RS/Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: HTA-T07R

Malware Hunting with the Sysinternals Tools

Mark Russinovich

CTO, Microsoft Azure Microsoft @markrussinovich



Challenge today's security thinking

THE WALL STREET JOURNAL. \equiv | tech

TECHNOLOGY

Symantec Develops New Attack on Cyberhac

Declaring Antivirus Software Dead, Firm Turns to Minimizing Damage Fre

b

RSAConference2015

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."

Microsoft



implecomputerupgrade.info/o/f3/dca5e38a280bdb6ef63c24bfae50e550/?subid=1a7640682aa88f54ddbf2d98c7f70887&transaction_id=





RSAConference2015







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



MICROSOFT CONFIDENTIAL - INTERNAL ONLY

RSAConference2015

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

plications	Processes	Services	Performanc	e Networking	king Users
Image Nam	ne	User Name	CPU	Memory (. Description
POWERPN	T.EXE	markruss	00	16,616 K	Microsoft Office PowerPoint
PPA.exe		markruss	00	309,576 K	C PPA.exe
Presentatio	onFon	LOCAL	00	8,228 K	PresentationFontCache.exe
procexp.ex	ke *32	markruss	00	1,388 K	Sysinternals Process Explorer
procexp64	.exe	markruss	02	68,812 K	Sysinternals Process Explorer
Realmon.e:	xe	markruss	00	1,472 K	Realmon
SearchInde	exer	SYSTEM	00	38,880 K	Microsoft Windows Search Inde
services.ex	ĸe	SYSTEM	00	9,728 K	Services and Controller app
ealmon.	exe	п	markrus	s	00 1,472 K Realmon
SnagitEdito	or.ex	markruss	00	15,624 K	Snagit Editor
SnagPriv.e	xe *32	markruss	00	1,524 K	Snagit RPC Helper
splwow64.	exe	markruss	00	11,956 K	C Print driver host for 32bit applic
spoolsy ex	e	SYSTEM	00	11,716 K	Spooler SubSystem App
spoolsv.ex	e	LOCAL	00	14,432 K	K Host Process for Windows Servi
svchost.ex		SYSTEM	00	6,292 K	K Host Process for Windows Servi 👻
svchost.ex svchost.ex	e				

RSAConference2015



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



#RSAC

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



#RSAC

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

]	POV	VERPN	r.exe:71	28 Propert	ies	- 🗆	×
GPU Graph Image	Threads Performa	TCP/IP nce	Security Performa	Environmer nce Graph	nt Job Disk a	o Str and Netwo	rings ork
Image File Version: Build Tim Path: C:\Prog	Microsof Microsof 15.0.44 e: Wed No gram Files M	ft PowerPo ft Corpora 54. 1000 v 07 02:3 icrosoft O	pint Ition 7:45 2012 ffice 15\rd	ot\office15\PC	WERPN	Explore	
"C:\Pro Current C:\Use Autostar n/a	gram Files \v directory: rs \markruss \ rt Location:	licrosoft (Documen	Dffice 15\F	loot\Office15\	POWERP	NT.EXE"	
Parent: User: Started: Comment: VirusTotal: Data Exec Address S	explorer.e NTDEV\ma 12:45:36 F : <u>0/47</u> ution Prever	xe(3800) rkruss PM 1/19/ ntion (DEF andomiza	2014 I) Status: I tion: I	mage: 32-bit Submit DEP (permaner Enabled, Force	<u>B</u> rin <u>K</u> il	<u>V</u> erify g to Fron I Process	t
				04		Cano	el



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

VIIUSIOLAI	
SHA256: 9at25b130t27560c2b2c8bte76d504tb626e817t36b3td6a7a15908467atc7b8	
File name: POWERPNT.EXE	
Detection ratio: 0 / 47	
Analysis date: 2014-01-17 21:53:09 UTC (1 day, 23 hours ago)	
© Probably harmless! There are strong indicators suggesting that this file is safe to use.	
Analysis Q File detail 3 Additional information Comments 0 Q Votes	
Antivirus Result Update	
AVG 20140117	
Ad-Aware	
Agnitum	
INISSIV.exe Oriknown	
svchost.exe	
CcmExec.exe <u>1/47</u>	
Parent: ProcExp.exe(7184) Ve	/erify
User: NTDEV\markruss	
Started: 12:48:29 PM 1/19/2014 Image: 64-bit	to Front
Comment:	Process
VirusTotal: Scanning file Submit	
Data Execution Prevention (DEP) Status: DEP (permanent)	
Address Space Load Randomization: Enabled	

RSAConference2015





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



MICROSOFT CONFIDENTIAL - INTERNAL ONLY

RSAConference2015

Investigating Autostarts

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

Microsoft

General Boot Ser	ion rvices Startup To	pols		
Startup Item Microsoft® Live Mesh Windows Liv Frust Antivi Frust Antivi Sysinternals Soagit	Manufacturer Microsoft Corp Microsoft Corp Microsoft Corp Computer Asso Unknown Sysinternals TechSmith Cor	Command %WINDIR%\system32\fveNotify.exe "C:\Users\markruss\AppData\Local\Micr "C:\Program Files (x86)\Windows Live\ C:\Program Files\CA\eTrust Antivirus\re C:\Windows\System32\Iecheck.exe C:\src\ZoomIt\Release\ZoomIt.exe C:\PPOGPA~2\TECHSModI\SNAGITad\	Location HKCU\SOFTWARE\ HKCU\SOFTWARE\ HKCU\SOFTWARE\ HKCU\SOFTWARE\ C:\Users\markruss\ C:\ProgramData\Mic	
🖊 IEHost 🛛 🛛	Inknown	C:\Windows\System32\	Iecheck.exe	HKCU\SOFTWARE\
		III Enable all OK Cancel	Disable all	

#RSAC

RS^AConference2015

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 Microsoft



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 RSAConference2015

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:

JIII 🛛 🖾 Lonon I 😾 Evolorer I 🛲 Internet Evolorer
Offline System
Select the Windows directory of the offline system:
System Root: e:\windows
User Profile: e:\users\abby a
🖅 Browse for Directory
Look in: Users
MPNetwo Name A
ystem\Cu
dp94xx Recent Places Mefault

Microsoft



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

								#D	CVC
pt	ions	User	Help					#1	SAC
,	Hid	e Empt	ty Locatio	ons					
	Hid	e Micro	osoft Entr	ries	k				
Hide Windows Entries									
	Hid	e Virus	Total Clea	an Entries	e e e e e e e e e e e e e e e e e e e				
	Scar	n Optic	ons						
	Fon	t		Autoru	ns Sca	n Optio	ns	>	<
			Scan	only per-user	locations	;			
			Verif	fy code signatu	res				
			Chec	ck VirusTotal.co	m				
			S	ubmit Unknown	Images				
					Re	scan	Can	cel	
									-

3	Autoruns	[NTDEV\markruss] - S	Sysinternals: www.sysinternals.com	1	- 🗆 🗙
ile Entry Options Us	ser Help				
🚽 🕋 🐴 🖸 🗙 🦻	Filter:				
🔌 AppInit 🛛 🔌 KnownD	LLs 🔮 Winlogon 🛸 W	'insock Providers 🛛 🍓 Print M	Monitors 🛛 🌒 LSA Providers 🛛 🔮 Network	Providers 🗃 WMI 🚦	Sidebar Gadgets
🖉 Everything 🛛 📓 Logor	n 🛛 🚼 Explorer 🛛 🥭 Interr	net Explorer 🛛 🔯 Scheduled 🛛	Tasks 🏽 🏶 Services 🗐 💻 Drivers 🚺 Co	odecs 🛛 🗂 Boot Execute	📑 Image Hijacks
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal 🔦
HKLM\SOFTWARE\Cla	sses\Protocols\Handler			12/12/2014 11:48 PM	
🗹 🚳 skypec2c	Skype Click to Call IE Add-on	Microsoft Corporation	c:\program files (x86)\skype\toolbars\intem	7/14/2014 9:16 AM	0/56
HKLM\Software\Classes	s*\ShellEx\ContextMenuHand	lers		12/28/2014 6:03 PM	
🗹 🚳 7-Zip	7-Zip Shell Extension	Igor Pavlov	c:\program files\7-zip\7-zip.dll	11/18/2010 8:08 AM	0/56
🖌 🚳 ANotepad++64	ShellHandler for Notepad++		c:\program files (x86)\notepad++\nppshell	5/12/2014 1:49 AM	0/56
🖌 🚳 EPP	Microsoft Security Client Sh	Microsoft Corporation	c:\program files\microsoft security client\sh	3/11/2014 11:33 AM	0/55
Spacit Main Sh	Snanit Shell Extension DLI	TechSmith Compration	c:\nmaram files (vR6)\techsmith\snaait 11\d	2/21/2013 1·15 PM	







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



MICROSOFT CONFIDENTIAL - INTERNAL ONLY

RSAConference2015

#RSAC

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

â	Process Monitor - Sysinternals:	www.sysinternals.com	-	
File Edit Event Filter Tools Options Help				
🛎 🖬 🍳 🅦 🖾 🗢 🗛 🚳 🗉	👫 🦻 🔜 🔜 🎝 🌆			
Time Process Name PID Operation	Path	Result	Detail	
9:07:4 Explorer EXE 4780 CloseFile 9:07:4 Explorer EXE 4780 QueryStandardInfo 9:07:4 Explorer EXE 4780 RegQueryKey 9:07:4 Explorer EXE 4780 RegQueryKey 9:0	C:\Users\markruss\AppData\Local\Microsoft\Windows. rC:\Users\markruss\AppData\Local\Microsoft\Windows. rC:\Users\markruss\AppData\Local\Microsoft\Windows. rC:\Users\markruss\AppData\Local\Microsoft\Windows. rC:\Users\markruss\AppData\Local\Microsoft\Windows. rC:\Users\markruss\AppData\Local\Microsoft\Windows. c:\Users\markruss\AppData\Local\Microsoft\Windows. c:\Users\markruss\AppData\Local\Microsoft\Windows. c:\Users\markruss\AppData\Local\Microsoft\Windows. c:\Users\markruss\AppData\Roaming\Microsoft\Wind HKCU\Software\Classes HKCU\Software\Classes HKCU\Software\Classes HKCU\Software\Classes HKCP\LSID\{00021401-0000-0000-000000000. HKCR\CLSID\{00021401-0000-0000-000000000. HKCR\CLSID\{00021401-0000-0000-000000000. C:\Users\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind cC\Users\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Clusers\markruss\AppData\Roaming\Microsoft\Wind f\Lisers\markruss\AppData\Roaming\Microsoft\Wind f\Users\markruss\AppData\Roaming\Microsoft\Wind f\Liser\Microsoft\Wind	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS .SUCCESS .SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS .SUCCESS .SUCCESS .SUCCESS .SUCCESS .NAME NOT FOUND .NAME NOT FOUND .NAME NOT FOUND .SUCCESS .SUCCESS .SUCCESS .SUCCESS .SUCCESS .SUCCESS .SUCCESS .SUCCESS .SUCCESS .SUCCESS	Allocation Size: 364,544, EndOfFile: 362,088, NumberOfLin Allocation Size: 6,291,456, EndOfFile: 6,291,456, NumberOfLin Allocation Size: 6,291,456, EndOfFile: 6,291,456, NumberOfLin Allocation Size: 6,291,456, EndOfFile: 6,291,456, NumberOf Allocation Size: 6,291,456, EndOfFile: 6,291,456, NumberOf Desired Access: Generic Read, Disposition: Open, Options Control: FSCTL_REQUEST_OPLOCK Query: Handle Tags, Handle Tags: 0x0 Query: Handle Tags, Handle Tags: 0x0 Desired Access: Read Desired Access: Read Query: Handle Tags, Handle Tags: 0x0 Desired Access: Maximum Allowed Length: 144 Desired Access: Generic Read, Disposition: Open, Options Allocation Size: 408, EndOfFile: 407, NumberOfLinks: 1, Del Simo Tune: Sunc TuneCorate Section. Desneptration:	 F F f t
9:07:4 Explorer.EXE 4780 QueryStandardInfo	rC:\Users\markruss\AppData\Roaming\Microsoft\Wind	. SUCCESS	Allocation Size: 408, EndOfFile: 407, NumberOfLinks: 1, Del	I
9.07.4	C:\Users\markruss\AppData\Hoaming\wilcrosoft\Wind. C:\Users\markruss\AppData\Hoaming\Wilcrosoft\Wind tC:\ HKCU\Software\Classes HKCU\Software\Classes HKCU\Software\Classes HKCU\Software\Classes HKCR\CLSID\{031E4825-7B94-4DC3-B131-E946B44C. HKCR\CLSID\{031E4825-7B94-4DC3-B131-E946B44C. HKCR\CLSID\{031E4825-7B94-4DC3-B131-E946B44C. HKCR\CLSID\{031E4825-7B94-4DC3-B131-E946B44C. HKCR\CLSID\{031E4825-7B94-4DC3-B131-E946B44C. C: HKCR\CLSID\{031E4825-7B94-4DC3-B131-E946B44C. HKCR\CLSID\{031E4825-7B94-4DC3-B131-E946B44C. HKCU\Software\Classes HKCU\Software\Classes HKCU\Software\Classes HKCU\Software\Classes	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUND SUCCESS SUCCESS SUCCESS NAME NOT FOUND SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Filter: FILE_NOTIFY_CHANGE_FILE_NAME Query: Name Query: Handle Tags, Handle Tags: 0x0 Query: Handle Tags, Handle Tags: 0x0 Desired Access: Read Desired Access: Read Query: Name Control: FSCTL_READ_USN_JOURNAL Query: Handle Tags, Handle Tags: 0x0 Desired Access: Maximum Allowed Length: 144 Control: FSCTL_READ_USN_JOURNAL Query: Name Query: Handle Tags, Handle Tags: 0x0 Query: Handle Tags, Handle Tags: 0x0 Query: Handle Tags, Handle Tags: 0x0	





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

vent #/29	Properties			
vent Proc	cess Stack			
Image				
	Host Process for Windows Ser Microsoft Corporation	vices		
Name:	svchost.exe			
Version:	6.00.6000.16386			
Path:				
C:\Windo	ows\System32\svchost.exe			
Command	Line:			
C:\Windo	ows\System32\svchost.exe -k L	.ocalSystemNetwork	Restricted	
PID:	1108	Туре:	32-bit	
Parent PID): 648	Virtualized:	False	
Session ID	: 0	Integrity:	System	
User:	NT AUTHORITY\SYSTEM			
Auth ID:	00000000:000003e7			
Started:	11/11/2006 3:14:39 PM	Ended:	(Running)	
DLLs:				
Path		Address	Size	•
C:\Windo	ws\System32\svchost.exe	0x7A0000	0x8000)
C:\Windo	ws\System32\wer.dll	0x6CC70000	0xDD000)
	ws\sustem32\unnn dll	0x6E3D0000	0x33000) 🚽



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



Stack Jump To Include Exclude Highlight	
Jump To Include Exclude Highlight	
Include Exclude Highlight	Ct
Exclude Highlight	
Highlight	

Process Name Image Path Command Line Company Description Version Path Operation Result Event Class Detail PID TID User Session





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"

Process Name	▼ [is	•	🔽 then 🛛 Include 🗨
Reset		CcmExec.exe csrss.exe Explorer.EXE InoTask.exe	Remove
Column	Relation	lsass.exe Ism.exe	A
 Process Name Process Name Operation Operation Path Path Path Path Path Path Path Path 	is begins with begins with ends with ends with ends with ends with	mspaint.exe OUTLOOK.EXE POWERPNT.EXE Procenon.exe SearchFilterHost.exe SearchProtocolHost.exe services.exe sidebar.exe svchost.exe System taskeng.exe	





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



MICROSOFT CONFIDENTIAL - INTERNAL ONLY



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

RS^AConference2015





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

Microsoft

Operational N	umber of events: 965	(!) New events a	available	
Level	Date and Time	Source	Event ID	Task Category
 Information 	7/27/2014 7:21:47 P	M Sysmon	1	(1)
 Information 	7/27/2014 7:21:47 P	M Sysmon	1	(1)
 Information 	7/27/2014 7:21:47 P	M Sysmon	1	(1)
Information	7/27/2014 7:21:47 P	M Sysmon	1	(1)
Information	7/27/2014 7:21:47 P	M Sysmon	1	(1)
Information	7/27/2014 7:21:47 P	M Sysmon	1	(1)
Information	7/27/2014 7:21:47 P	M Sysmon	1	(1)
Information	7/27/2014 7:21:41 P	M Sysmon	3	(1)
Information	7/27/2014 7:21:41 P	M Sysmon	2	(1)
	7/27/2014 7:21:41 P	M Sysmon	3	(1)
	7/27/2014 7:20:45 P	M Sysmon	3	(1)
Information	7/27/2014 7:10:55 0	M Sysmon	2	(1)
Event 1, Sysmon				
General Detai	ls			
Friendly Vie	ew 🔿 XML View	,		
+ Syste - Even	em tData			
Uto	:Time	7/28/2014 2	2:21 AM	
Pro	cessGuid	{00502001-	B3BB-53D	5-0000-001020B81A63}
Pro	cessId	15060		
Ima	age 🛛	C:\WINDOW	/S\system	32\eventvwr.exe
Co	mmandLine '	C:\WINDO	/ WS\svstem	132\eventvwr.exe"
Use	ər	NTDFV/mar	kruss	
		0vao2d0	in abb	
100				
ler	minalSessionic			
Int	egrityLevel	Medium		
Ha	shType	SHA1		
Ha	sh	1CBCCBAB8	A152EC2F	64E910797CED089880F66
Par	entProcessGui	d {0050200	1-53F7-53	C0-0000-00107DCD0E00}
Pai	entProcessId	5508		
Par	rentimage	C:\WINDOW	/S\Explore	r.EXE

ntCommandLine C:\WINDOWS\Explorer.EXE

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>
```

RS^AConference2015





Unwanted Software



MICROSOFT CONFIDENTIAL - INTERNAL ONLY

RSAConference2015

The Case of the Unwanted Software

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

← →	/aartemis.com/?ty _F P	🔹 🖒 🛃 Aartemis Por	tal Site – My H 🗙			- □ × + ₩	
						Ŷ	Reminder
	1					Search	Your Computer Is Not Backed Up, Backup Your Files Online Today
	You		_				FREE Computer Backup Available
Facebook	Tube	Yahoo!	ESPN	Badoo	Windows Live	ebay eBay	Backup Now
Service Twitter	Pinterest	flickr Flickr	AOL	CNN	Netflix	9hoho Humor -	1:42 PM مراا الله ۱:42 PM الله 11/17/2013
in Micross	a,	337 CAMES	1	6	Н	2	

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:

RivacylconClient.exe	55,492 K	21,728 K	3552 Intel(R) Management and Se	. Intel Corporation
OBRUpd.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
ochrome.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:

•	_	(ar our occoro			The notround, c. v. rogramblata carbonite (carbonite backup	
💣 Н	IKLM	\System\CurrentC	ontrolSet\Services			10/25/2013 5:51 AM
✓		AdobeARMser	Adobe Acrobat Updater I	ke (Verified) Adobe Systems	c:\program files (x86)\common files\adobe\arm\1.0\armsvc	4/4/2013 1:05 PM
✓	Ē	Apple Mobile D	Provides the interface to	Ap (Verified) Apple Inc.	c:\program files (x86)\common files\apple\mobile device $\sup\ldots$	5/17/2012 7:06 PM
✓	Ē	AtherosSivc	Atheros BT Stack Servic	e (Verified) Qualcomm Atheros	c:\program files (x86)\dell wireless\bluetooth suite\adminservi	8/7/2012 10:05 PM
-	Ē	BackupStack	Backup Stack	(Verified) JDI BACKUP LIMITED	c:\program files (x86)\mypc backup\backupstack.exe	9/19/2013 2:37 PM
✓	Ē	Bonjour Service	Enables hardware device	es (Verified) Apple Inc.	c:\program files\bonjour\mdnsresponder.exe	8/30/2011 9:52 PM
-	Ē	CarboniteService	Carbonite Backup Servic	e (Verified) Carbonite	c:\program files\carbonite\carbonite backup\carboniteservic	10/10/2013 7:07 AM
-	Ē	Dell WMI Servi			c:\program files (x86)\dell\dellosd\dellosdservice.exe	7/31/2012 8:03 PM
	100		K C I A	AZ 20 D C 1 L		A REPORT OF A DRA

RSAConference2015



The Case of the Unwanted Software (Cont)

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

	? ×									
General	Security	curity Privacy Content Connections Programs								
Home page										
To create home page tabs, type each address on its own line.										
http://bing.com										
Use current Use default Use new tab										
Startup)									
0.										

 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:

) Process Monitor	C:\Users\Daryl\A		Sysinternals - ww	KITCHEN\Daryl	"C:\Users\Daryl\	11/17/2013 1:31: n/	
⊡ 🤇	iexplore.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/	
🔝 igfxtra	ay.exe (4944)	igfxTray Module	C:\Windows\Syst		Intel Corporation	KITCHEN\Daryl	"C:\Windows\Sys	10/28/2013 5:34: n/	
III hkom	id.exe (4992)	hkcmd Module	C:\Windows\Syst		Intel Corporation	KITCHEN\Daryl	"C:\Windows\Sys	10/28/2013 5:34: n/	
I. iqfxpe	ers.exe (5016)	persistence Module	C:\Windows\Syst		Intel Corporation	KITCHEN\Daryl	"C:\Windows\Sys	10/28/2013 5:34: n/	
<	2	< <							
Description:	Internet Explorer								
Company:	ompany: Microsoft Corporation								
Path:	C:\Program Files\Internet	Explorer\jexplore.exe							
Command:	nd: "C:\Program Files\Internet Explorer \jexplore.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

RS∧^COnference2015



💓 #RSAC

Scareware

Sysinte	erna	IS ANTIVITUS								
1	S	vsinternals Antivirus®	Helps Protect your PC	Windows is in danger						
	Sys	item Scan	anning for viruses	8						
2	Sy	PeStudio 8.04 - Windows Executable	Image Analysis - www.winitor.	com 🗖 🗖 💌						
0		File Help								
	Pfi									
副	Fir	C:\temp\a43eb72b116475d6081.exe	Property	Value						
		indicators (8/15)	Fixed Information							
	Up		File OS	The file was designed for 32-bit Windows						
Assess	DOS Stub (120 bytes)		File Type	The file is an Application						
63	Se	DOS Header (64 bytes)	File Date							
		File Header (20 bytes)	Translation Information							
	Se	Directories (1/15)	Language	1033 (en-US)						
1		Sections Headers (1/4)	Code page	1200						
	En	Imported Libraries (0)	Version Information							
-		- Imported Symbols (0)	CompanyName	EZB Systems, Inc.						
	Su	Exported Symbols (0)	LegalCopyright	Copyright © 1998-2005 Mark Russinovich.						
	_	Exceptions (0)	LegalTrademarks	Copyright © 1998-2005 Mark Russinovich.						
-		Relocations (0)	ProductName	Slopier pompal hainberr garbo's						
		Certificates (0)	FileVersion	1.00.0008						
		Thread Local Storage (n/a)	ProductVersion	1.00.0008						
	8	Resources (3)	InternalName	Cyclomet						
		Debug Information (n/a)	OriginalFilename	Cyclomet.exe						
		Manifest (n/a)								
		Version information (1/12)								
		Overlay (n/a)								
		Images (1 of 1)]							

RSAConference2015



MICROSOFT CONFIDENTIAL - INTERNAL ONLY



Analyzing FakeRean

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



MICROSOFT CONFIDENTIAL - INTERNAL ONLY





Detonation Chambers



MICROSOFT CONFIDENTIAL - INTERNAL ONLY

RSAConference2015

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	vstem32\TSWbPrxy.exe C:\Windows\system32\TSWbPrxy.exe -Embedding			
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\System32\regsvr32.exe	Medium		
	Bypass UAC			
C:\Windows\System32\migwiz\migwiz.exe	"C:\Windows\System32\migwiz\migwiz.exe"	C:\Windows\explorer.exe	High	





Summary



MICROSOFT CONFIDENTIAL - INTERNAL ONLY





RSAConference2015

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

crosoft

- Other chapters by tool group
 - Security, process, AD, desktop, ...





My Cyberthrillers:



- 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



