Microsoft Sysmon Deployment

Dimitris Margaritis

16/1/2017

Opinions are my own coming from 2 years of experience with sysmon

For configuration and details about Sysmon events look at Mark Russinovich presentation in RSA 2016

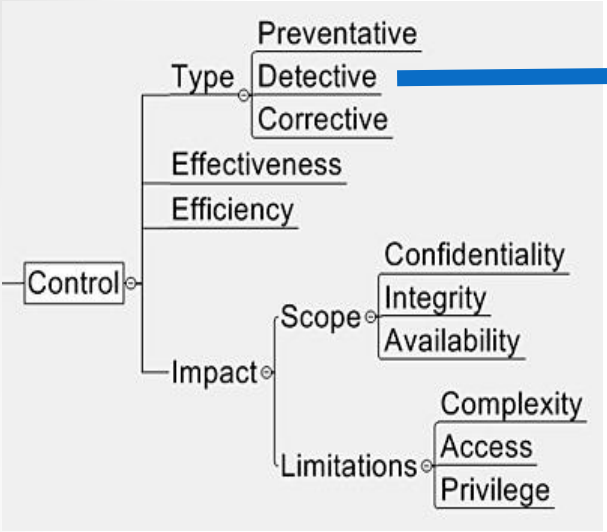
https://www.rsaconference.com/events/us16/agenda/sessions/2461/tracking-hackers-on-your-network-with-sysinternals

This presentation was created by having in mind the deployment of Sysmon in medium to large networks (thousands of hosts) to be used not only for IR and Forensics but also for Hunting.

Agenda

- Answer Ws and Hs
  - Why Sysmon?
  - How much log data?
  - Which is a sample configuration?
  - Which systems first?
  - How end-up to an acceptable volume of events?
- Filtering - Collection
- Detections with EventID=1 & EventIDs != 1
- Takeaways

Why Sysmon?



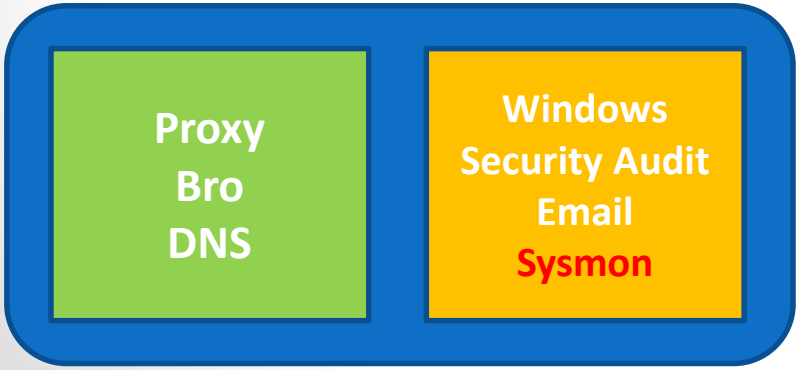
Sysmon

Prevention is Ideal

BUT

DETECTION IS A MUST

Log Management System



Why Sysmon?

Malware free attacks on the rise not detected by traditional tools

Not easy to correlate process creation and net connections

No way to log hashes of attachments

No way to capture thread injections, driver loads and much more

Integrates easily to Windows Event Collection environments

Its FREE

Sysmon in IR pyramid of needs

https://github.com/swannman/ircapabilities

Sysmon deployment challenges & rewards

#1:Filters on events in order to keep events volume to affordable levels.

#2: Sysmon doesn't provide any analysis for the log data and this needs additional tool(s) & effort.

#1: Detections that not possible by other existing controls

#2 Rich DFIR info

#3: Get additional insight about your systems and your network. Don't allow attackers to know your systems better than you!

Sysmon Configuration is a cycle process

Minimize false positives

Establish a maintenance procedure to update configuration when new Threat Intel info is available e.g for registry monitoring

Sysmon Events and Filtering

Proposal for filtering on events when starting with sysmon

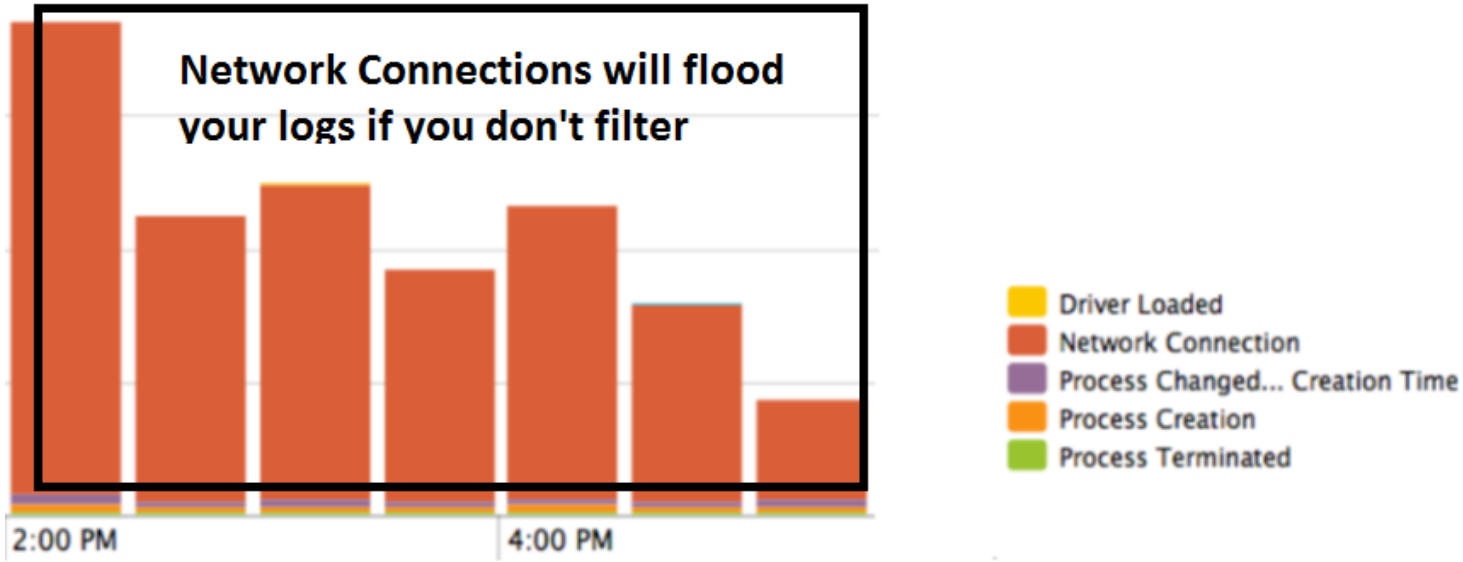
Event ID	Action	Comment/Filter example
Event ID 1: Process creation	Filter	Filter for noisy processes like antivirus Good example at https://github.com/crypsisgroup/Splunkmon/blob/master/sysmon.cfg
Event ID 2: A process changed a file creation time	None	Verbose
Event ID 3: Network connection	Filter	Get only non-browser connections to Internet
Event ID 4: Sysmon service state changed	All	
Event ID 5: Process terminated	None	
Event ID 6: Driver loaded	All	
Event ID 7: Image loaded	None	Verbose with performance issues in win 7
Event ID 8: CreateRemoteThread	All	One way to create malicious thread on another process, some of the other techniques would use the NTCreateThreadEx (http://securityxploded.com/ntcreatethreadex.php)

Sysmon Events and Filtering(cont)

Event ID	Action	Comment/Possible filter
Event ID 9: RawAccessRead	Filter	Verbose. Can monitor user profiles directories
Event ID 10: ProcessAccess	Filter	Get process access to lsass.exe and exclude legitimate processes
Event ID 11: FileCreate	Filter	Monitor at least startup folder
Event ID 12: RegistryEvent(Object create and delete)	Filter	1)Monitor Run and RunOnce keys 2)Modules loaded by lsass <HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders> 3)AppInit_DLLs(if still in windows7 ☺) HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
Event ID 13: RegistryEvent (Value Set)	Filter	
Event ID 14: RegistryEvent (Key and Value Rename)	Filter	
Event ID 15: FileCreateStreamHash	Filter	Hashes of attachments
Event ID 255: Error	All	

Sysmon Network Connections

Network connections are very useful for malware detection but the default configuration is extremely verbose



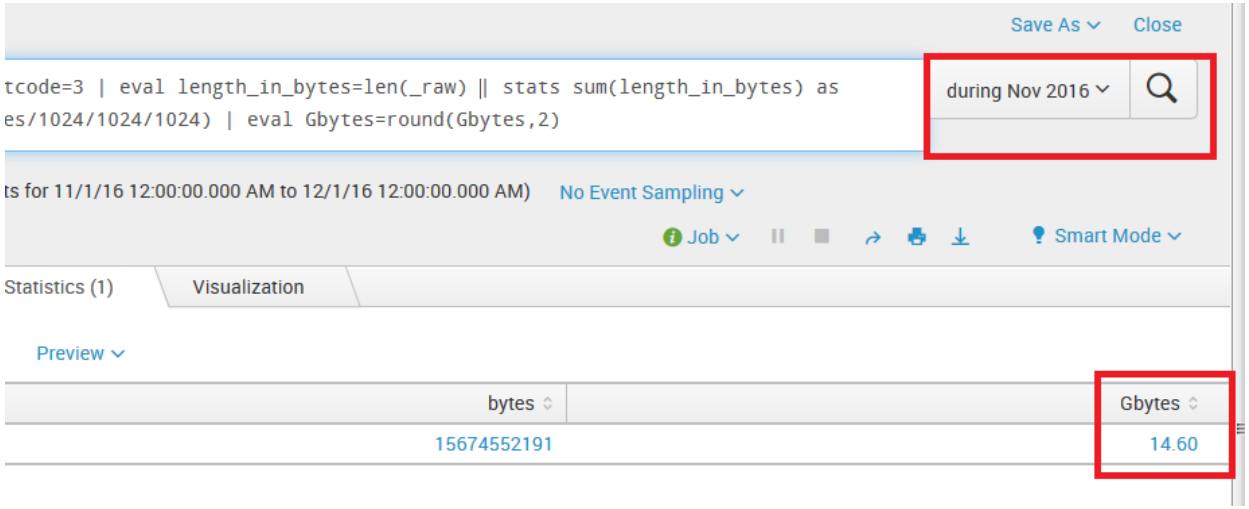
Proposal : Log non-browser's connection towards Internet

Benefit : Can detect malware that communicates with C2 by NOT using browsers

Volume for non-browsers network connections to Internet?

+- 1.500 endpoints

Volume of EventCode 3
max 15 GB/month



Each network is different.

Volume may differ based on workstation config

Sysmon Configuration Example(1/3)

```
<Sysmon schemaversion="3.20">
 <!--Capture SHA256 hashes -->
  <HashAlgorithms>sha256</HashAlgorithms>
  <EventFiltering>
<!--Don't log Events 2,5,9-->
  <FileCreateTime onmatch="include"/>
    <ProcessTerminate onmatch="include"/>
    <RawAccessRead onmatch="include"/>
        <!-- Log  process creation -->
      <ProcessCreate onmatch="exclude">
      <Image condition="contains">McAfee</Image>
      <Image condition="contains">NVIDIA Corporation</Image>
      <Image condition="end with">System32\audiodg.exe</Image>
      <CommandLine condition="contains">Splunk</CommandLine>
      <User condition="is">NT AUTHORITY\NETWORK SERVICE</User>
      <ParentImage condition="contains">Tanium</ParentImage>
    </ProcessCreate>
  <!-- Log all drivers except if the signature -->
  <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="include">
     <Signature condition="contains">microsoft</Signature>
     <Signature condition="contains">windows</Signature>
    </DriverLoad>
```

Sysmon Configuration Example(2/3)

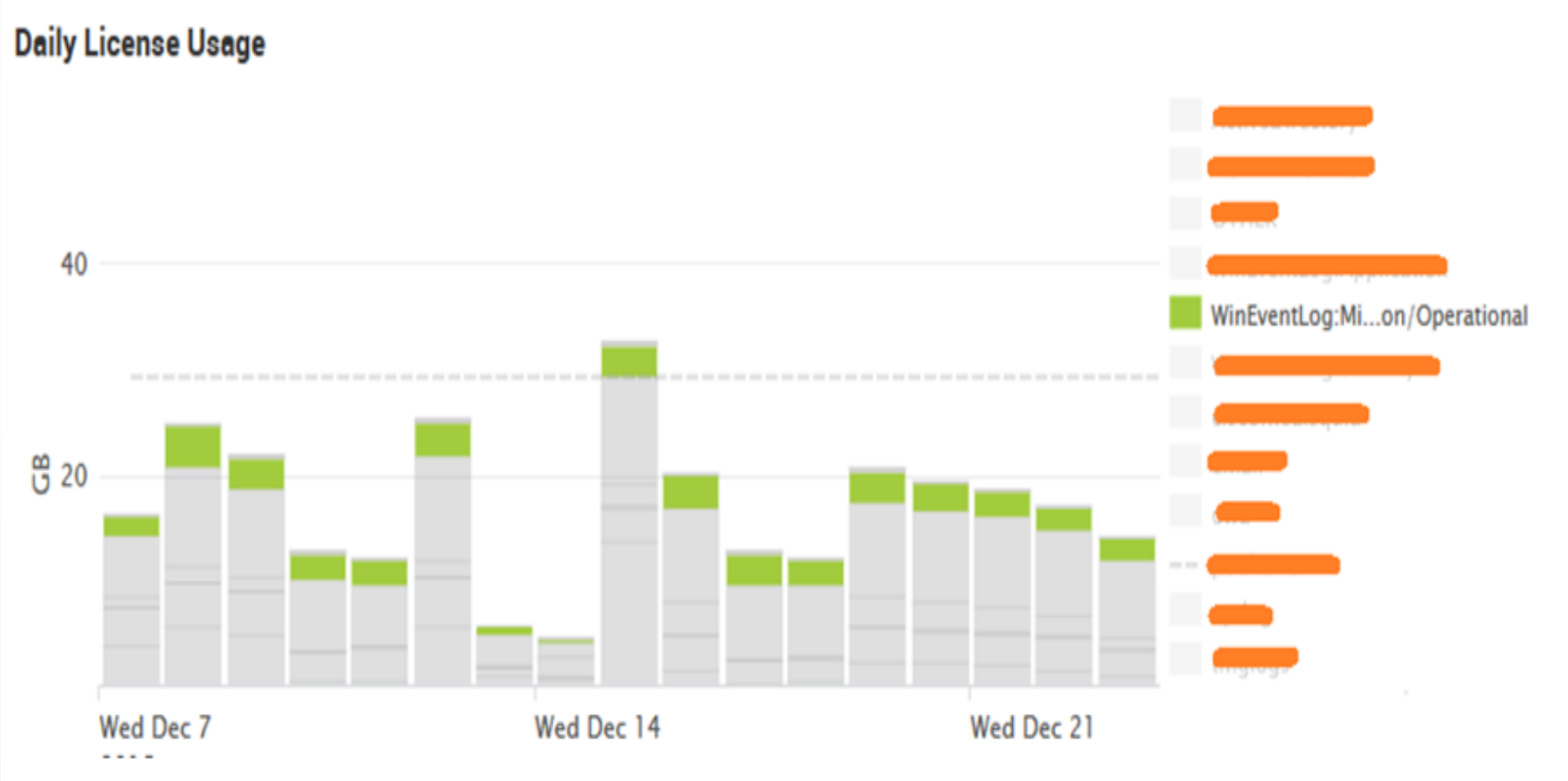
```
  <!-- Log non browser connections to proxy
   If users are using laptopts with split VPN then something else is needed :-
<NetworkConnect onmatch="include">
                <DestinationIp condition="contains">xx.xx.xx</DestinationIp>
                 </NetworkConnect>
<NetworkConnect onmatch="exclude">
        <Image condition="contains">chrome.exe</Image>
        <Image condition="contains">iexplore.exe</Image>
        <Image condition="contains">firefox.exe</Image>
        <Image condition="contains">outlook.exe</Image>
        <Image condition="contains">Skype.exe</Image>
        <Image condition="contains">lync.exe</Image>
        <Image condition="contains">GoogleUpdate.exe</Image>
</NetworkConnect>
   <!-- Log all create remote threads -->
    <CreateRemoteThread onmatch="exclude"/>
<!-- Log process access to lsass.exe -->
    <ProcessAccess onmatch="include">
    <TargetImage condition="contains">lsass.exe</TargetImage>
</ProcessAccess>
<ProcessAccess onmatch="exclude">
    <SourceImage condition="contains">McAfee </SourceImage>
    <SourceImage condition="contains">CcmExec.exe  </SourceImage>
    <SourceImage condition="contains">wmiprvse.exe</SourceImage>
    <SourceImage condition="contains">msiexec.exe</SourceImage>
    <SourceImage condition="contains">GoogleUpdate.exe</SourceImage>
    <SourceImage condition="contains">FlashPlayer</SourceImage>
    <SourceImage condition="contains">svchost.exe</SourceImage>
    <SourceImage condition="contains">MRT.exe</SourceImage>
    <SourceImage condition="contains">mfevtps.exe.exe</SourceImage>
    <SourceImage condition="contains">services.exe</SourceImage>
    <SourceImage condition="contains">wininit.exe</SourceImage>
 </ProcessAccess>
```

Sysmon Configuration Example(3/3)

```
<!-- NEW EVENTS IN SYSMON  5 -->
 <FileCreate onmatch="include">
        <TargetFilename condition="contains">\Startup\</TargetFilename>
</FileCreate>
<RegistryEvent onmatch="include">
    <TargetObject condition="contains">
    Software\Microsoft\Windows\CurrentVersion\Run</TargetObject>
<!-- Useful especially in windows 7-->
    <TargetObject condition="contains">
    Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs</TargetObject>
<!-- Modules loaded by lsass-->
    <TargetObject condition="contains">
    CurrentControlSet\Control\SecurityProviders </TargetObject>
<!-- Detect macro malware that bypass UAC  -->
    <TargetObject condition="contains">
    Software\Classes\mscfile\shell\open\command </TargetObject>
</RegistryEvent>
<!-- Log the hashes of attachments opened by Outlook  -->
<FileCreateStreamHash onmatch="exclude">
    <TargetFilename  condition="contains">Content.Outlook</TargetFilename>
</FileCreateStreamHash>
 </EventFiltering>
</Sysmon>
```

Total Volume?

- With the above filtering **total volume** of sysmon logs for +- 1.500 endpoints is max 5 GB/day



Additional filtering to reduce volume?

- Depending on tools used additional filtering is possible.
- In case of Splunk, Heavy Forwarder can be used to filter even on field level and send to SIEM the most important fields e.g for EventID 1

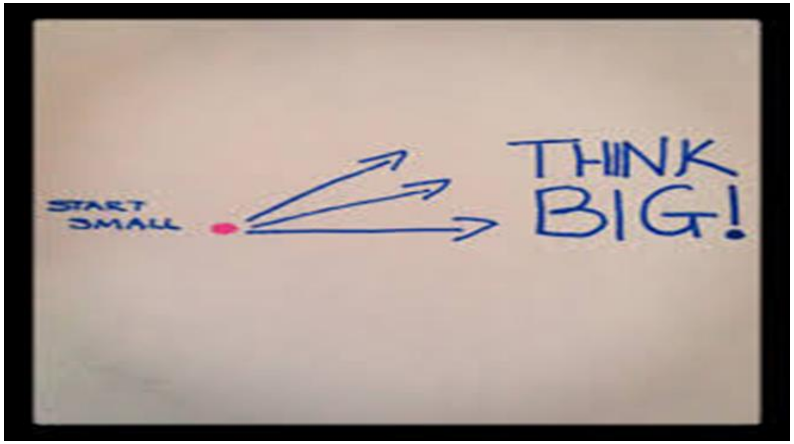
Time, ComputerName, SID, Commandline, ParentCommandline,Hash to achieve savings in storage and possibly in SIEM cost if license is based on volume. Doable but needs extra dose of effort!

Where should I start ?

- Sysmon should be installed on all systems (endpoints & servers not necessarily with same config)

- Logs can initially stay local but the **target should be to have logs out of the boxes**

- 90% + of the attacks start on endpoints so this should be the first group, with web servers a good second choice for detecting web shells



Centralizing Sysmon logs

Use Windows Event Forwarding to help with intrusion detection

Ted Hardy [MSFT] | Last Updated: 5/31/2016 | 2 Contributors

https://technet.microsoft.com/itpro/windows/keep-secure/use-windows-event-forwarding-to-assist-in-instrusion-detection

Capacity Planning for WEC Servers : 10K x 10 K

No more than 10,000 concurrently active WEF Clients per WEC server and no more than 10,000 events/second average event volume

Experience from the field :
A small virtual server can act as collector for 1.500 systems

Find Noisy processes

```
index=wrkevt eventcode=1 | stats count by Image
```

✓ 1,357,270 events (1/13/17 12:00:00.000 AM to 1/13/17 4:22:09.000 PM) No Event Sampling

Events | Patterns | Statistics (3,144) | Visualization

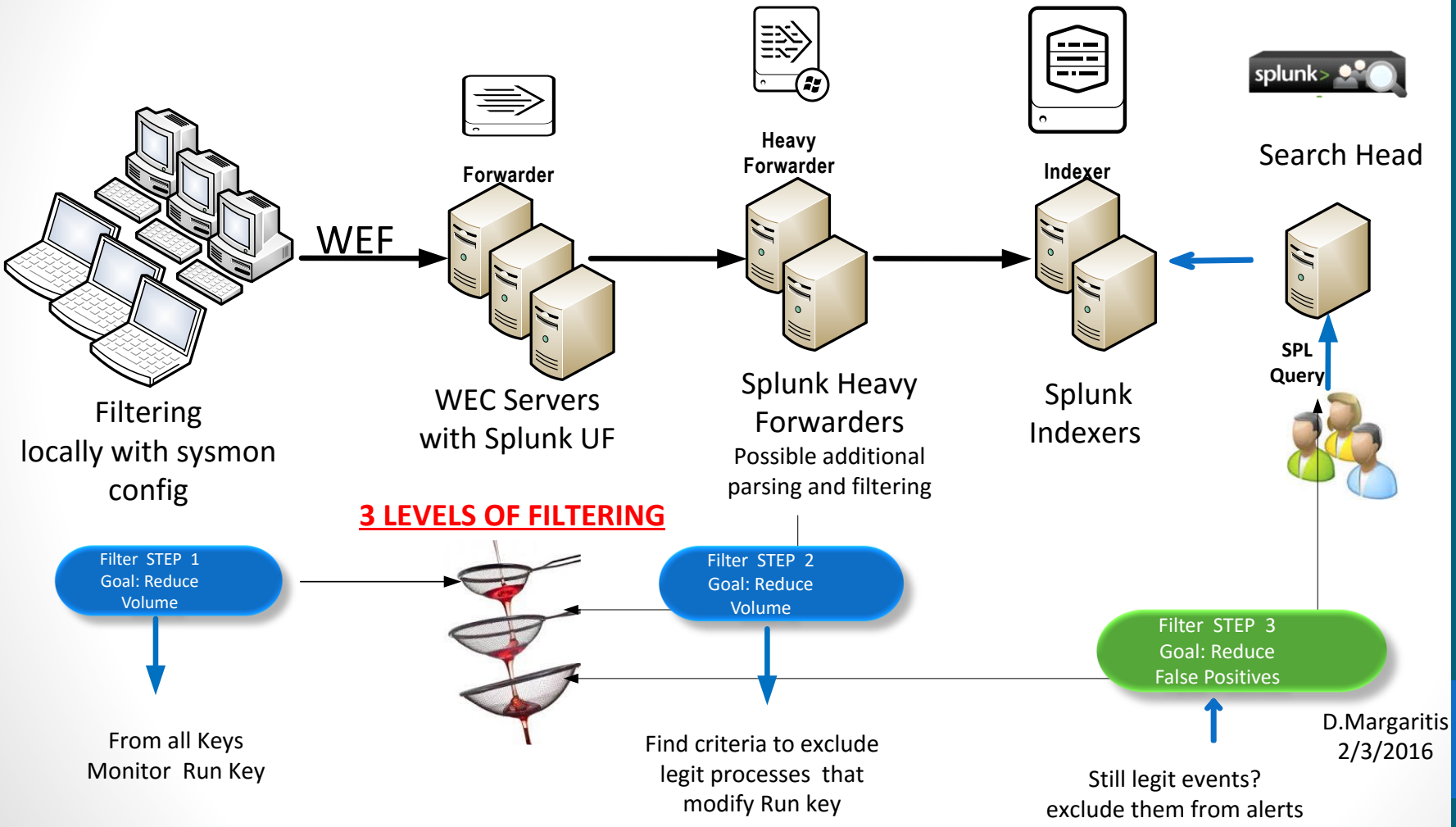
100 Per Page | Format | Preview

Image	count
C:\Windows\System32\conhost.exe	128022
C:\Windows\System32\wbem\WmiPrvSE.exe	127326
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\cvtres.exe	58681
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe	58679
C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe	43207
C:\Windows\System32\SearchFilterHost.exe	38658
C:\Windows\System32\wbem\WmiApSrv.exe	33290
C:\Windows\System32\SearchProtocolHost.exe	31288
C:\Program Files (x86)\McAfee\VirusScan Enterprise\x64\scan64.exe	29965
C:\Windows\System32\dllhost.exe	28745
C:\Windows\System32\cscript.exe	24980
C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe	21602
C:\Program Files\Autodesk\Content Service\Connect.Service.ContentService.exe	21590
C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe	21010
C:\Windows\System32\svchost.exe	18862
C:\Windows\System32\audiodg.exe	18119

Some of them can be filtered e.g conhost.exe

Send Sysmon logs to SIEM

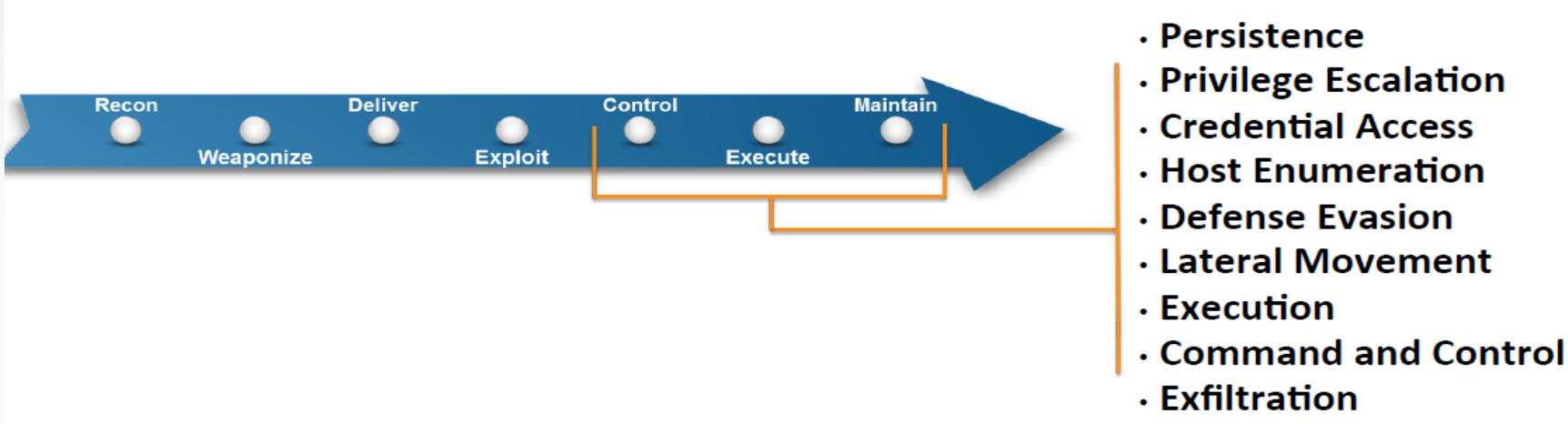
-Depends on the destination system and the available ways to import data e.g for Splunk the easiest way is to install Splunk Universal Forwarder on WEC servers.



D.Margaritis
2/3/2016

Detections

ATT&CK Threat Based Model



Consists of :

-Tactic phases derived from Cyber Attack Lifecycle

-List of techniques available to adversaries for each phase

-Possible methods of detection and mitigation

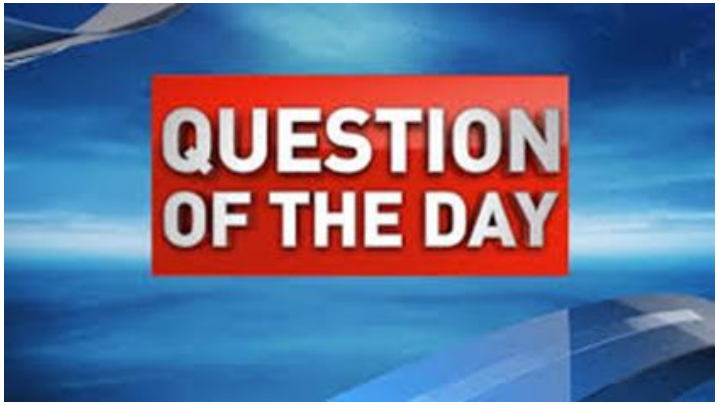
ATT&CK Model : Sysmon Detections

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Rundll32	Automated Collection	Data Compressed	Communication Through Removable Media
Winlogon Helper DLL	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Clipboard Data	Data Encrypted	Connection Proxy
Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data Staged	Data Transfer Size Limits	Custom Command and Control Protoco
New Service	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	MSBuild	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Registry Run Keys / Start Folder	Web Shell	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Regsvr32	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Obfuscation
Scheduled Task	File System Permissions	DLL Search	Network Sniffing	Peripheral Device	Remote File	Process	Data from Removable	Exfiltration Over Other Network	Fallback

ATT&CK Execution

Execution
Command-Line Interface
Execution through API
Rundll32
InstallUtil
PowerShell
Process Hollowing
Regsvcs/Regasm

- Most of Execution Techniques can be detected by analyzing sysmon event ID 1
- In some cases rules are simple with no false positives e.g execution of InstallUtil.exe, Regsvcs.exe, Regasm.exe, rcsi.exe,Msbuilt.exe etc
- However monitoring of cmd.exe, cscript.exe, powershell.exe is challenging because there are a lot of legitimate events.
- For cmd.exe in web servers you can look for events where the web server process spawn cmd.exe as child process while in endpoints look for events where cmd.exe is child of browsers images or office images
- Especially for powershell, analysis of powershell logs is needed and with Sysmon you can monitor if adversary tries to disable powershell v5 logging!



Do we really need Sysmon Event ID 1 for detections based on process command line and parent-child relationships?

Old 4688
Sysmon v2

New 4688
Sysmon v5

Sysmon Event ID 1 vs Windows 4688

Due to the volume of information either Sysmon Event ID 1 OR windows event 4688 is realistic to be logged

	Sysmon EventID 1	Windows Event 4688
Advantages	-Filtering -Can be easily correlated with other sysmon events e,g EventID 3 leading to detections that otherwise are impossible (example with rundll32)	-No need for another program deployment and maintenance - easy configuration through Group Policy -No need for testing
Disadvantages	Tests are needed to deploy sysmon especially in critical systems	1.No filtering capability-logs can be flooded by noisy processes 2.Hash is logged in the AppLocker log and need correlation of the two logs that maybe is very “expensive” in huge volumes 3.Missing all other possibilities offered by sysmon

Detections based on Sysmon EventID=1

Detection rules based on Sysmon EventID 1

Examples of detection rules based on Sysmon Events ID 1 -

[1]www.securitylogs.org

- Parent-Child relationships for Office, Abrobat, Browsers
- Abused Windows Commands

[2]http://security-research.dyndns.org/pub/slides/BotConf/2016/Botconf-2016_Tom-Ueltschi_Sysmon.pdf

- Abnormal svchost.exe
- Advanced Detection(Adwind RAT)

[3]http://www.crypsisgroup.com/images/site/CG_WhitePaper_Splunkmon_1216.pdf

- “net” Reconnaissance of Domain Admin Group
- Credential Harvesting with WMI and WCE

Real Case : Attacker Uses Windows Commands

Usual commands to find what's going on

_time	ParentCommandLine	CommandLine
2016-06-23 11:55:03	CMD.EXE	net use
2016-06-23 11:55:01	CMD.EXE	whoami
2016-06-23 11:54:07	CMD.EXE	tasklist
2016-06-23 11:53:39	net start	C:\Windows\system32\net1 start
2016-06-23 11:53:39	CMD.EXE	net start
2016-06-23 11:53:35	CMD.EXE	netstat -ano
2016-06-23 11:53:29	CMD.EXE	net view
2016-06-23 11:51:19	CMD.EXE	ipconfig /all
2016-06-23 11:51:14	Rundll32.EXE "C:\ProgramData\[redacted]	CMD.EXE
2016-06-23 11:27:17	C:\Windows\system32\cmd.exe /c netstat -nao | findstr /r "LISTENING"	findstr /r "LISTENING"

Attempt to kill splunk process

_time	ParentCommandLine	CommandLine
2016 [illegible] 38:58	CMD.EXE	taskkill /f /im splunkd.exe
2016-[illegible] 4:48	CMD.EXE	find "1388"
2016-[illegible] 34:48	CMD.EXE	tasklist

Detections based on Sysmon EventID !=1

Sysmon EventID 3

Malware can hide but it Must Run and Communicate with C2

Regsvr32.exe

(using Sysmon EventID 3)

Malware uses legitimate windows executable for C2 communication

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets
lsass.exe	480	TCP	testmachine	49156	testmachine	0	LISTENING	
lsass.exe	480	TCPV6	testmachine	49156	testmachine	0	LISTENING	
regsvr32.exe	3640	TCP	testmachine	49335	79.142.77.157	http	SYN_SENT	
regsvr32.exe	3640	TCP	testmachine	49336	109.225.177.86	8080	SYN_SENT	
regsvr32.exe	3640	TCP	testmachine	49337	185.62.214.51	http	SYN_SENT	
regsvr32.exe	3640	TCP	testmachine	49338	58.214.89.219	8080	SYN_SENT	
regsvr32.exe	3640	TCP	testmachine	49339	136.94.134.27	http	SYN_SENT	
services.exe	464	TCP	testmachine	49155	testmachine	0	LISTENING	

Untangling Kovter's persistence methods : Malwarebytes Labs

LogName=Microsoft-Windows-Sysmon/Operational
EventCode=3
Image: C:\Windows\System32\regsvr32.exe

You don't need this detection rule if you have configure your host firewall to block outgoing connection from regsvr32.exe. Who has done this ☺

Rundll32.exe & DLL in user profile for C2 communication

- Question : Rundll32.exe is used by many programs to make legitimate network connections to Internet. How can we identify a malicious DLL dropped in user profile folder and use rundll32 for C2 communication?

- Answer : Correlate Sysmon EventID1 & 3

eventcode=1 commandline="*C:\\Users*\\AppData*

eventcode=3 Image="C:\\Windows\\System32\\rundll32.exe

Amongst others BlackEnergy APT dropper was using this technique
https://goo.gl/MRZsq8

Sysmon EventID 8

Malware can run as Thread of a remote Process

Malware as thread on remote process

(using Sysmon EventID 8)

Detection Rule: Find rare injections to browsers

Real Case : Malware bypass AV and injects code to IE

Search String: sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" eventcode=8 targetimage=*iexplore.exe | eval ppid=sourceimage+";"+targetimage |rare ppid

View results in Splunk

ppid	count
C:\[redacted];C:\Program Files (x86)\Internet Explorer\iexplore.exe	1
C:\Windows\System32\svchost.exe;C:\Program Files\Internet Explorer\iexplore.exe	750
C:\Windows\System32\wbem\WmiPrvSE.exe;C:\Program Files\Internet Explorer\iexplore.exe	2943
C:\Windows\System32\svchost.exe;C:\Program Files (x86)\Internet Explorer\iexplore.exe	8717

Attack against KeePass

(using Sysmon EventID 8)

Security in 2017: Ransomware will remain king

Posted December 14, 2016 by Malwarebytes Labs

Ransomware will become personal.

Most ransomware attacks today are indiscriminant. For the most part, cyber criminals issue ransomware at random, hitting anyone and everyone that they can. However, it's increasingly likely that *targeted* ransomware attacks will become the new norm.

Password managers will become a huge target.

In 2017, password managers, digital vaults where users store passwords and other authentication data, will become a huge target for cybercriminals.

KeeThief

Allows for the extraction of KeePass 2.X key material from memory, as well as the backdooring and enumeration of the KeePass trigger system.

- CreateRemoteThread detected:
- UtcTime: 2016-08-04 14:08:20.536
- **SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe**
- TargetProcessId: 11364
- **TargetImage: C:\Program Files (x86)\KeePass Password Safe 2\KeePass.exe**
- StartModule: C:\Windows\SYSTEM32\ntdll.dll
- StartFunction: DbgUiRemoteBreakin

Sysmon EventID 10

Malware access
lsass for credentials

Mimikatz

John Lambert
@JohnLaTwC

Following

Defense spurring offense: @gentilkiwi's #mimikatz now with least privilege to hide better :) twitter.com/gentilkiwi/sta …

Event Properties - Event 10, Sysmon

General | Details

```
Process accessed:
UtcTime: 2016-11-26 01:04:49.779
SourceProcessGUID: {310d7396-dfaf-5838-0000-0010bbcc
SourceProcessId: 3548
SourceThreadId: 3724
SourceImage: C:\temp\mimikatz.exe
TargetProcessGUID: {310d7396-dd6f-5838-0000-00101f620
TargetProcessId: 512
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1410
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+6aaea|C:\Windows\system32\KERNELBASE.dll+fbf8|C:
\temp\mimikatz.exe+4c5eb|C:\temp\mimikatz.exe+4c8b2|C:\temp\mimikatz.exe+4cc18|C:\temp
\mimikatz.exe+4c55a|C:\temp\mimikatz.exe+382cc|C:\temp\mimikatz.exe+3813f
```

GrantedAccess	permissions
0x00000010	VMRead
0x00000400	QueryInfo
0x00001000	QueryLimitedInfo

BUT many ways to run mimikatz without writing to disk

Detect Mimikatz when not written on disk

- Scenario : Run Cobaltstrike, elevate priv, dump creds (tested in win7)

Level	Date and Time	Source	Event ID	Task Category
Information	16/01/2017 12:28:12	Sysmon	10	Process accessed (rule: ProcessAccess)
Information	16/01/2017 12:22:55	Sysmon	10	Process accessed (rule: ProcessAccess)
Information	16/01/2017 12:22:46	Sysmon	10	Process accessed (rule: ProcessAccess)
Information	16/01/2017 12:12:22	Sysmon	10	Process accessed (rule: ProcessAccess)

Event 10, Sysmon

General Details

Process accessed:
UtcTime: 2017-01-16 11:28:12.405
SourceProcessGUID: {2ff1e125-ae4b-587c-0000-0010a4476300}
SourceProcessId: 2884
SourceThreadId: 3592
SourceImage: C:\WINDOWS\system32\rundll32.exe
TargetProcessGUID: {2ff1e125-aa70-587c-0000-0010bdab0000}
TargetProcessId: 708
TargetImage: C:\WINDOWS\system32\lsass.exe
GrantedAccess: 0x143a
CallTrace: C:\WINDOWS\SYSTEM32\ntdll.dll+4bf9a|C:\WINDOWS\system32\KERNELBASE.dll+189b7|UNKNOWN(0000000000222A68)

date	host	user	pid	activity
01/16 12:28	[illegible]	[illegible]	6412	run mimikatz's sekurlsa::logonpasswords command

Sysmon EventIDs 12-14

Malware uses Registry

Attackers try to avoid PSv5 logging

Using Sysmon Registry monitoring

- Configuration of PowerShell v5 in registry is written in keys under HKLM\software\policies\Microsoft\windows\powershell
  - https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.htm
- Its easy to monitor these keys and if there is any action there after initial configuration is at least suspicious!

Sysmon Events when attacker disables/enables PS Module and Transcription Logging

_time	TargetObject	Details
2017-01-16 17:21:11	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription\EnableInvocationHeader	1
2017-01-16 17:21:11	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription\EnableTranscripting	1
2017-01-16 17:21:11	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\EnableModuleLogging	1
2017-01-16 14:45:35	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription\EnableInvocationHeader	0
2017-01-16 14:45:22	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\Transcription\EnableTranscripting	0
2017-01-16 14:44:26	\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\EnableModuleLogging	0

Persistence using Run keys

- One of the techniques used to establish persistence is to be executed at system startup by adding a registry value under any of the following registry keys:
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run[Once]\
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run[Once]\

- In an enterprise network admins maybe use these keys to run legitimate things in startup ☺ that must be excluded
- Amongst others Cozyduke and Dridex was using this technique
  - https://www.f-secure.com/documents/996508/1030745/CozyDuke

Before the computer shuts down, Cridex dumps the DLL to the %APPDATA% folder creates the following registry key so that the threat runs each time Windows starts:

```
HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Run "wmnotify
Type: REG_SZ
Data: " rundll32.exe C:\DOCUME~1\[User Name]\APPLIC~1\1.tmp NfInitialize"
```

AppInit DLLs *

(using Sysmon EventID 13)

DLLs that are specified in the AppInit_DLLs value in the Registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows are loaded by user32.dll into every process that loads user32.dll

```
index=[redacted] AppInit_DLLs | table ComputerName,TargetObject,Details
```

✓ 2 events (1/5/17 4:10:00.000 PM to 1/5/17 5:10:42.000 PM) No Event Sampling

Events | Patterns | Statistics (2) | Visualization

100 Per Page | Format | Preview

ComputerName	TargetObject	Details
[redacted]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs	[redacted]pih.dll
[redacted]	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs	[redacted]pih.dll

*The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled but windows 7 is still alive!

Local Port Monitor

A port monitor can be set through the AddMonitor API call to set a DLL to be loaded at startup.[1] This DLL must be located in `C:\Windows\System32` and will be loaded by the print spooler service, spoolsv.exe, on boot.[2] Adversaries can use this technique to load malicious code at startup that will persist on system reboot.

This same functionality is achieved by creating specifically formatted Registry keys at `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors`.[2]

- Monitor registry writes to HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors

Sysmon EventID 15

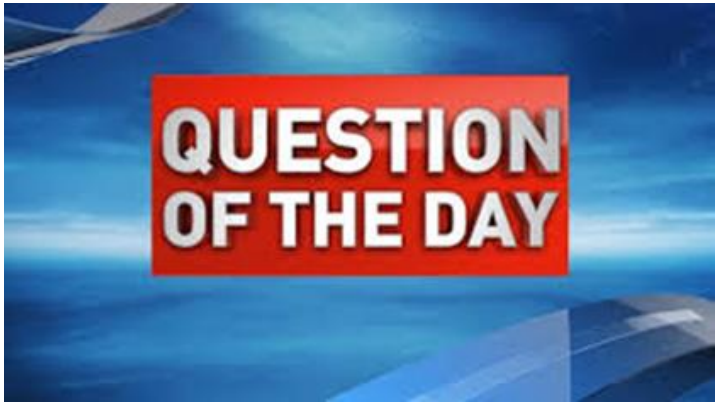
Malware is delivered through email attachments

Useful for Incident Response

Find which users have opened a malicious attachment for which the hash is known

Very useful in IR

1/6/17 5:46:00.000 PM	01/06/2017 05:46:00 PM LogName=Microsoft-Windows-Sysmon/Operational SourceName=Microsoft-Windows-Sysmon EventCode=15 EventType=4 Type=Information ComputerName=[redacted] User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 TaskCategory=File stream created (rule: FileCreateStreamHash) OpCode=Info RecordNumber=1571816 Keywords=None Message=File stream created: UtcTime: 2017-01-06 16:46:00.216 ProcessGuid: {2E8B67F6-7A2F-586B-0000-0010F3290D00} ProcessId: 3832 Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe TargetFilename: C:\Users\[redacted]\Downloads\[redacted].pdf CreationUtcTime: 2017-01-06 16:46:00.010 Hash: SHA256=AABD0759AC605EF8E9FD80E3045F05C85660C9E8E91A87D3



Can we trust Event Logging?

However, the listed plugin "EventLogEdit" is significant for digital forensics and incident response (DFIR) professionals investigating APT cases. While we understand that event logs can be cleared and event logging stopped, surgically editing event logs is usually considered to be a very advanced capability (if possible at all). We've seen rootkit code over the years (some was published on the now defunct rootkit.com) that supported this feature, but often made the system unstable in the process.

http://malwarejake.blogspot.be/2017/01/implications-of-newest-shadow-brokers.html

Takeaways

Takeaways

#1 Together with Bro IDS and an open source solution for data analysis like ELK is a **free** "Advanced Detection Solution".

#2 Centralization of logs is easy and without big investments using WEC. Creating alerts without false positives in some cases is very challenging.

#3 Sysmon doesn't hide itself and we still need to analyse windows events

#4 By analyzing sysmon logs to trace anomalies you can be a GREAT Analyst ☺

Take Away #5
Raise the bar of your detection capabilities

Install Sysmon

"Traditional Defenders think about stopping attacks
Modern Defenders think about increasing attacker requirement"

John Lambert
Microsoft General Manager

Take Away #6 reduce the number of admins!

#Mimikatz can patch EventLog Service and stop ALL logging.

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # event::drop
"EventLog" service patched

mimikatz # _
```

Casey Smith @subTee · Apr 6

This is a blast!

I have my arbitrary Log Writer to SysMon/Operational Log working.

Complete Control Over Messages

Stop ALL logging can be detected what if malware selectively hides events?

Mark Russinovich @markrussinovich · Apr 20

@subTee Admin == game over. Hopefully sysmon captures initial entry, and events shipped off box before malware activates.

Stay Tuned

RSAConference | Where the world talks security

EVENTS | BLOGS | VIDEOS | JOB BOARD | Search the site...

USA 2017 February 13 – 17 Moscone Center, San Francisco

POWER OF OPPORTUNITY

Register

- USA 2017
- Register
- Agenda
- NEW for 2017
- Keynotes
- Reserve a Seat
- **Sessions & Events**
- Monday Activities
- Special Events
- Topics & Tracks

How to Go from Responding to Hunting with Sysinternals Sysmon

Reserve a Seat | February 14, 2017 | 1:15 PM - 2:00 PM | Moscone South | 306

← View all Sessions

Sysinternals Sysmon can help you precisely detect and track an attacker's movement inside your Windows networks, but only if you know how to use it effectively. Get a deep dive from Sysmon's author on its design, capabilities, latest enhancements, and guidance for collecting and alerting on its rich forensic data with popular log analytics services.

Session Code:
HTA-T09

Core Topics:
Hackers & Threats

Delivery Format:
Classroom

Classification:

THANK YOU
@dmargaritis