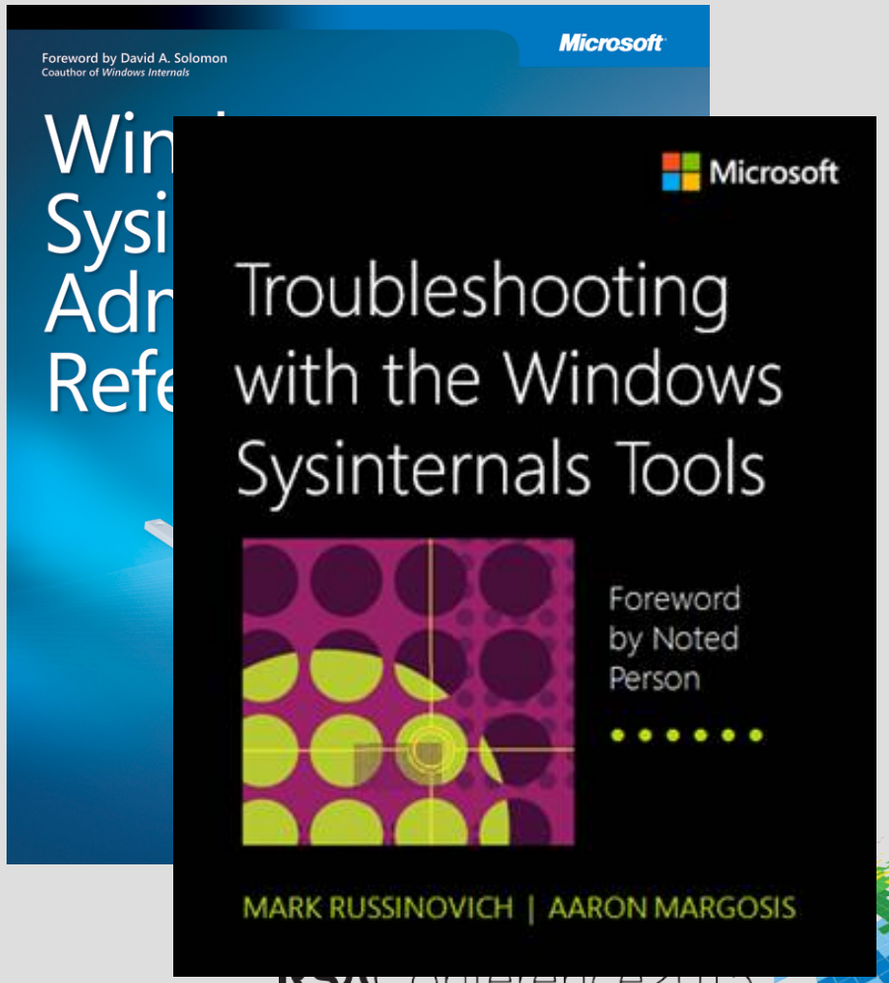
The Future of Malware

- We've seen the trends:
  - Malware that pretends to be from Microsoft or other legitimate companies
  - Malware protected by sophisticated rootkits
  - Malware that has stolen certificates
- Cleaning is going to get much, much harder
  - Targeted and polymorphic malware won't get AV/AS signatures
  - Malware can directly manipulate Windows structures to cause misdirection
  - All standard tools will be directly attacked by malware
  - There will be more un-cleanable malware
- You can't know you're infected unless you find a symptom

Prevent and Detect

The Sysinternals Administrator's Reference

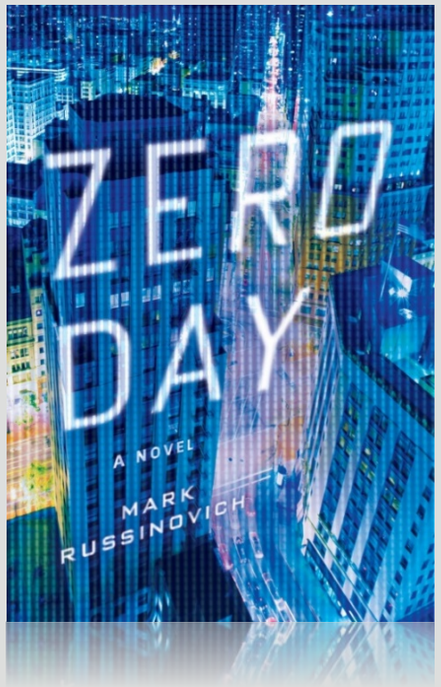
- The official guide to the Sysinternals tools
  - Covers every tool, every feature, with tips
  - Written by Mark Russinovich and Aaron Margosis
- Full chapters on the major tools:
  - Process Explorer
  - Process Monitor
  - Autoruns
- Other chapters by tool group
  - Security, process, AD, desktop, …

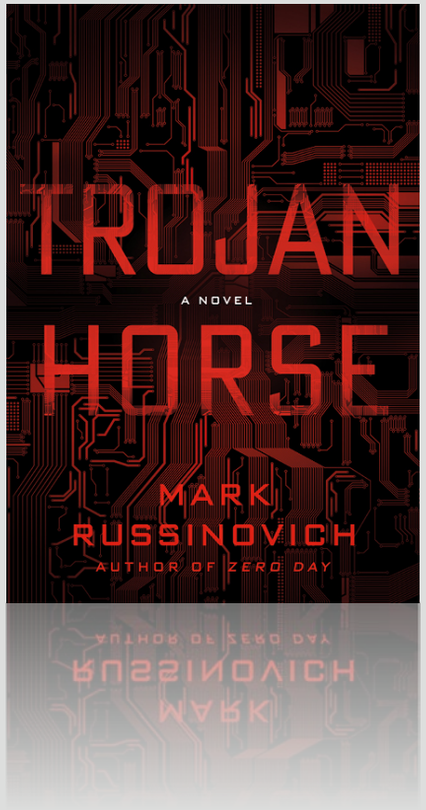


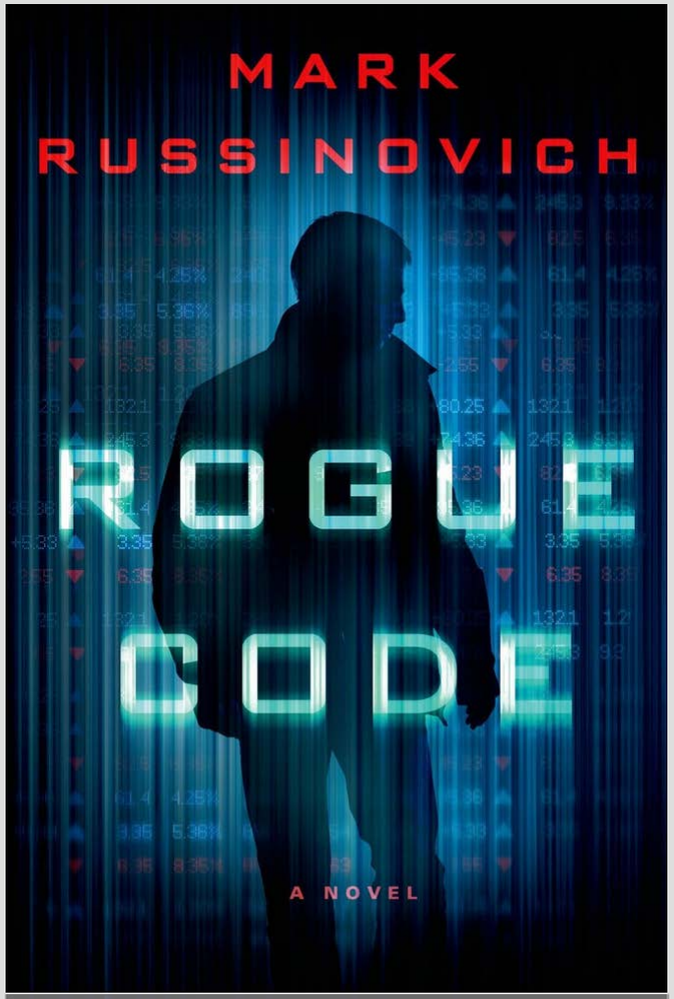
My Cyberthrillers:

www.russinovich.com

- Zero Day: cyberterrorism
- Trojan Horse: state-sponsored cyberwarfare
- Rogue Code: financial cybercrime and insider threats







Rogue Code book giveaway and signing at the Microsoft Boot @ 3:00pm

Book signing at the RSA bookstore @ 1:00pm tomorrow

@markrussinovich