Extending Your Incident Response Capabilities with Sysmon

Improving Your Threat Hunting Abilities

@petermorin123

Peter Morin

- Over 20yrs in the field
- Halifax, Nova Scotia
- KPMG Cyber Security practice
- IR, threat hunting, cloud security, insider threat, protection of critical infrastructure and incident response

Intro

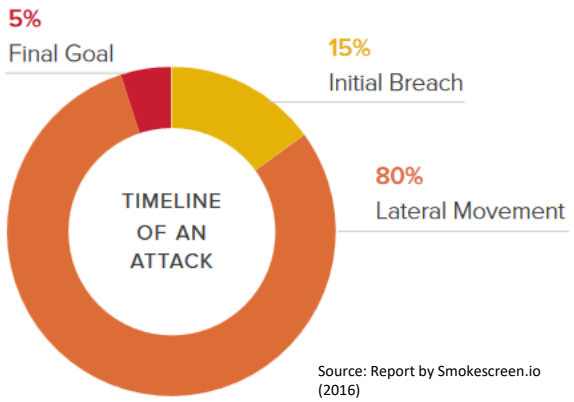
- Talk about the free Sysinternals tool, **Sysmon**.
  - Sysmon tool and compare its outputs to standard EVT logs
  - Malware – the infection point, whether or not it has spread, and the effects on the infected system
  - Sysmon command line usage, understanding its events and configuration options including the use of configuration file
  - Use cases where Sysmon can improve your detection and IR capabilities

State of Cyber Defense

- Traditional defensive posture
  - Maintain a strong perimeter
  - Implement layered security controls
  - Block known attacks and malicious IP addresses
  - Policies to discourage misuse or insider threat
  - Basic endpoint security products

Detecting Lateral Movements

- Initial breach **normally doesn't yield value** to attackers
- Important part of the attack - hands on keyboard ($$$ being spent)
- 80% of the attack is spent during lateral movement
- Your biggest win
- Attacker is moving blindly



Source: Report by Smokescreen.io (2016)

Typical Lateral Movements

- Goal is to stay under the radar
- Attackers use “legitimate” sysadmin tools
- Typical methods
  - Pass-the-hash (theft of NTLM hashes)
  - SMB scanning (i.e. file shares)
  - PowerShell scripts
  - Psexec
  - Windows Management Instrumentation (WMI)
  - RDP and other remote access (i.e. VNC)
  - Password brute-force

Can we win?

- You have to be really in touch with what your network looks like, its assets and humans.
- Prevent Attackers from achieving their goal
- Reduce Attack Dwell Time
- Change Mindset – focus on behavior
- **Adapt…adapt…adapt!**

Why Threat Hunting?

- Investigating at **enterprise-scale**
- **Repeatable** analysis tasks for both **proactive** and **reactive** hunting
- Finding evidence of compromise with minimal leads
- **Less on detection** technology and more on key attacker **tactics, techniques, and procedures (TTPs)** and related **behaviors**

86%
IT professionals say that their organization **is involved in some kind of threat hunting**.

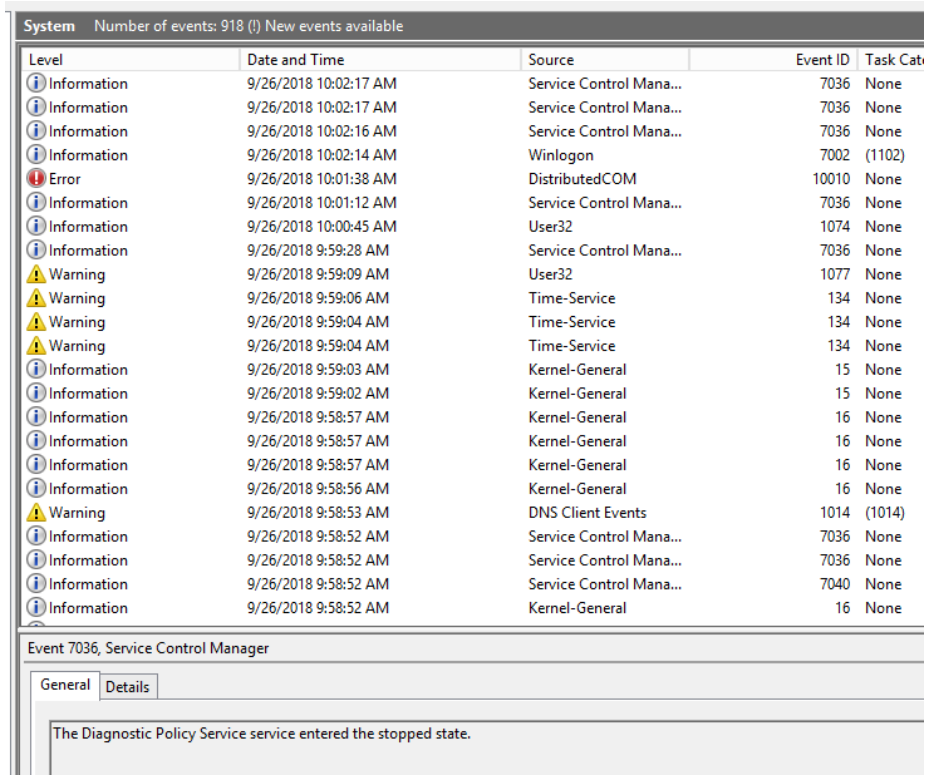
Source: 2016 SANS Survey

Threat Hunting - Questions

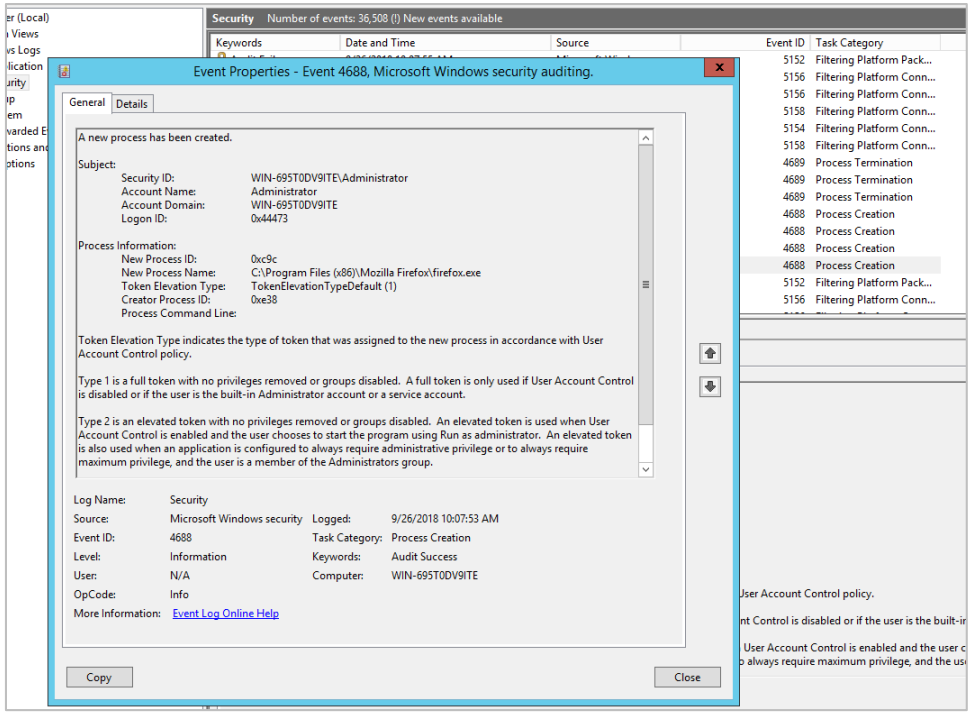
- Network breach or you get hit with malware
  - What was the entry point?
  - Did they spread between systems?
  - What happened on a particular system?
- Built-in Windows tooling - hard to answer questions
  - process creates and DLL loading info is limited
  - Network connection information can be too limited and also too verbose
  - Common attacker behavior (i.e. thread injection) not captured

Windows Event logs

- Local log files where events occurring a Windows system are documented
  - **Application** –logged by an application
  - **System** - logged by the O/S
  - **Security** – security of the system
- Events are tracked by **Event ID**
- Security events: User logon/logoff, Privilege use and Object access, etc.
- **Single most import piece of security data** on a Windows host – short of using a third-party endpoint agent or collecting memory



Event Logs – Data Limitations



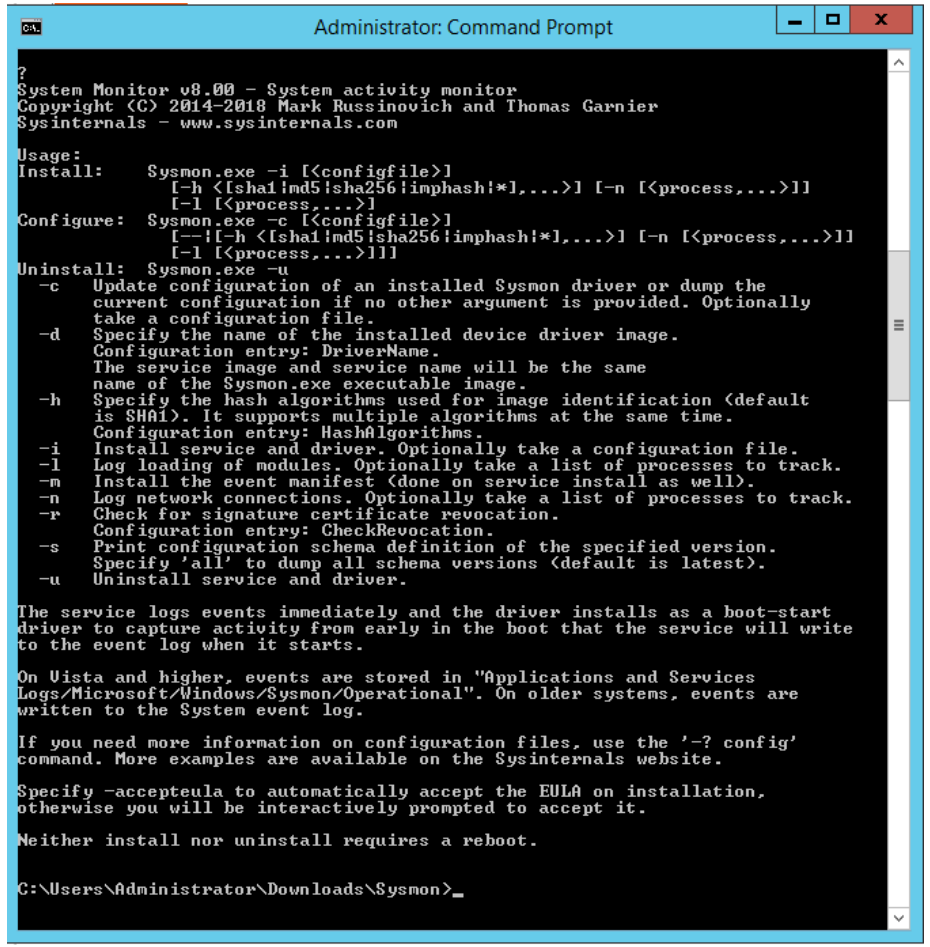
- Some events missing all together
- Other events missing important information
- No way to filter what is logged
- **Event 4688** (new process created)
  - Program name
  - Process path
  - Process ID
  - Info about who executed it

What is Sysmon?

- Microsoft System Monitor
- Version 8 is available at sysinternals.com
- Windows Sysinternals Suite / Mark Russinovich
- Windows service and device driver (2 MB)
  - Single binary includes 32-bit and 64-bit versions of both
  - Service doubles as command-line frontend
  - Logs system activity to the EventLog

Installation

- **sysmon -i -accepteula [options]**
  - Extracts binaries into %systemroot%
  - Registers event log manifest
  - Enables default configuration
  - Option such as the hashing method, etc.
- Can be installed from a network location
  - \\ServerName\sysmon -accepteula -i [OPTIONS]
  - Sysmon will copy it’s files to the local system



Installation Options

- -h [hash,...] = Specify which hash types to record.
  - Use "*" for all or -h SHA256 to turn on SHA256 for example
  - Options are MD5, SHA1, SHA256, and IMPHASH.

Installation Options

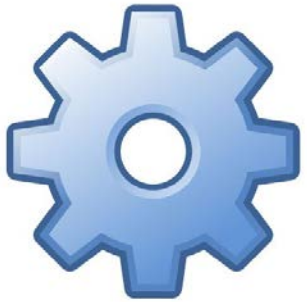
- -n [process,...] = Enable logging of network connections (potential performance hit).
  - You can specify a single process by using a process name like -n **firefox.exe,cmd.exe,powershell.exe**
  - **You will not see any Event ID: 3 events**

Installation Options

- -l [process,...] = Enable logging of image loaded events (potential performance hit).
  - You can specify a single process by using a process name like -l **iexplore.exe,calc.exe**
  - **You will not see any Event ID: 7 events (image loaded)**

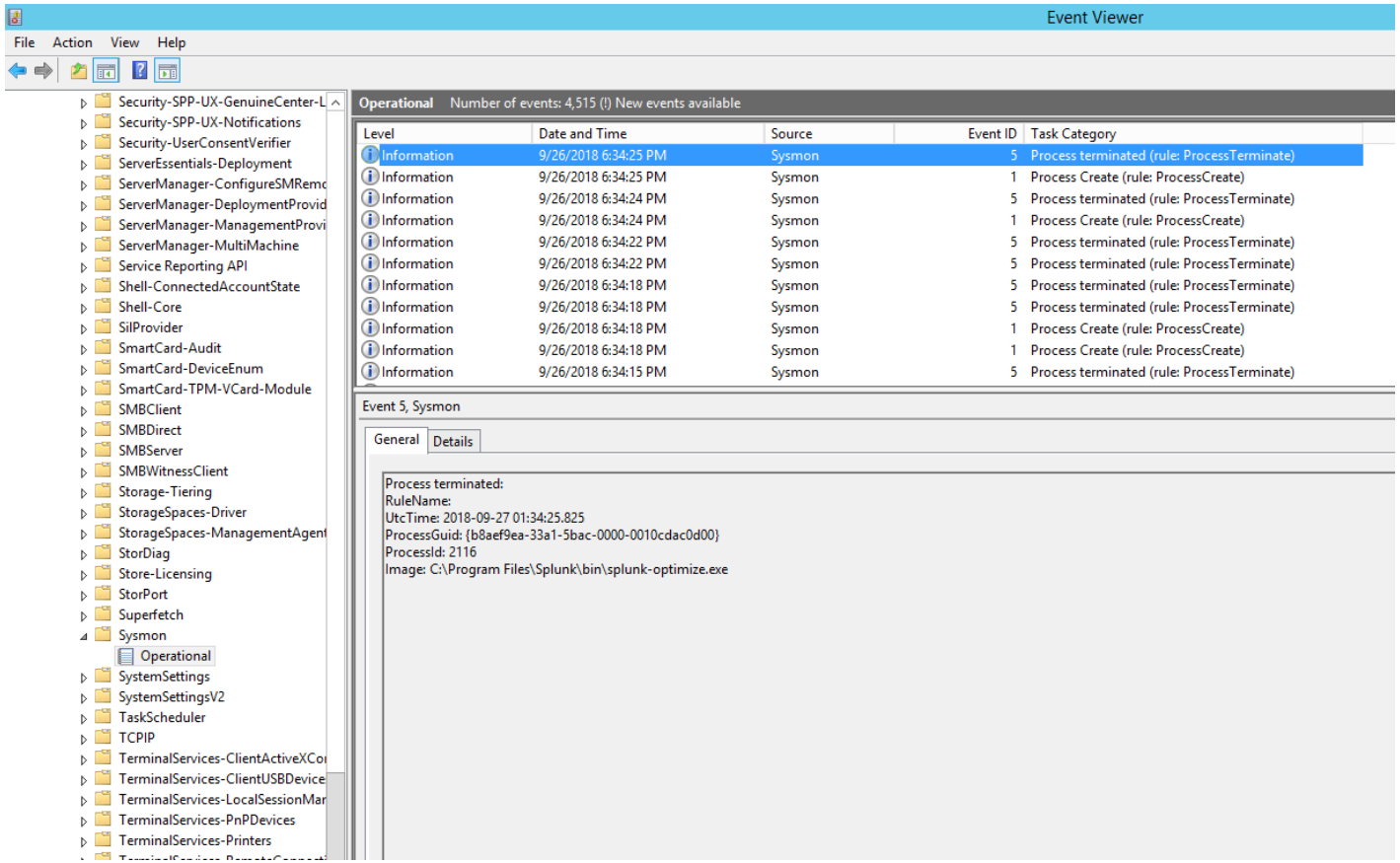
Sysmon Events

- The service logs events immediately
- Driver installs as a boot-start driver to capture activity from early in the boot process
- Sysmon does not replace your existing event logs



Sysmon Events

Applications and Services Logs/Microsoft/Windows/Sysmon/Operational



Sysmon Events

Event ID	Category	Description
1	Process creation	extended information about a newly created process
2	A process changed a file creation time	registered when a file creation time is explicitly modified by a process
3	Network connection	logs TCP/UDP connections on the machine
4	Sysmon service state changed	reports the state of the Sysmon service (started or stopped)
5	Process terminated	reports when a process terminates
6	Driver loaded	provides information about a driver being loaded on the system
7	Image loaded	when a module is loaded in a specific process
8	CreateRemoteThread	detects when a process creates a thread in another process
9	RawAccessRead	detects when a process conducts reading operations from the drive using the \\.\ denotation
10	ProcessAccess	process opens another process, an operation that's often followed by information queries or reading and writing the address space of the target process.
11	FileCreate	File create operations are logged when a file is created or overwritten
12	RegistryEvent (Object create and delete)	Registry key and value create and delete operations map to this event type

Sysmon Events

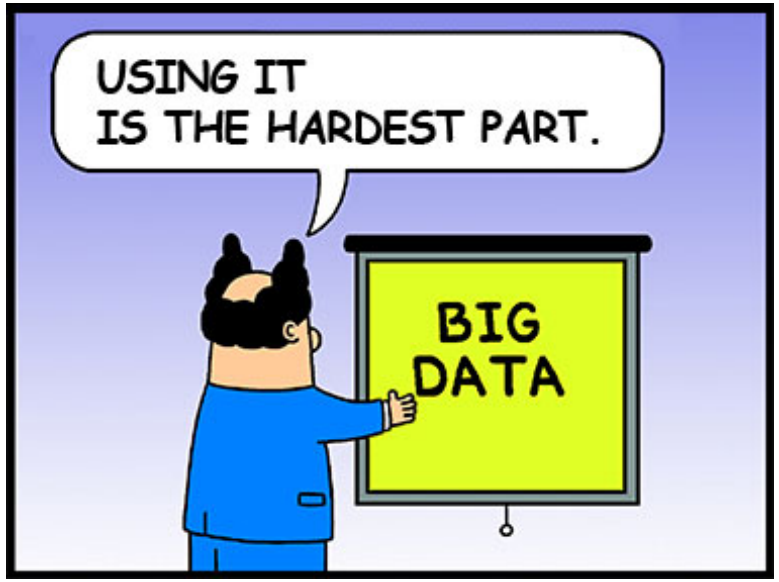
Event ID	Category	Description
13	RegistryEvent (Value Set)	This Registry event type identifies Registry value modifications
14	RegistryEvent (Key and Value Rename)	Registry key and value rename operations map to this event type, recording the new name of the key or value that was renamed
15	FileCreateStreamHash	when a named file stream is created, and it generates events that log the hash of the contents of the file to which the stream is assigned (the unnamed stream), as well as the contents of the named stream
16	Sysmon Configuration Changed	reports any changes to the Sysmon configuration
17	PipeEvent (Pipe Created)	when a named pipe is created
18	PipeEvent (Pipe Connected)	when a named pipe connection is made between a client and a server
19	WmiEvent (WmiEventFilter activity detected)	When a WMI event filter is registered
20	WmiEvent (WmiEventConsumer activity detected)	logs the registration of WMI consumers, recording the consumer name, log, and destination
21	WmiEvent (WmiEventConsumerToFilter activity detected)	When a consumer binds to a filter, this event logs the consumer name and filter path.
255	Error	This event is generated when an error occurred within Sysmon

Why are these important?

- **Event ID 11: FileCreate**
  - Useful for monitoring autostart locations (i.e. temporary and download directories)
  - Common places malware drops during initial infection.
- **Event ID 12: RegistryEvent** (Object create and delete)
  - Useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.
- **Event ID 17: PipeEvent** (Pipe Created)
  - Malware often uses named pipes for inter-process communication.

Death by Data

- It can log, a huge amount of data
  - Process launches
  - DLLs loaded by processes, drivers by the system
  - Network connections
  - Etc….
- As you can imagine, **this can quickly add up** if you don't need to see every single thing that happens in Windows…



Sysmon Config Files

- Sysmon includes the ability to filter events before they are written to the Event Log – **these are key!**
- You can build (or download) configuration files
- They make it easier to deploy a preset configuration and to filter captured events.

Configuration

- You can do things like: only log network events from processes named “iexplore.exe” or located in C:\Users, drivers not signed by Microsoft, etc.
- It's up to you to determine how much data you want included.
- Sysmon configuration file
  - install: sysmon -i -accepteula c:\SysmonConfig.xml
  - update: sysmon -c c:\SysmonConfig.xml
  - use Psexec or PowerShell during an IR

Event Tags

- Each event is specified using its tag
- To see all tags, dump the full configuration schema:
  - **sysmon -s**
- "onmatch" can be "include" or "exclude"
  - Include and exclude refer to filter effect

```
<tag onmatch="exclude">
        <exclude filter/>
        …
</tag>

<tag onmatch="include">
        <include filter/>
        …
</tag>
```

Source: Mark Russinovich

Filter Examples

- Include only Google Chrome network activity:

```
<NetworkConnect onmatch="include">
        <Image condition="contains">chrome.exe</Image>
 </NetworkConnect >
```

- Include thread injections into winlogon and lsass:

```
<CreateRemoteThread onmatch="include">
        <TargetImage condition="image">lsass.exe</TargetImage>
        <TargetImage condition="image">winlogon.exe</TargetImage>
 </CreateRemoteThread >
```

- Exclude all Microsoft-signed image loads:

```
<ImageLoad onmatch="exclude">
        <Signature condition="contains">microsoft</Signature>
</ImageLoad>
```

Source: Mark Russinovich

Event Tags With No Filters

- Useful for enabling specific event types
- If no filter, onmatch has opposite effect:
  - Include: won't log any events
  - Exclude: log all events of the tag type
- This configuration enables the following:
  - ProcessCreate: because of onmatch exclude
  - ProcessTerminate: because it is omitted and by default enabled

```
<Sysmon  schemaversion="2.01">
  <EventFiltering>
    <ProcessCreate onmatch="exclude"/>
    <DriverLoad onmatch="include"/>
    <ImageLoad onmatch="include"/>
    <FileCreateTime onmatch="include"/>
    <NetworkConnect onmatch="include"/>
    <CreateRemoteThread onmatch="include"/>
    <RawAccessRead onmatch="include"/>
  </EventFiltering>
</Sysmon>
```

Source: Mark Russinovich

Good Example

- Exclude Splunk binaries on a Universal Forwarder:

```
<ProcessCreate onmatch="exclude">
    <ParentImage condition="is">
        C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe
    </ParentImage>
    <ParentImage condition="is">
        C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe
    </ParentImage>
    <ParentImage condition="is">
        C:\Program Files\SplunkUniversalForwarder\bin\btool.exe
    </ParentImage>
</ProcessCreate>
```

@SwiftOnSecurity's Configuration

- Very common go-to Sysmon config
- Follows MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) to identify attacker behavior
- Regularly updating the config to include information from the community (i.e. ion-storm)
- **https://github.com/SwiftOnSecurity/sysmon-config**

@SwiftOnSecurity's Configuration

```
    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <!--COMMENT: By default this configuration takes a very conservative approach to netwo
    <!--COMMENT: [ https://attack.mitre.org/wiki/Command_and_Control ] [ https://attack.r
    <!--TECHNICAL: For the DestinationHostname, Sysmon uses the GetNameInfo API, which
    filtering.-->
    <!--TECHNICAL: For the DestinationPortName, Sysmon uses the GetNameInfo API for the
    <!--TECHNICAL: These exe do not initiate their connections, and thus includes do not wor
    <!-- https://www.first.org/resources/papers/conf2017/APT-Log-Analysis-Tracking-Attack-
    <!--DATA: UtcTime, ProcessGuid, ProcessId, Image, User, Protocol, Initiated, SourceIsIpv
    DestinationIp, DestinationHostname, DestinationPort, DestinationPortName-->
<NetworkConnect onmatch="include">
        <!--Suspicious sources for network-connecting binaries-->
    <Image condition="begin with">C:\Users</Image>
        <!--Tools downloaded by users can use other processes for networking, but this is a v
    <Image condition="begin with">C:\ProgramData</Image>
        <!--Normally, network communications should be sourced from "Program Files" not fr
    <Image condition="begin with">C:\Windows\Temp</Image>
        <!--Suspicious anything would communicate from the system-level temp directory-->
        <!--Suspicious Windows tools-->
    <Image condition="image">at.exe</Image>
        <!--Microsoft:Windows: Remote task scheduling, removed in Win10 | Credit @ion-sto
    <Image condition="image">certutil.exe</Image>
        <!--Microsoft:Windows: Certificate tool can contact outbound | Credit @ion-storm @F
    <Image condition="image">cmd.exe</Image>
        <!--Microsoft:Windows: Remote command prompt-->
    <Image condition="image">cmstp.exe</Image>
        <!--Microsoft:Windows: Connection manager profiles can launch executables from We
        @NickTyrer @Oddvarmoe @KyleHanslovan @subTee -->
```

- Network traffic sourced from C:\ProgramData or c:\Windows\Temp
- Network connections using nc.exe
- Etc….

Let’s Talk Events - 4688

- Sysmon events to detect new EXEs and DLLs
- Could have been used to detect ransomware such as Petya or Wannacry which used SMB to spread
- Work was done by an EXE – if we would have been looking for new (unknown) EXEs and DLLs
- **Event ID 4688** Process Creation for success, is a Security log event produced every time an EXE loads as a new process.

Event 4688 vs. 1

- If we simply keep a **running baseline of known EXE names** and compare each **4688** against that list, you'll know as soon as something new, like **Petya's EXEs**, run on your network.
- The only problem with using 4688 is it's based on **EXE name** (including path)
- What happens if the attacker uses a name similar to that of a known file (C:\Windows\mssecsvc.exe or overwrites an exe (i.e. notepad.exe)?

Event 4688 vs. 1

- **Sysmon logs the hash of each EXE**.
- Sysmon event ID 1 is logged the same time as 4688 but it also provides the hash of the EXE.
- Even if the attacker does replace a known EXE, the hash will change
- Your comparison against known hashes will fail – thus detecting a **new EXE executing** for the first time in your environment

Event 1, Sysmon

General Details

```
Process Create:
UtcTime: 2016-04-17 07:16:05.332
ProcessGuid: {1ecf1276-3835-5713-0000-0010a1bc3200}
ProcessId: 6856
Image: C:\Windows\System32\eventvwr.exe
CommandLine: "C:\Windows\System32\eventvwr.exe"
CurrentDirectory: C:\WINDOWS\system32\
User: MOTI-PC\motib
LogonGuid: {1ecf1276-2e3b-5713-0000-002001ef0400}
LogonId: 0x4EF01
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=7A2C326970EFF8B9E2194377078B22944808CB71
ParentProcessGuid: {1ecf1276-2e3c-5713-0000-0010dd560500}
ParentProcessId: 4432
```

Event 4688 vs. 1

Information 9/13/2014 12:21:04 PM Sysmon

Event 1, Sysmon

General Details

Process Create:
UtcTime: 9/13/2014 7:21 PM
ProcessGuid: {00000000-9920-5414-0000-0010ba4b8a02}
ProcessId: 3928
Image: C:\Users\test\AppData\Local\Temp\drvinst-2.exe
CommandLine: "C:\Users\test\AppData\Local\Temp\drvinst-2.exe" /ci 10298 /e
User: Vera-PC\test
LogonGuid: {00000000-d33f-5412-0000-0020a7d11701}
LogonId: 0x117D1A7
TerminalSessionId: 1
IntegrityLevel: Medium
HashType: SHA1
Hash: 7297DFCED5D4686860F5936015EAC1085EFBFD42
ParentProcessGuid: {00000000-96e0-5414-0000-0010e31cba02}
ParentProcessId: 1044
ParentImage: C:\Users\test\AppData\Local\SwvUpdater\Updater.exe
ParentCommandLine: C:\Users\test\AppData\Local\SwvUpdater\Updater.exe

Antivirus scan for a96b6

virustotal

SHA256: a96b6460cf356fceac19e7ef65da417d7475b70067804ff7d4665b64ee0965fd
File name: inethnfd-setup.exe
Detection ratio: 22 / 55
Analysis date: 2014-09-15 04:39:59 UTC (1 year, 5 months ago)

0 0

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
AVG	Generic_r.TL	20140915
Agnitum	PUA.Amonetize!	20140914

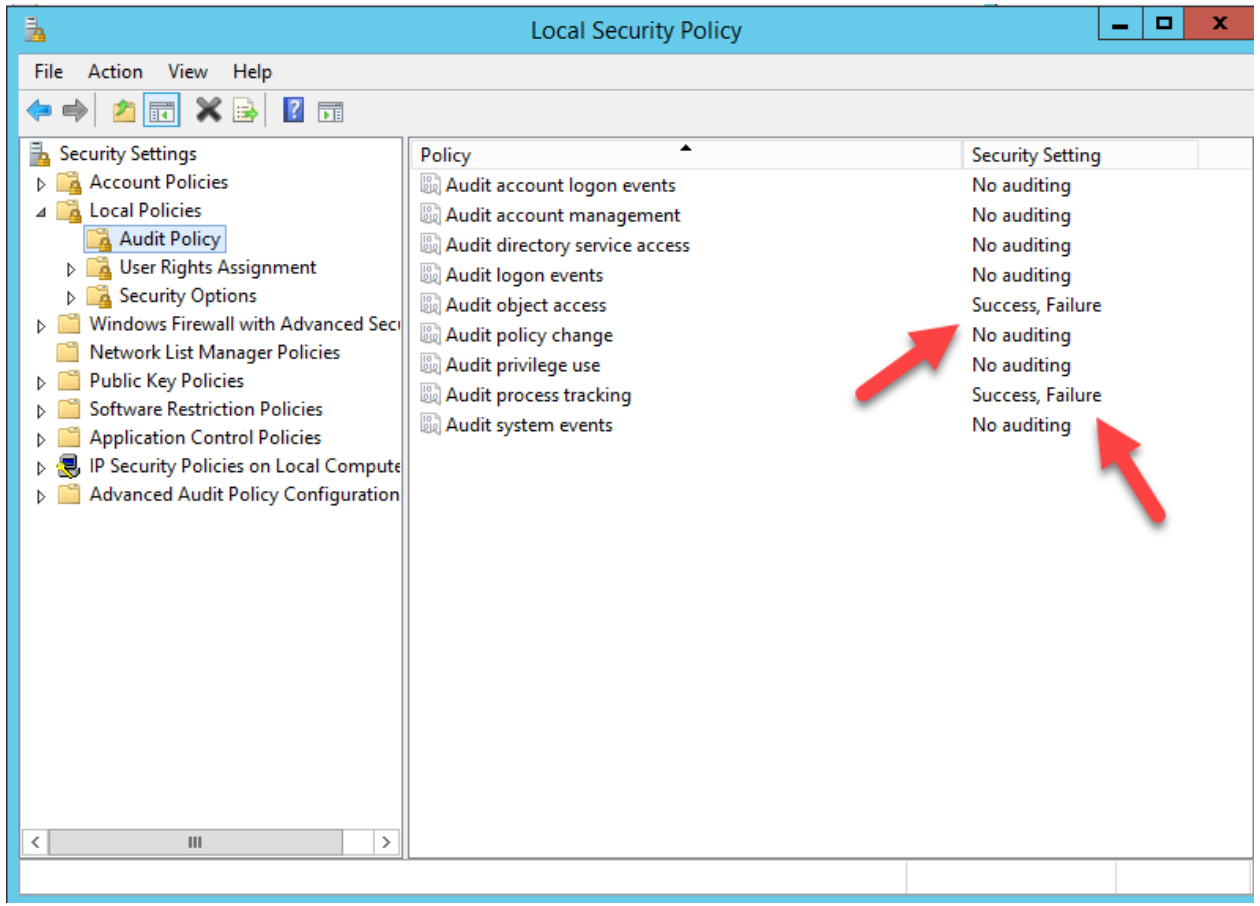
@petermorin123

Event 4688 vs. 1

- Logs **process creation** with **full command line** for both current and parent processes
- Records the hash of process image files using SHA1 (the default), MD5 or SHA256
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs
- Optionally **logs network connections**, including each connection's source process, IP addresses, port numbers, hostnames and port names

Object Auditing

- Object Auditing must be enabled for Process Create events to show up



Use Cases

- **Productivity App** (e.g. Word, Excel, PowerPoint, Outlook) **launches cmd.exe or powershell.exe**
  - Productivity applications launching shells may be indicative of a malicious document or email.
  - After eliminating any exceptions, this should be a very high fidelity pattern, indicating something malicious happening.

General | Details

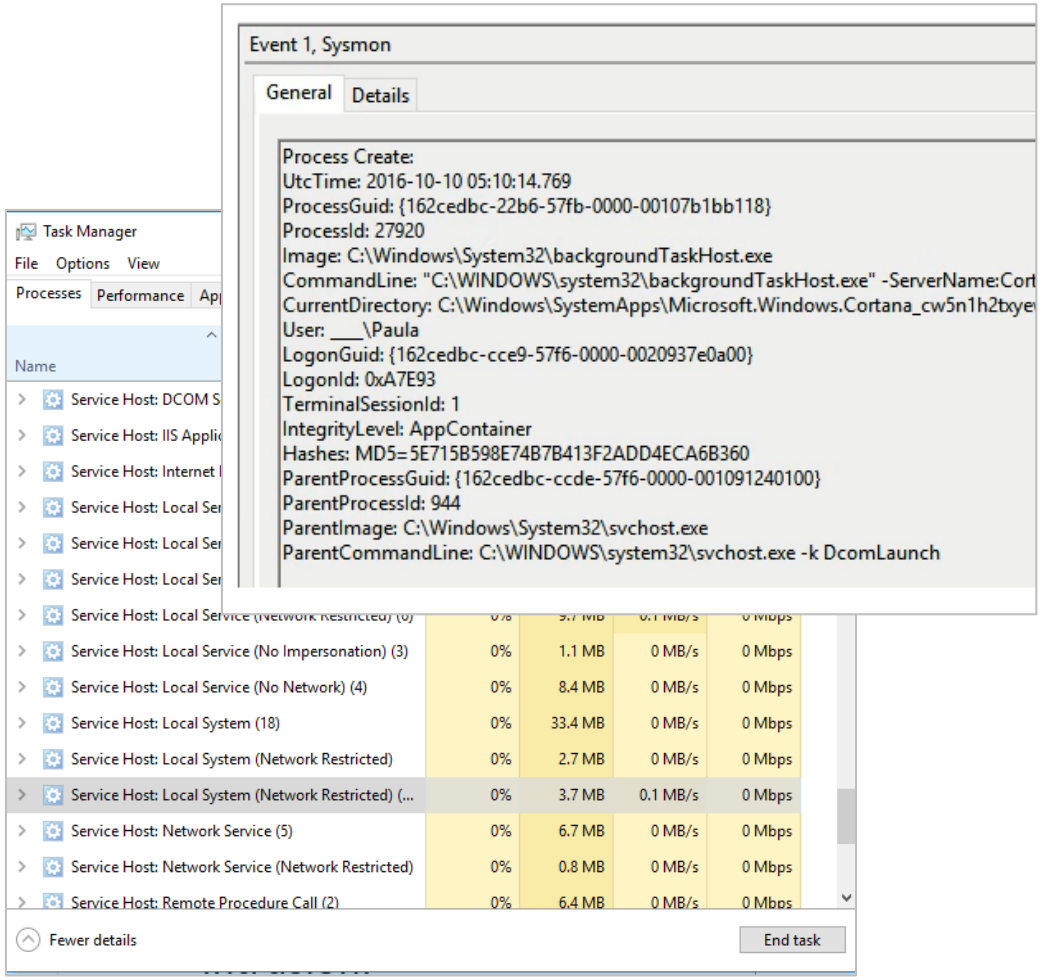
```
Process Create:
UtcTime: 2017-04-06 03:03:01.926
ProcessGuid: {3424c687-afe5-58e5-0000-001084319c01}
ProcessId: 3872
Image: C:\Windows\SysWOW64\cmd.exe
CommandLine: "C:\Windows\System32\cmd.exe" /c calc.exe
CurrentDirectory: C:\Users\labuser\Desktop\
User: LabWin8\labuser
LogonGuid: {3424c687-dfea-58e3-0000-0020a5680100}
LogonId: 0x168A5
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: MD5=59A1D4FACD7B333F76C4142CD42D3ABA
ParentProcessGuid: {3424c687-afe1-58e5-0000-001078019c01}
ParentProcessId: 2068
ParentImage: C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE
ParentCommandLine: "C:\Program Files (x86)\Microsoft Office\Office15\WINWORD.EXE" /n "C:
\Users\labuser\Desktop\bad.doc" /o ""
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	4/5/2017 8:03:02 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreat
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	LabWin8
OpCode:	Info		
More Information:	Event Log Online Help		

Source: Vector8 Blog

Use Cases

- **Abnormal parent of svchost.exe**
  - The parent of **svchost.exe is normally services.exe**.
  - Attackers use the name svchost.exe to hide their operations - often several svchosts running on a typical Windows host.
  - Also, the actual svchost.exe may be called by a malicious program in order to achieve the intent of the intrusion.



Source: Vector8 Blog

Use Cases

- **Whoami.exe running**
  - While whoami.exe is a standard Windows executable that you may see running occasionally
  - Provides current user on your computer, including your login name, groups you belong to, privileges, etc.
  - it's not very common for your average user to run it – **usually not by PowerShell**
  - whoami is used by system administrators, attackers, etc.
  - This pattern might serve more as a hunting lead than a stand-alone detection.

Command Prompt

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\petermorin>whoami.exe
ca\petermorin
```

```
Process Create:
UtcTime: 2016-12-30 20:55:21.119
ProcessGuid: {24140161-c9b9-5866-0000-0010fd781800}
ProcessId: 1092
Image: C:\Windows\System32\whoami.exe
CommandLine: "C:\Windows\system32\whoami.exe"  /user
CurrentDirectory: C:\Users\nzelada.HF\Documents\
User: HF\nzelada
LogonGuid: {24140161-c859-5866-0000-002091040c00}
LogonId: 0xc0491
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=EC2231C0FEA6B821A5ED097419744205
ParentProcessGuid: {24140161-c9b7-5866-0000-00108b491800}
ParentProcessId: 3080
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -s -
NoLogo -NoProfile
```

Source: Vector8 Blog

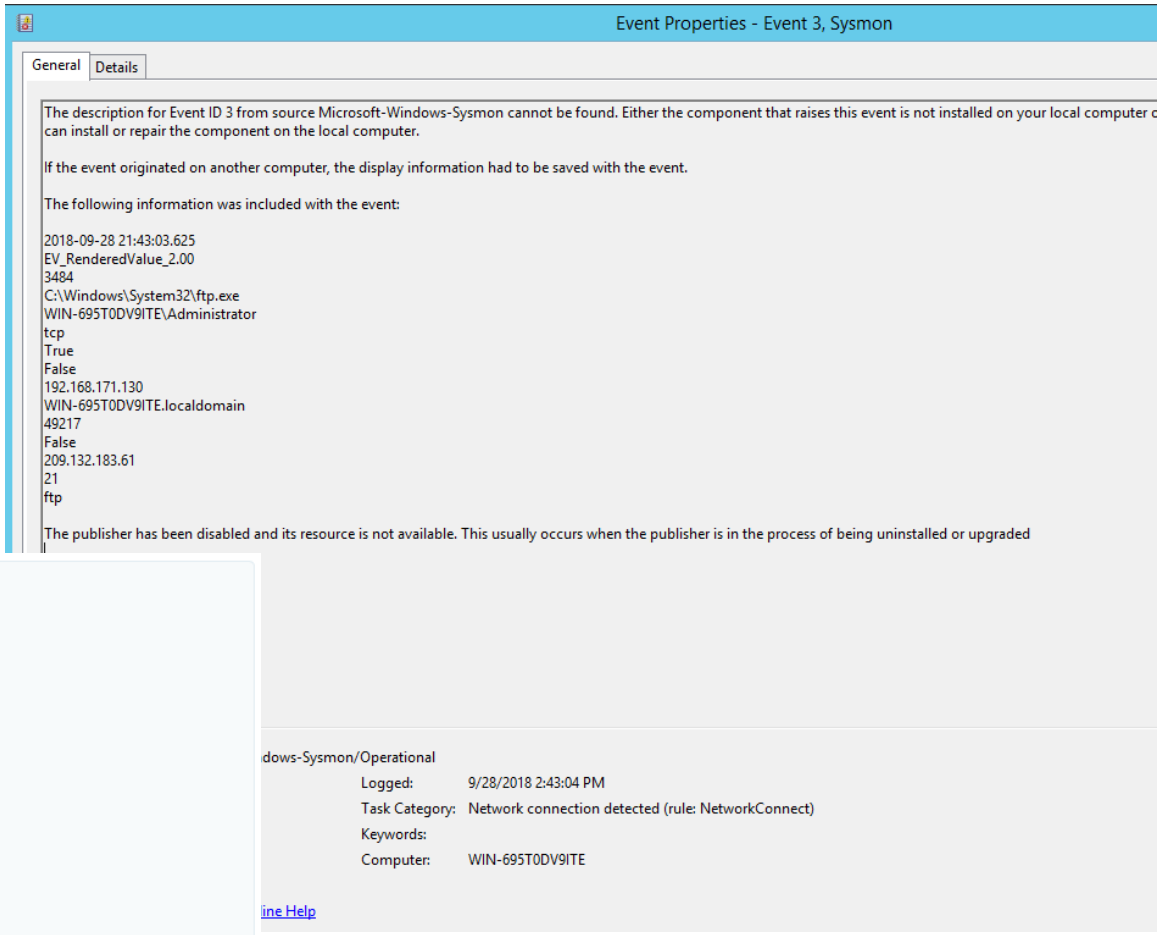
Use Cases

- **net.exe use ***
  - Similar to whoami, “net use” is occasionally used by administrators, and very often used by attackers to move laterally across your environment.
  - A more sophisticated use of these two patterns might be to combine them and look for the **occurrence of whoami.exe and net.exe occurring on the same system in a short time window.**

Source: Vector8 Blog

Use Cases

- **Exfiltration of data**, tracking network connections.




```
<NetworkConnect onmatch="include">
    <DestinationPort condition="is">80</DestinationPort>
    <DestinationIp condition="is">1.2.3.4</DestinationIp>
    <DestionationPortName
condition="is">kerberos</DestionationPortName>
</NetworkConnect>
```

Use Cases

- **Mimikatz**
- Process injection - Inject a DLL into the lsass process and start up a thread
- Allowing Mimikatz to access and do what lsass can
- Standard EVT does not log this
- Sysmon provides this information

General Details

```
Process accessed:
UtcTime: 2017-02-13 04:27:33.709
SourceProcessGUID: {889f23d9-35b2-58a1-0000-001005c7b900}
SourceProcessId: 2220
SourceThreadId: 4904
SourceImage: C:\demo\mimikatz.exe
TargetProcessGUID: {889f23d9-e575-58a0-0000-0010c64f0000}
TargetProcessId: 544
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1410
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+a5594|C:\Windows\system32\KERNELBA
665e2|C:\demo\mimikatz.exe+6694d|C:\demo\mimikatz.exe+66521|C:\demo\mimika
49be7|C:\demo\mimikatz.exe+499d1|C:\demo\mimikatz.exe+6bc45|C:\Windows\syst
\Windows\SYSTEM32\ntdll.dll+5c5b4
```

Use Cases

Event Code 10: “Process Accessed” – When lsass is accessed

```
"mimikatz" NOT "EventCode=4658" NOT "EventCode=4689" EventCode=10 | stats count by _time, SourceImage, TargetImage, GrantedAccess
```

✓ 27 events (04/09/2017 03:00:41.000 to 04/09/2017 03:45:41.001) No Event Sampling

Job

Events | Patterns | Statistics (13) | Visualization

20 Per Page | Format | Preview

_time	SourceImage	TargetImage	GrantedAccess
2017-09-04 03:26:29	C:\Windows\system32\cmd.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1FFFFF
2017-09-04 03:26:29	C:\Windows\system32\conhost.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1FFFFF
2017-09-04 03:26:29	C:\Windows\system32\csrss.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1FFFFF
2017-09-04 03:26:29	C:\Windows\system32\taskmgr.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1000
2017-09-04 03:26:29	C:\Windows\system32\taskmgr.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1400
2017-09-04 03:26:29	C:\Windows\system32\taskmgr.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1410
2017-09-04 03:26:30	C:\Windows\system32\lsass.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1000
2017-09-04 03:26:30	C:\Windows\system32\lsass.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1478
2017-09-04 03:26:39	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	C:\Windows\system32\lsass.exe	0x1010
2017-09-04 03:26:40	C:\Windows\system32\wbem\wmiprvse.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	0x1400

Event Code 7 – “Image Loaded” – We see Mimikatz importing all kinds of other DLLs that it needs

```
"mimikatz" NOT "EventCode=4658" NOT "EventCode=4689" EventCode=7 | stats count by _time, Image, ImageLoaded
```

✓ 53 events (04/09/2017 03:00:41.000 to 04/09/2017 03:45:41.001) No Event Sampling

Events | Patterns | Statistics (53) | Visualization

20 Per Page | Format | Preview

_time	Image	ImageLoaded
2017-09-04 03:26:29	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe
2017-09-04 03:26:29	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	C:\Windows\System32\KernelBase.dll
2017-09-04 03:26:29	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	C:\Windows\System32\advapi32.dll
2017-09-04 03:26:29	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	C:\Windows\System32\bcryptprimitives.dll
2017-09-04 03:26:29	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	C:\Windows\System32\combase.dll
2017-09-04 03:26:29	C:\Users\Artanis\Documents\mimikatz_trunk\x64\mimikatz.exe	C:\Windows\System32\crypt32.dll

Example – Osiris Ransomware

- Part of the Locky family
- Acts like a traditional ransomware
- Osiris invades the system using spam technique or by exploiting detected system vulnerabilities.
- Malware is a .js file that drops the Osiris ransomware

Final Example – Osiris Ransomware

- Initial running of the malware from the desktop, which is `typical since this is designed to be double clicked by a user after a download.

```
Process Create:
UtcTime: 2016-12-11 15:58:06.435
ProcessGuid: {e29500a3-778e-584d-0000-0010fb549e00}
ProcessId: 2400
Image: C:\Windows\System32\wscript.exe
CommandLine: "C:\Windows\System32\WScript.exe" "C:\Users\IEUser
\Desktop\malware.js"
CurrentDirectory: C:\Users\IEUser\Desktop\
User: WIN-4M6JEQRPH70\IEUser
LogonGuid: {e29500a3-e6ab-5836-0000-00207a590100}
LogonId: 0x1597a
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes:
SHA1=860265276B29B42B8C4B077E5C651DEF9C81B6E9,MD5=D1AB72DB2BEDD2F255D3
5DA3DA0D4B16,SHA256=047F3C5A7AB0EA05F35B2CA8037BF62DD4228786D07707064D
BD0D46569305D0,IMPHASH=62EA1D2DA2B1481E969D080A6B29D775
ParentProcessGuid: {e29500a3-e6ab-5836-0000-0010857d0100}
ParentProcessId: 1352
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

Source: 909research.com

Final Example – Osiris Ransomware

- We can follow this through the logs by using the ProcessGuid of the process that starts the malware
- Some files are dropped in the Temp folder

```
TimeCreated  : 12/11/2016 10:58:06 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 11
Message      : File created:
               UtcTime: 2016-12-11 15:58:06.996
               ProcessGuid: {E29500A3-778E-584D-0000-0010FB549E00}
               ProcessId: 2400
               Image: C:\Windows\System32\WScript.exe
               TargetFilename: C:\Users\IEUser\AppData\Local
\Microsoft\Windows\Temporary Internet Files\Content.IE5\W8N
               S2AMB\o48qpgndy[1].txt
               CreationUtcTime: 2016-12-11 15:58:06.996

TimeCreated  : 12/11/2016 10:58:07 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 11
Message      : File created:
               UtcTime: 2016-12-11 15:58:07.605
               ProcessGuid: {E29500A3-778E-584D-0000-0010FB549E00}
               ProcessId: 2400
               Image: C:\Windows\System32\WScript.exe
               TargetFilename: C:\Users\IEUser\AppData\Local
\Temp\GPt3ly2wE
               CreationUtcTime: 2016-12-11 15:58:07.605
```

Source: 909research.com

Final Example – Osiris Ransomware

- Command and control domain is contacted (vxhcf-31.srv.cat)
- HTTP no via a browser
- We can still track via the processGuid

```
TimeCreated  : 12/11/2016 10:58:07 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 3
Message      : Network connection detected:
               UtcTime: 2016-11-25 06:00:48.931
               ProcessGuid: {E29500A3-778E-584D-0000-0010FB549E00}
               ProcessId: 2400
               Image: C:\Windows\System32\wscript.exe
               User: WIN-4M6JEQRPH70\IEUser
               Protocol: tcp
               Initiated: true
               SourceIsIpv6: false
               SourceIp: 192.168.87.141
               SourceHostname: WIN-4M6JEQRPH70.localdomain
               SourcePort: 49562
               SourcePortName:
               DestinationIsIpv6: false
               DestinationIp: 134.0.11.154
               DestinationHostname: vxhcf-31.srv.cat
               DestinationPort: 80
               DestinationPortName: http
```

Source: 909research.com

Final Example – Osiris Ransomware

- Command and control was contacted probably for the 2nd stage executable (GPt3ly2wE.zk) since .js files are typically just a dropper

```
TimeCreated  : 12/11/2016 10:58:08 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 11
Message      : File created:
               UtcTime: 2016-12-11 15:58:08.182
               ProcessGuid: {E29500A3-778E-584D-0000-0010FB549E00}
               ProcessId: 2400
               Image: C:\Windows\System32\WScript.exe
               TargetFilename: C:\Users\IEUser\AppData\Local
\Temp\GPt3ly2wE.zk
               CreationUtcTime: 2016-12-11 15:58:08.182
```

Source: 909research.com

Final Example – Osiris Ransomware

- The file GPt3ly2wE.zk is run using rundll32.exe
- The main encryption binary in DLL form.
- We now must follow the new ProcessGuid to make sure we get all the details of the new child process.

```
TimeCreated  : 12/11/2016 10:58:08 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 1
Message      : Process Create:
               UtcTime: 2016-12-11 15:58:08.213
               ProcessGuid: {E29500A3-7790-584D-0000-001000679E00}
               ProcessId: 3380
               Image: C:\Windows\System32\rundll32.exe
               CommandLine: "C:\Windows\System32\rundll32.exe"
C:\Users\IEUser\AppData\Local\Temp\GPT3LY~1.ZK,f7
               CurrentDirectory: C:\Users\IEUser\Desktop\
               User: WIN-4M6JEQRPH70\IEUser
               LogonGuid: {E29500A3-E6AB-5836-0000-00207A590100}
               LogonId: 0x1597a
               TerminalSessionId: 1
               IntegrityLevel: Medium
               Hashes:
SHA1=8939CF35447B22DD2C6E6F443446ACC1BF986D58,MD5=51138BEEA3E2C21EC
44D0932C71762A8,SHA256=5AD3C3

7E6F2B9DB3EE8B5AEEDC474645DE90C66E3D95F8620C48102F1EBA4124,IMPHASH=
EF8A44FE2F9AD4AB85E55004AAA024A9
               ParentProcessGuid: {E29500A3-778E-
584D-0000-0010FB549E00}
```

Source: 909research.com

Final Example – Osiris Ransomware

- A new command and control domain is contacted (213.ip-51-254-141.eu), for the encryption key transfer

```
TimeCreated  : 12/11/2016 10:58:13 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 3
Message      : Network connection detected:
               UtcTime: 2016-11-25 06:00:53.506
               ProcessGuid: {E29500A3-7790-584D-0000-001000679E00}
               ProcessId: 3380
               Image: C:\Windows\System32\rundll32.exe
               User: WIN-4M6JEQRPH70\IEUser
               Protocol: tcp
               Initiated: true
               SourceIsIpv6: false
               SourceIp: 192.168.87.141
               SourceHostname: WIN-4M6JEQRPH70.localdomain
               SourcePort: 49563
               SourcePortName:
               DestinationIsIpv6: false
               DestinationIp: 51.254.141.213
               DestinationHostname: 213.ip-51-254-141.eu
               DestinationPort: 80
               DestinationPortName: http
```

Source: 909research.com

Final Example – Osiris Ransomware

- The HTML message file saying "you've been encrypted" is written to various places on disk and the process ends

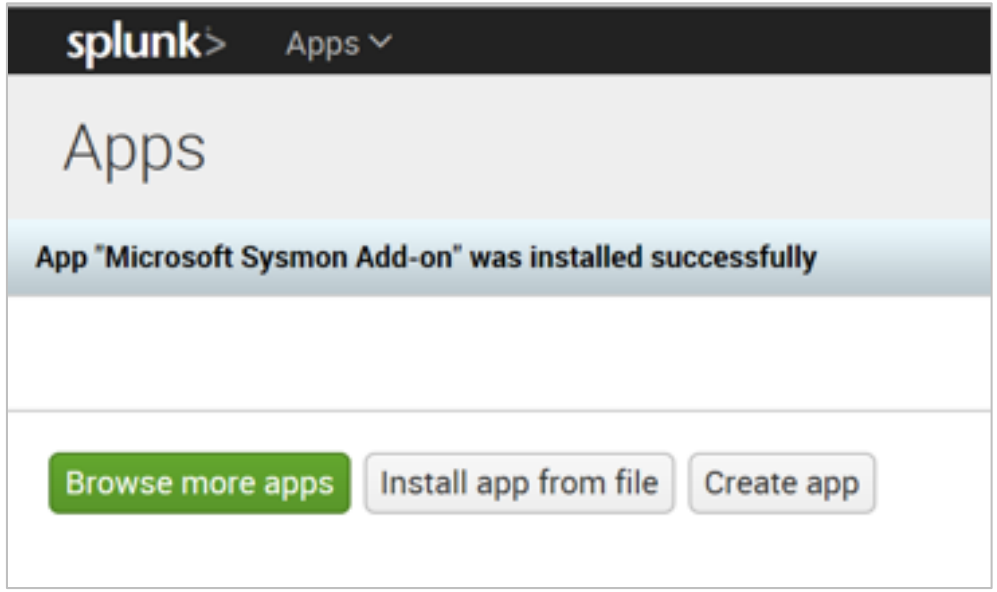
```
TimeCreated  : 12/11/2016 10:59:11 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 11
Message      : File created:
               UtcTime: 2016-12-11 15:59:11.050
               ProcessGuid: {E29500A3-7790-584D-0000-001000679E00}
               ProcessId: 3380
               Image: C:\Windows\System32\rundll32.exe
               TargetFilename: C:\Users\IEUser\Desktop\OSIRIS-
79f4.htm
               CreationUtcTime: 2016-12-11 15:59:11.050

TimeCreated  : 12/11/2016 10:59:11 AM
ProviderName : Microsoft-Windows-Sysmon
Id           : 11
Message      : File created:
               UtcTime: 2016-12-11 15:59:11.050
               ProcessGuid: {E29500A3-7790-584D-0000-001000679E00}
               ProcessId: 3380
               Image: C:\Windows\System32\rundll32.exe
               TargetFilename: C:\ProgramData\Adobe\Updater6
\4CR5T3SP--GUA7--EEHF--5050A725--CABDC0DA17C9.osiris
               CreationUtcTime: 2016-12-11 15:59:11.050
```

Source: 909research.com

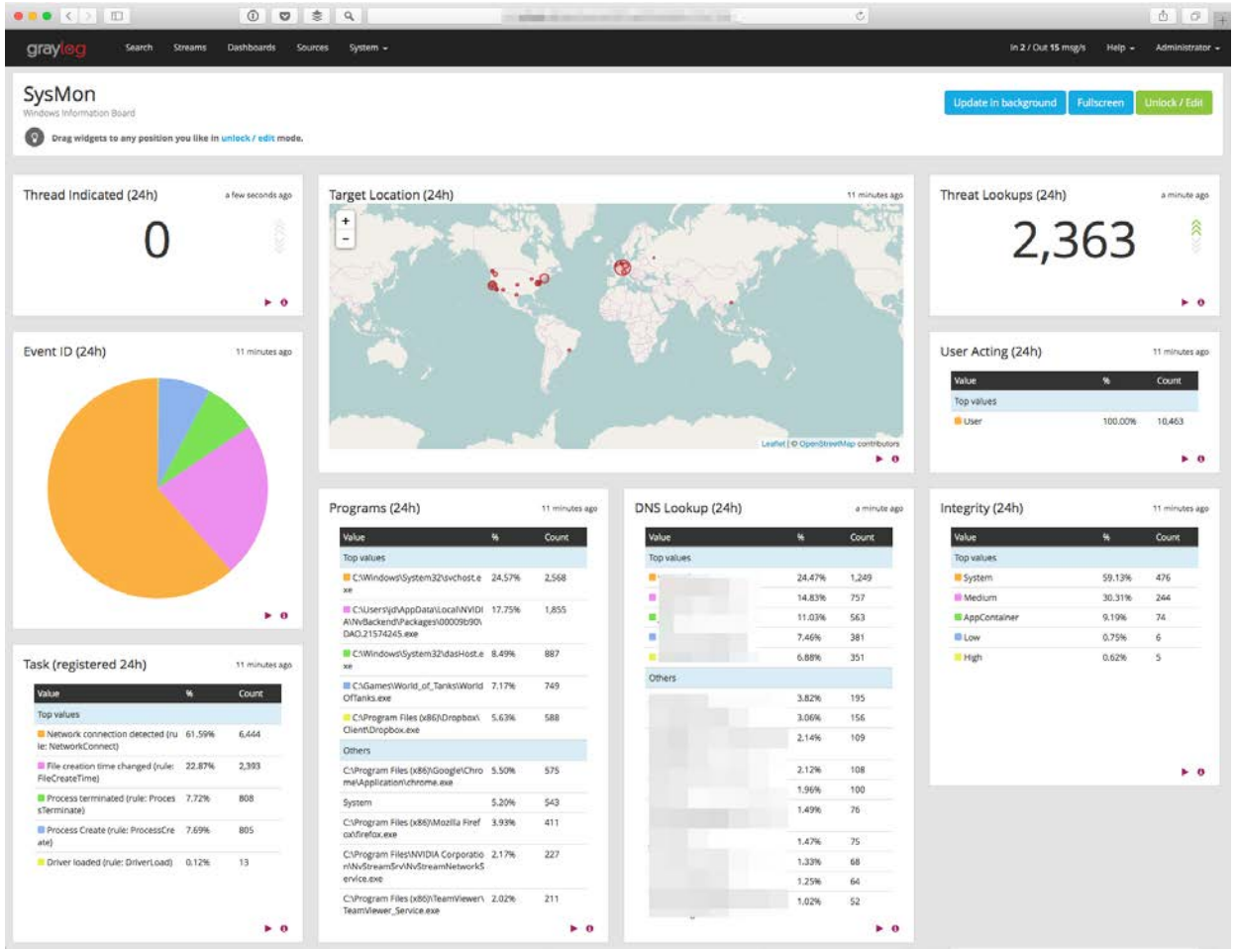
SIEM Support

- ArcSight FlexConnector
- Alienvault NSM Plugin (via NXLog)
- IBM QRadar Content Extension
- Logrythm
- Elk Stack
- Splunk universal forwarder



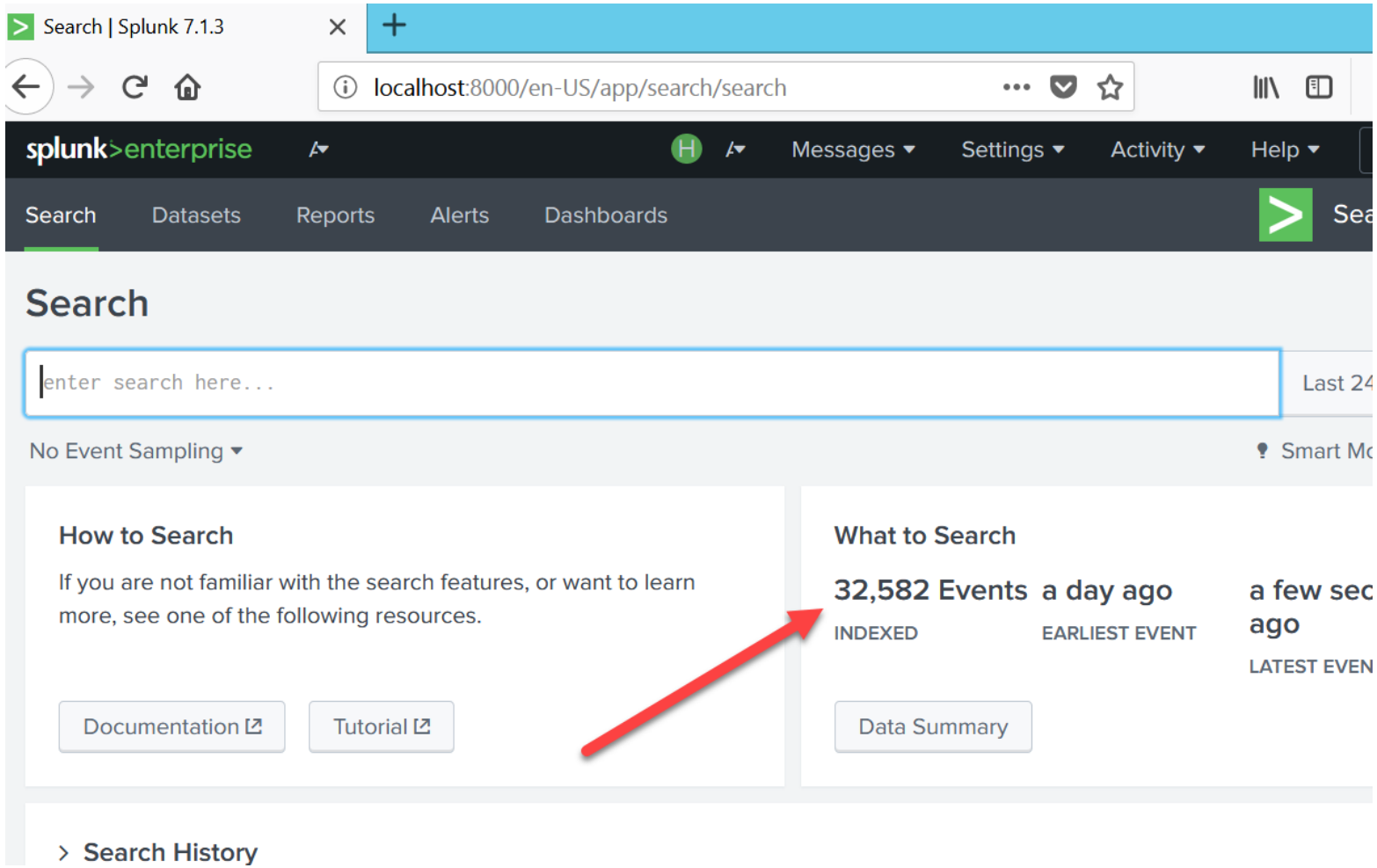
SIEM Support

- Integrating with Gray Log
- Data enrichment with threat intelligence prior to sending to SIEM



@petermorin123

Ingestion Overload – my local VM



Search | Splunk 7.1.3

localhost:8000/en-US/app/search/search?q=search sourcetype%3D"XmlWinEventLog%3AMicrosoft-Window

splunk>enterprise App: Search & Reporting Administrator Messages Settings Activity Help Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Close

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1 | dedup Hashes | table Hashes Image ParentImage
```

Last 24 hours

✓ 26 events (9/11/18 7:00:00.000 AM to 9/12/18 7:40:26.000 AM) No Event Sampling Job Smart Mode

Events Patterns Statistics (26) Visualization

20 Per Page Format Preview Prev 1 2 Next

Hashes	Image	ParentImage
SHA1=B014C7659B5A1DCBC92982D7061AFB011CA006F7	C:\Program Files\Splunk\bin\splunk-optimize.exe	C:\Program Files\Splunk\bin\splunkd.exe
SHA1=F2F236E9DC19B62BFF539CA9D1DDEA155B6276C4	C:\Program Files\Splunk\bin\splunk-powershell.exe	C:\Program Files\Splunk\bin\splunkd.exe
SHA1=57F1504F5DCEDDAD1C8BAA7B80A48CC3DDB849FA	C:\Program Files\Splunk\bin\splunk-admon.exe	C:\Program Files\Splunk\bin\splunkd.exe
SHA1=C30752C185CDE3CD9858411AEE14A82613BE9EC6	C:\Program Files\Splunk\bin\splunk-regmon.exe	C:\Program Files\Splunk\bin\splunkd.exe
SHA1=DB11513B7DE73034F4C9BB5D4B3EFD7199002D9D	C:\Program Files\Splunk\bin\splunk-winprintmon.exe	C:\Program Files\Splunk\bin\splunkd.exe
SHA1=155518DB285BDF2EF95F4AFD972FC1E23030312B	C:\Program Files\Splunk\bin\splunk-netmon.exe	C:\Program Files\Splunk\bin\splunkd.exe
SHA1=2EBACC2EF0A6AAC7F3C31B230A7124E60B8A731C	C:\Program Files\Splunk\bin\splunk-MonitorNoHandle.exe	C:\Program Files\Splunk\bin\splunkd.exe
SHA1=718FB64DAC1E54D6EEAD4D36296AD8F228C89CE2	C:\Program Files\Splunk\bin\splunkd.exe	C:\Program Files\Splunk\bin\splunkd.exe

sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1 | dedup Hashes | table Hashes Image ParentImage

SIEM

- So essentially, now you can search across your logs for common hashes
- So if you now have a hash of a known bad app, you can find out where it is being executed
- Detect the lateral movement path of the attacker

Conclusion

- Shocked that it isn't part of Windows already
- Experiment with different configurations
- You can also deploy custom configurations during IR situations
- **Remember either you have some kind of voodoo magic security or you aren't detecting it…**

Questions? Comments?

Peter Morin

petermorin123@gmail.com

Twitter: @petermorin123

http://www.petermorin.com