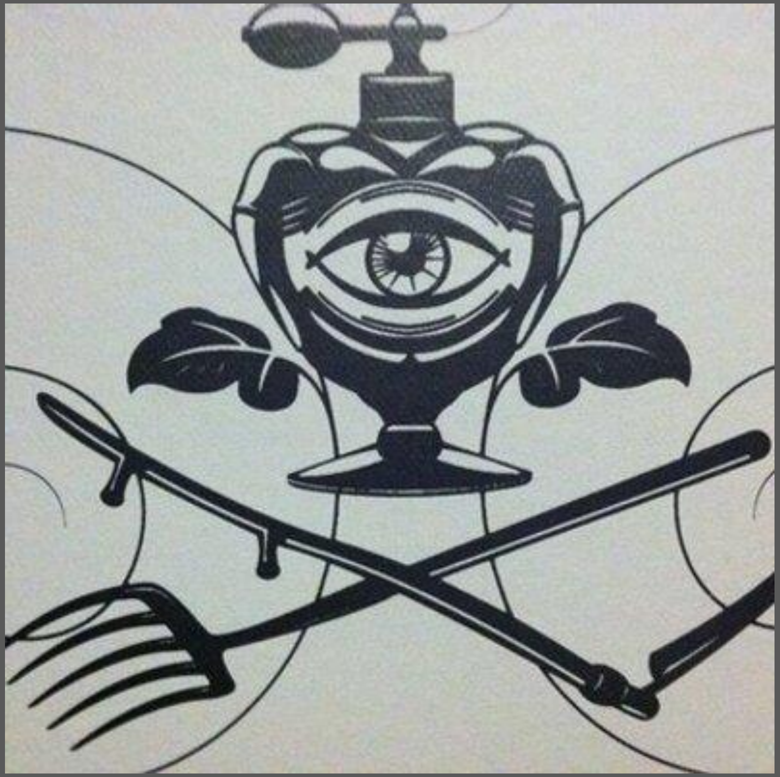
Project Obsidian

Obsidian Forensics:

The Importance of Sysmon for Investigations

ExtremePaperClip

whoami



ExtremePaperClip:

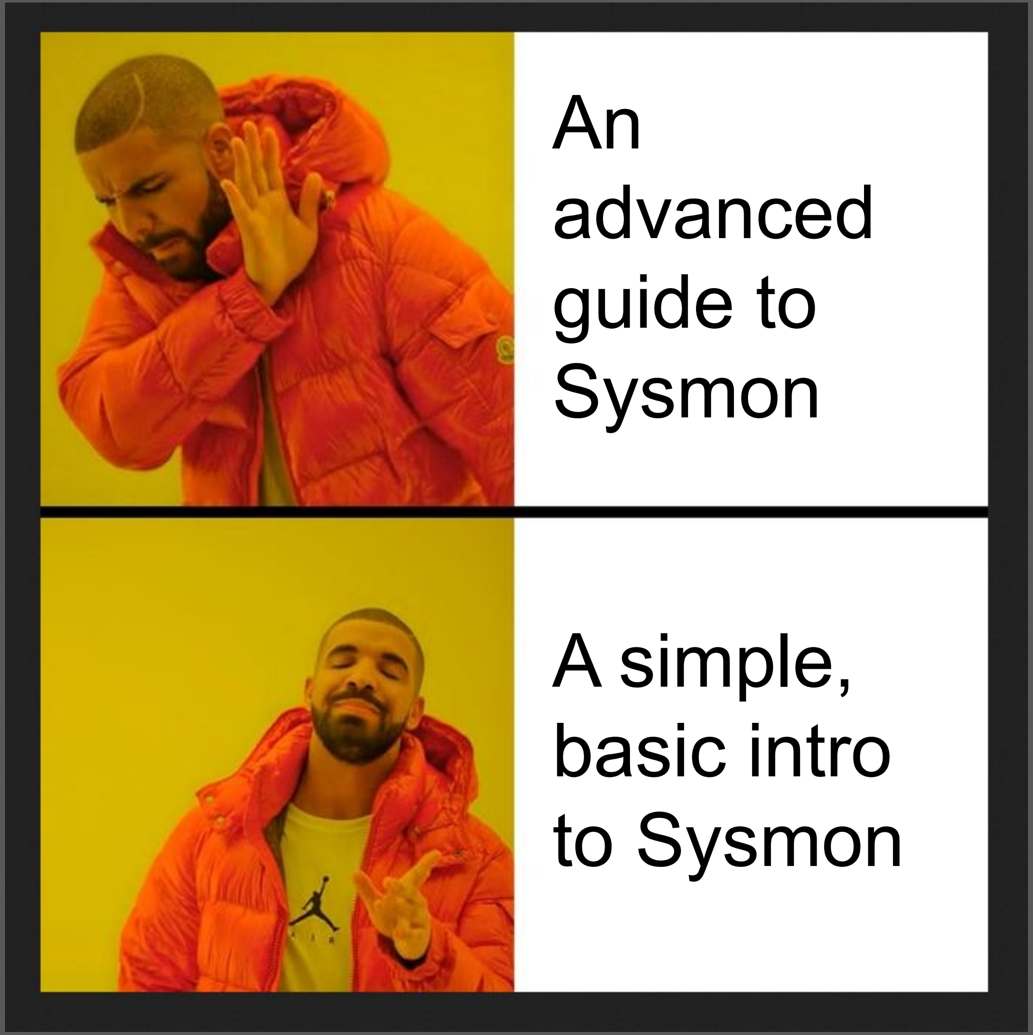
- Digital Forensics Nerd
- Linux Geek
- InfoSec Dork
- Lifelong Student of Everything
- Amateur History Buff
- Spice Fanatic
- Loads of Fun

@ExtremePaperC

What this talk is… and is not

This talk IS NOT

This talk IS



agenda

1 - What is Sysmon?

2 - Overview of the Sysmon Events

3 - What is the Sysmon Config?

4 - Installing Sysmon

5 - Examples of my favorite Sysmon Events

6 - Sysmon examples during an investigation

What is Sysmon?

TL;DR

Sysmon creates the logs that *should* exist in Windows Event Logs by default, but do not.

What is Sysmon?

SOME FACTS ABOUT SYSMON:

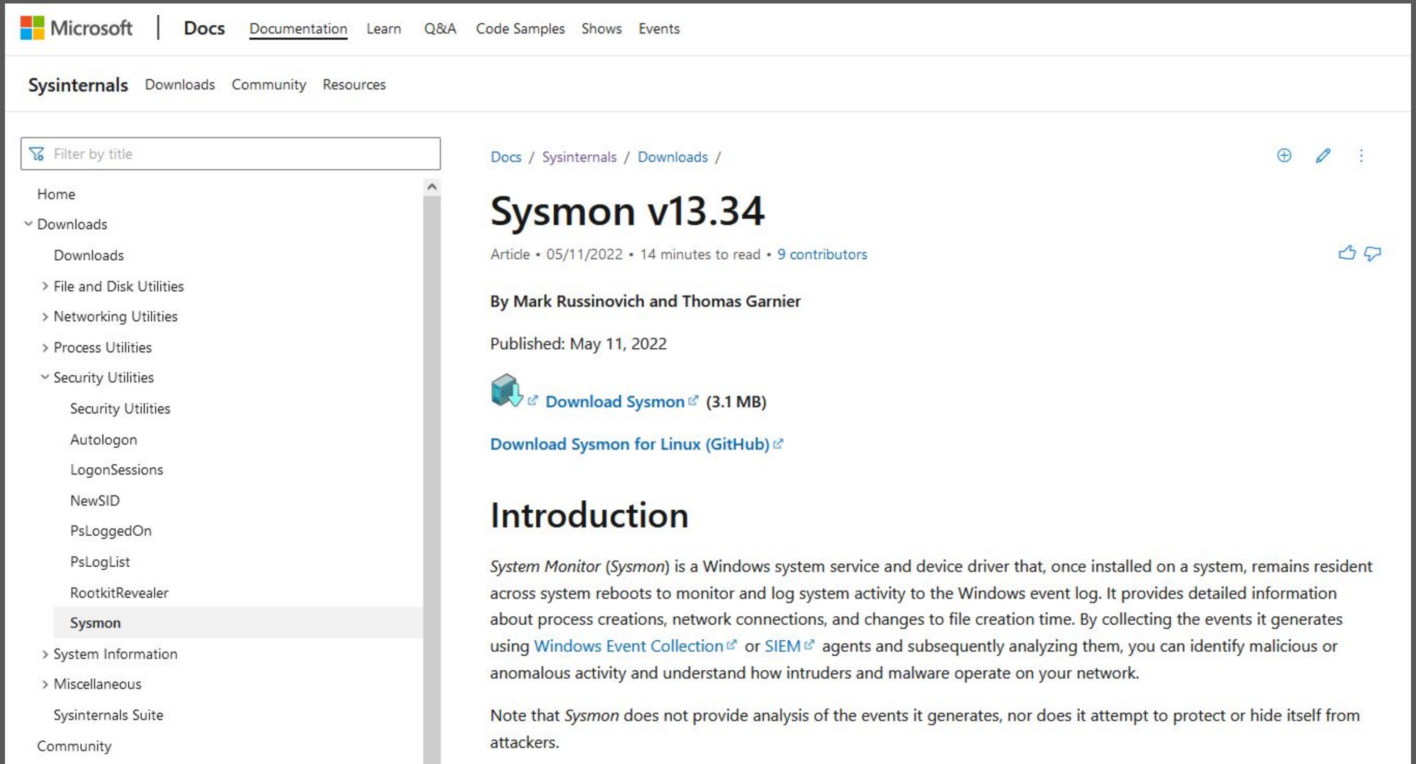
Sysmon (short for System Monitor)

Part of Windows Sysinternals

Released in 2014

Device Driver & Service

Creates logs specifically for Security



Sysmon v13.34

Article • 05/11/2022 • 14 minutes to read • 9 contributors

By Mark Russinovich and Thomas Garnier

Published: May 11, 2022

Download Sysmon (3.1 MB)

Download Sysmon for Linux (GitHub)

Introduction

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Brief History of Sysmon

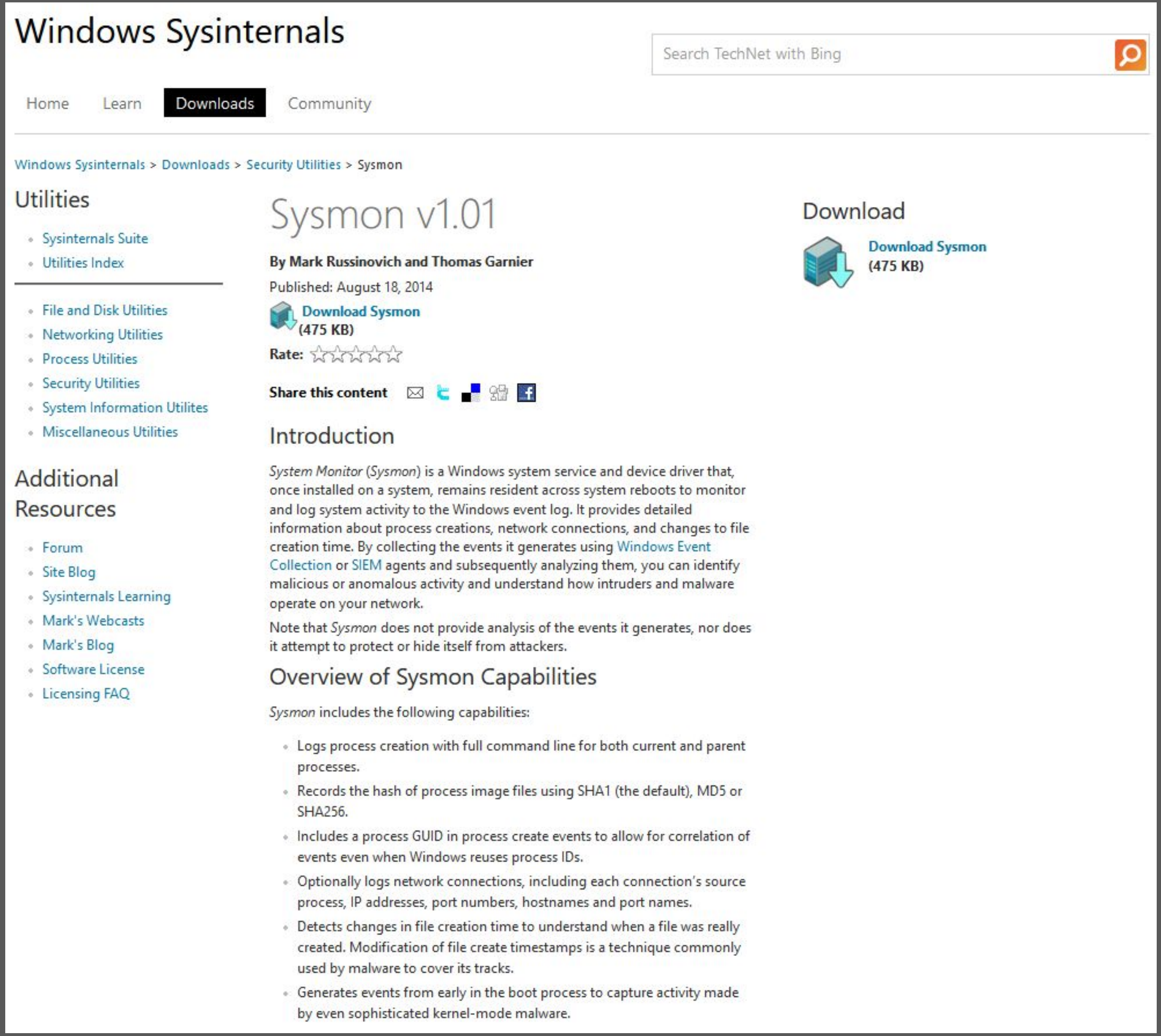
First released in 2014

Initially only had 3 Event ID's

Event ID 1:
Process creation

Event ID 2:
A process changed a file creation time

Event ID 3:
Network connection



Sysmon v1.01

By Mark Russinovich and Thomas Garnier

Published: August 18, 2014

Download Sysmon
(475 KB)

Rate: ☆☆☆☆☆

Share this content

Introduction

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

Overview of Sysmon Capabilities

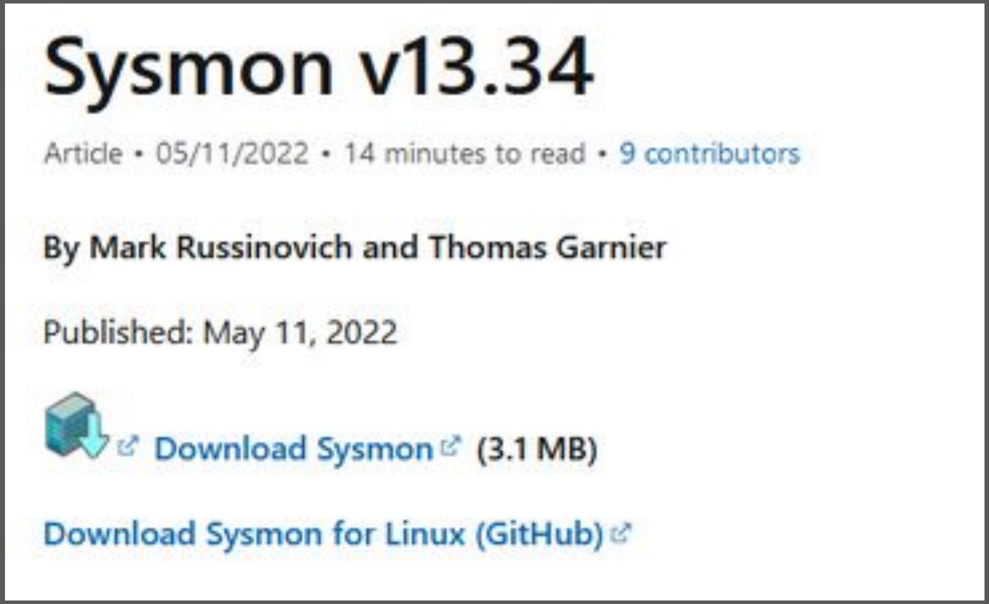
Sysmon includes the following capabilities:

- 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.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

Source: https://web.archive.org/web/20140902191844/http://technet.microsoft.com/en-us/sysinternals/dn798348

Overview of the Sysmon Events

The latest version of Sysmon has 26 Event IDs



Sysmon v13.34

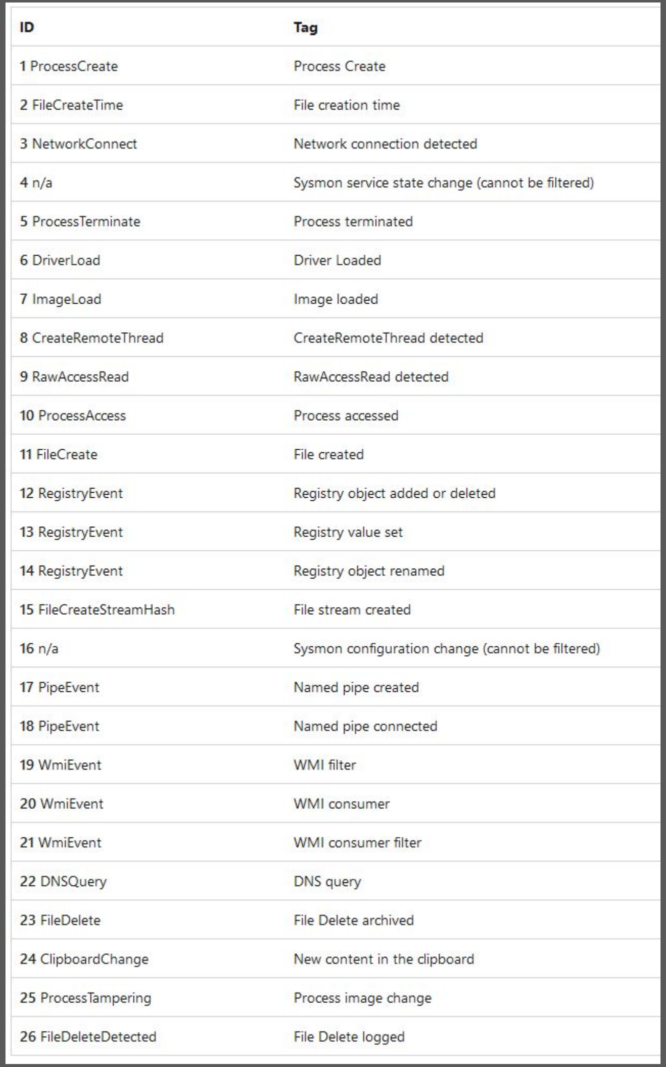
Article • 05/11/2022 • 14 minutes to read • 9 contributors

By Mark Russinovich and Thomas Garnier

Published: May 11, 2022

Download Sysmon (3.1 MB)

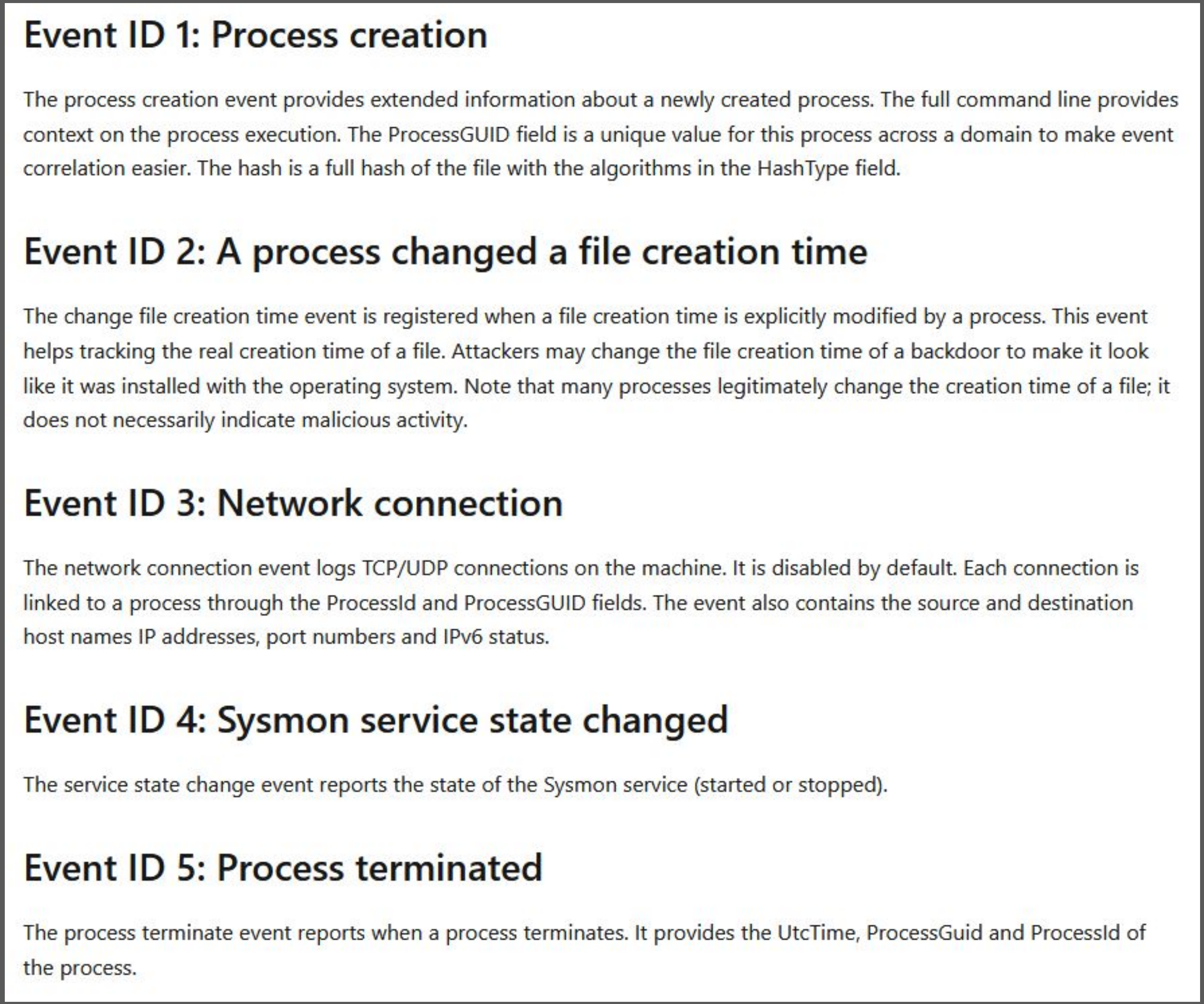
Download Sysmon for Linux (GitHub)



ID	Tag
1 ProcessCreate	Process Create
2 FileCreateTime	File creation time
3 NetworkConnect	Network connection detected
4 n/a	Sysmon service state change (cannot be filtered)
5 ProcessTerminate	Process terminated
6 DriverLoad	Driver Loaded
7 ImageLoad	Image loaded
8 CreateRemoteThread	CreateRemoteThread detected
9 RawAccessRead	RawAccessRead detected
10 ProcessAccess	Process accessed
11 FileCreate	File created
12 RegistryEvent	Registry object added or deleted
13 RegistryEvent	Registry value set
14 RegistryEvent	Registry object renamed
15 FileCreateStreamHash	File stream created
16 n/a	Sysmon configuration change (cannot be filtered)
17 PipeEvent	Named pipe created
18 PipeEvent	Named pipe connected
19 WmiEvent	WMI filter
20 WmiEvent	WMI consumer
21 WmiEvent	WMI consumer filter
22 DNSQuery	DNS query
23 FileDelete	File Delete archived
24 ClipboardChange	New content in the clipboard
25 ProcessTampering	Process image change
26 FileDeleteDetected	File Delete logged

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Overview of the Sysmon Events



Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.

Event ID 2: A process changed a file creation time

The change file creation time event is registered when a file creation time is explicitly modified by a process. This event helps tracking the real creation time of a file. Attackers may change the file creation time of a backdoor to make it look like it was installed with the operating system. Note that many processes legitimately change the creation time of a file; it does not necessarily indicate malicious activity.

Event ID 3: Network connection

The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.

Event ID 4: Sysmon service state changed

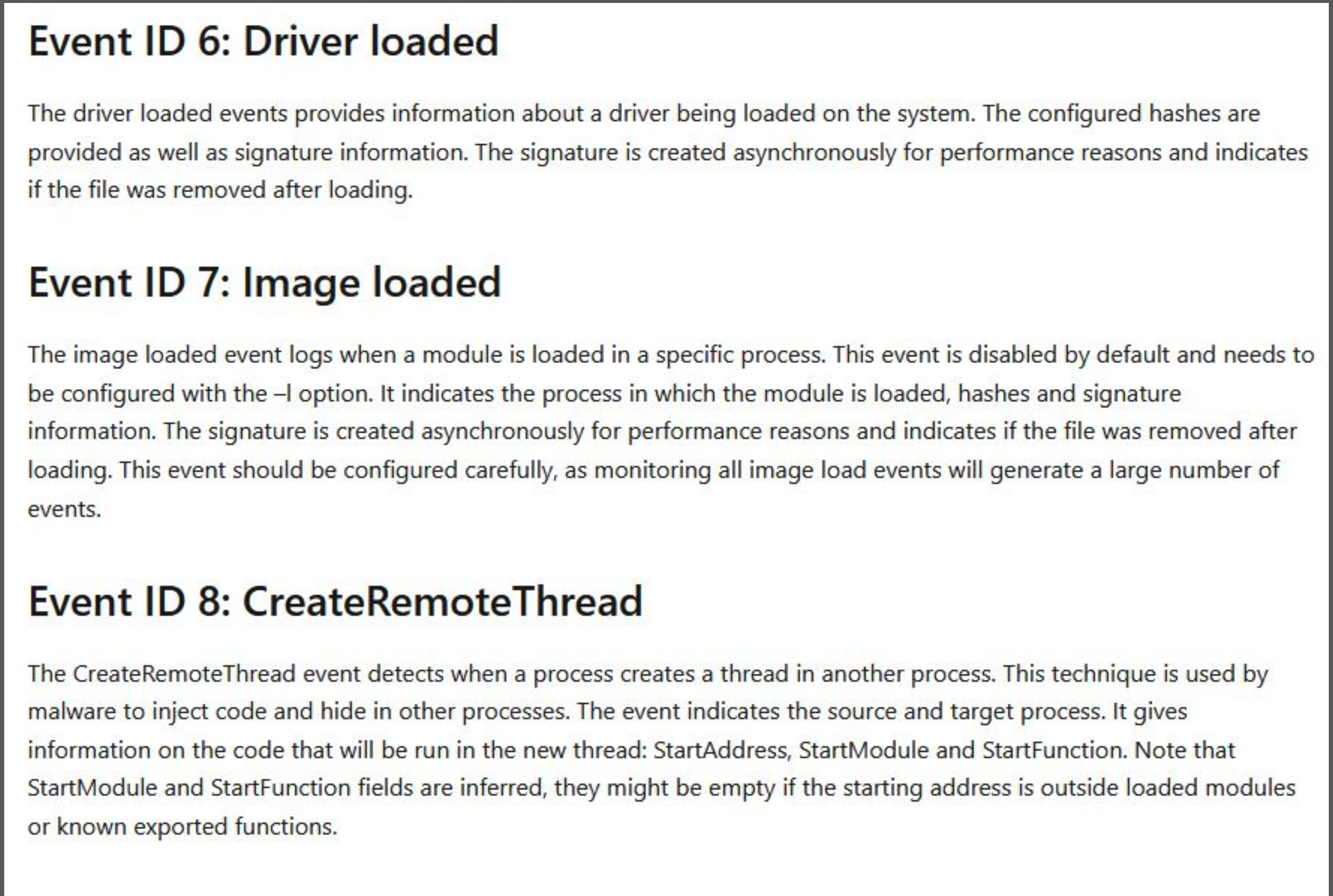
The service state change event reports the state of the Sysmon service (started or stopped).

Event ID 5: Process terminated

The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Overview of the Sysmon Events



Event ID 6: Driver loaded

The driver loaded events provides information about a driver being loaded on the system. The configured hashes are provided as well as signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading.

Event ID 7: Image loaded

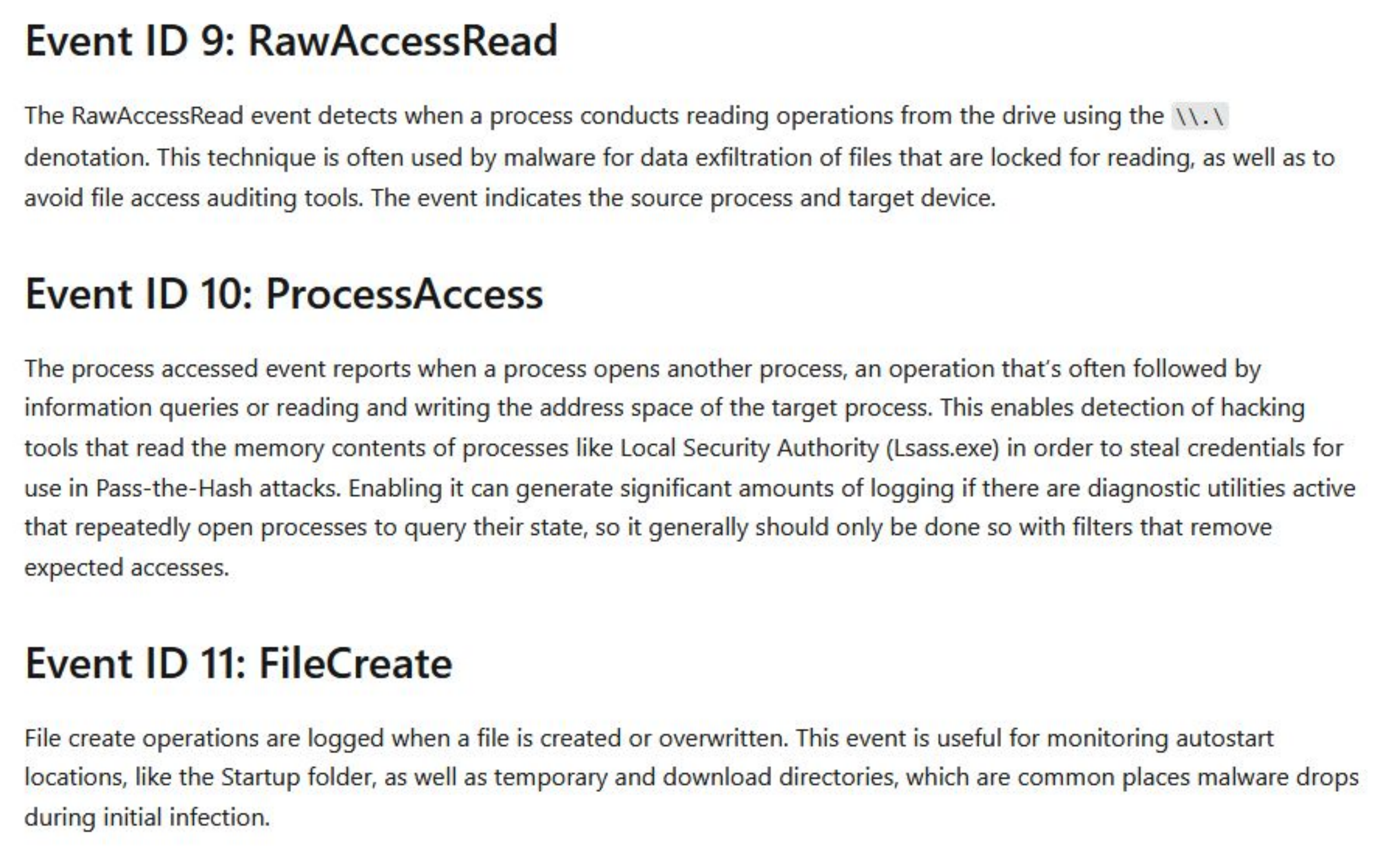
The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the –l option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading. This event should be configured carefully, as monitoring all image load events will generate a large number of events.

Event ID 8: CreateRemoteThread

The CreateRemoteThread event detects when a process creates a thread in another process. This technique is used by malware to inject code and hide in other processes. The event indicates the source and target process. It gives information on the code that will be run in the new thread: StartAddress, StartModule and StartFunction. Note that StartModule and StartFunction fields are inferred, they might be empty if the starting address is outside loaded modules or known exported functions.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Overview of the Sysmon Events



Event ID 9: RawAccessRead

The RawAccessRead event detects when a process conducts reading operations from the drive using the `\\.\` denotation. This technique is often used by malware for data exfiltration of files that are locked for reading, as well as to avoid file access auditing tools. The event indicates the source process and target device.

Event ID 10: ProcessAccess

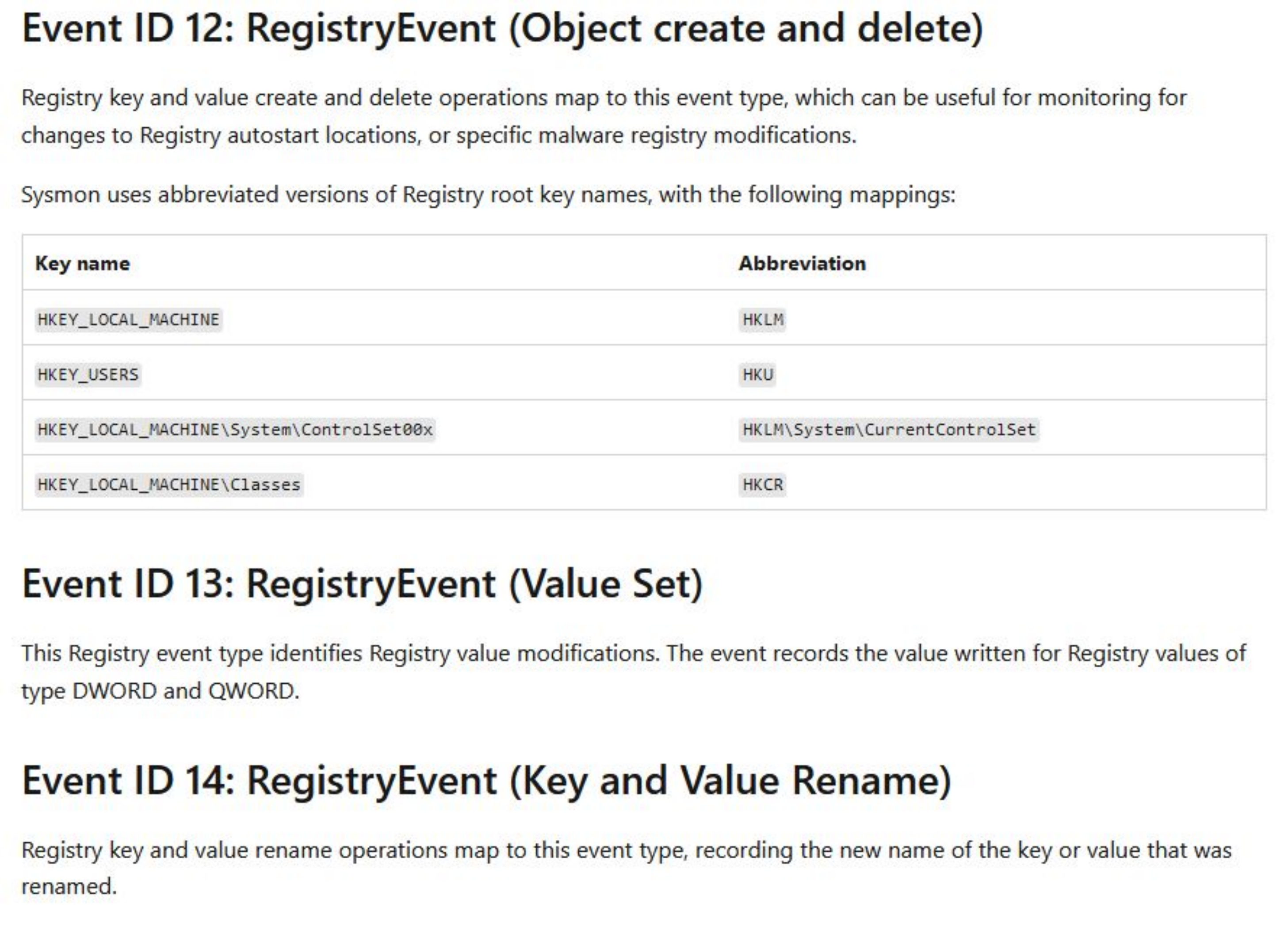
The process accessed event reports when a process opens another process, an operation that's often followed by information queries or reading and writing the address space of the target process. This enables detection of hacking tools that read the memory contents of processes like Local Security Authority (Lsass.exe) in order to steal credentials for use in Pass-the-Hash attacks. Enabling it can generate significant amounts of logging if there are diagnostic utilities active that repeatedly open processes to query their state, so it generally should only be done so with filters that remove expected accesses.

Event ID 11: FileCreate

File create operations are logged when a file is created or overwritten. This event is useful for monitoring autostart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Overview of the Sysmon Events



Event ID 12: RegistryEvent (Object create and delete)

Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.

Sysmon uses abbreviated versions of Registry root key names, with the following mappings:

Key name	Abbreviation
`HKEY_LOCAL_MACHINE`	`HKLM`
`HKEY_USERS`	`HKU`
`HKEY_LOCAL_MACHINE\System\ControlSet00x`	`HKLM\System\CurrentControlSet`
`HKEY_LOCAL_MACHINE\Classes`	`HKCR`

Event ID 13: RegistryEvent (Value Set)

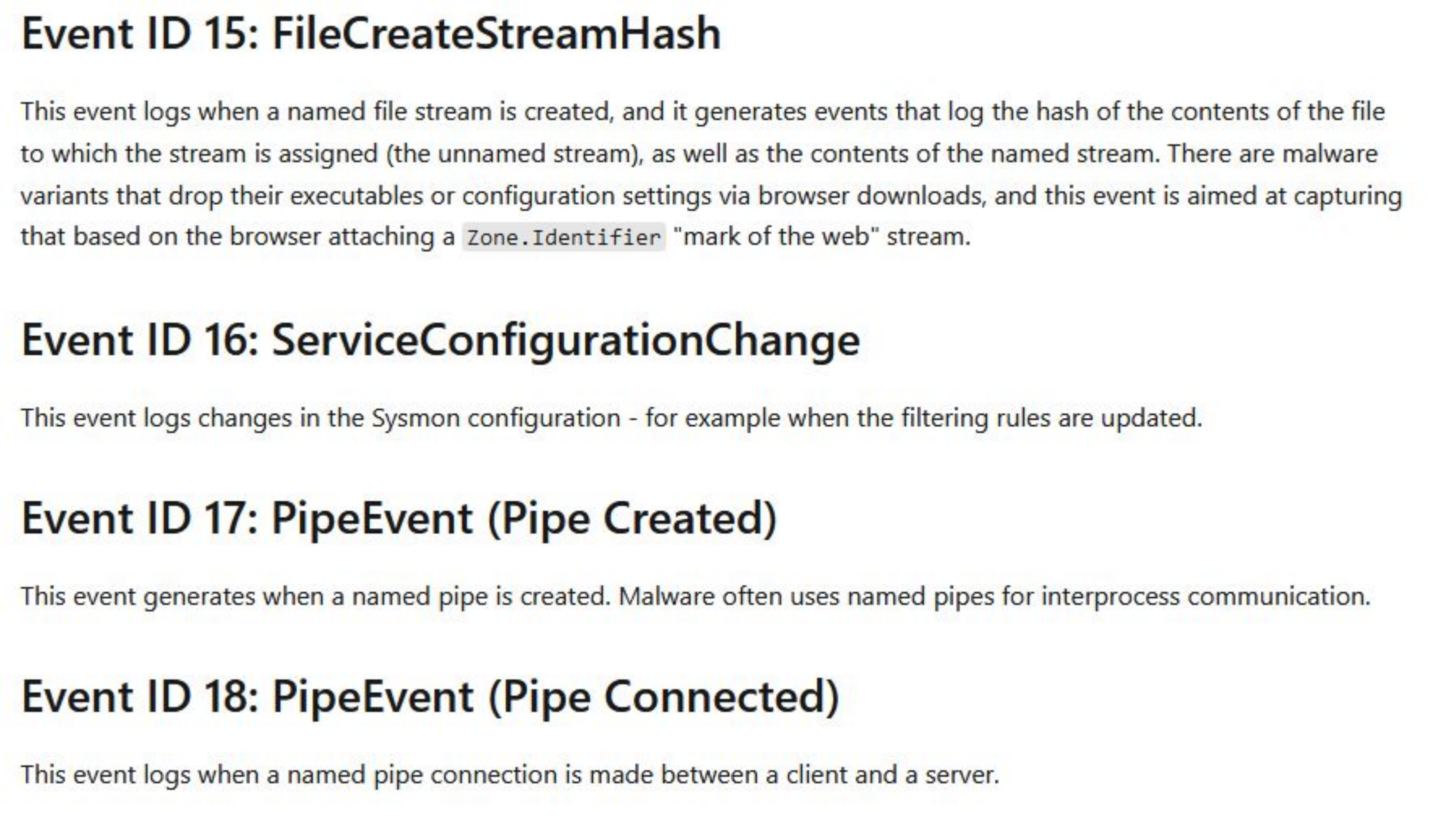
This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type DWORD and QWORD.

Event ID 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.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Overview of the Sysmon Events



Event ID 15: FileCreateStreamHash

This event logs 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. There are malware variants that drop their executables or configuration settings via browser downloads, and this event is aimed at capturing that based on the browser attaching a `Zone.Identifier` "mark of the web" stream.

Event ID 16: ServiceConfigurationChange

This event logs changes in the Sysmon configuration - for example when the filtering rules are updated.

Event ID 17: PipeEvent (Pipe Created)

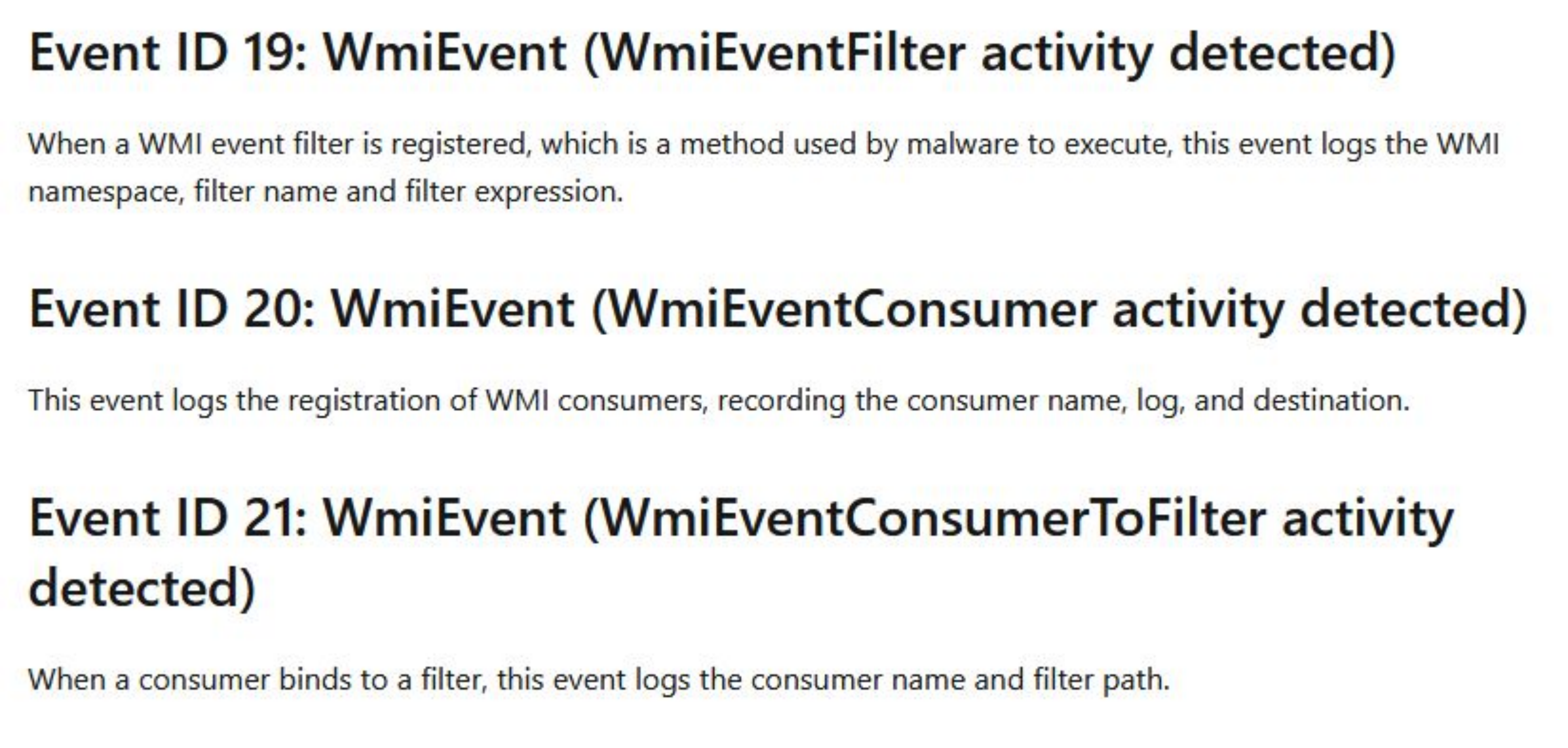
This event generates when a named pipe is created. Malware often uses named pipes for interprocess communication.

Event ID 18: PipeEvent (Pipe Connected)

This event logs when a named pipe connection is made between a client and a server.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Overview of the Sysmon Events



Event ID 19: WmiEvent (WmiEventFilter activity detected)

When a WMI event filter is registered, which is a method used by malware to execute, this event logs the WMI namespace, filter name and filter expression.

Event ID 20: WmiEvent (WmiEventConsumer activity detected)

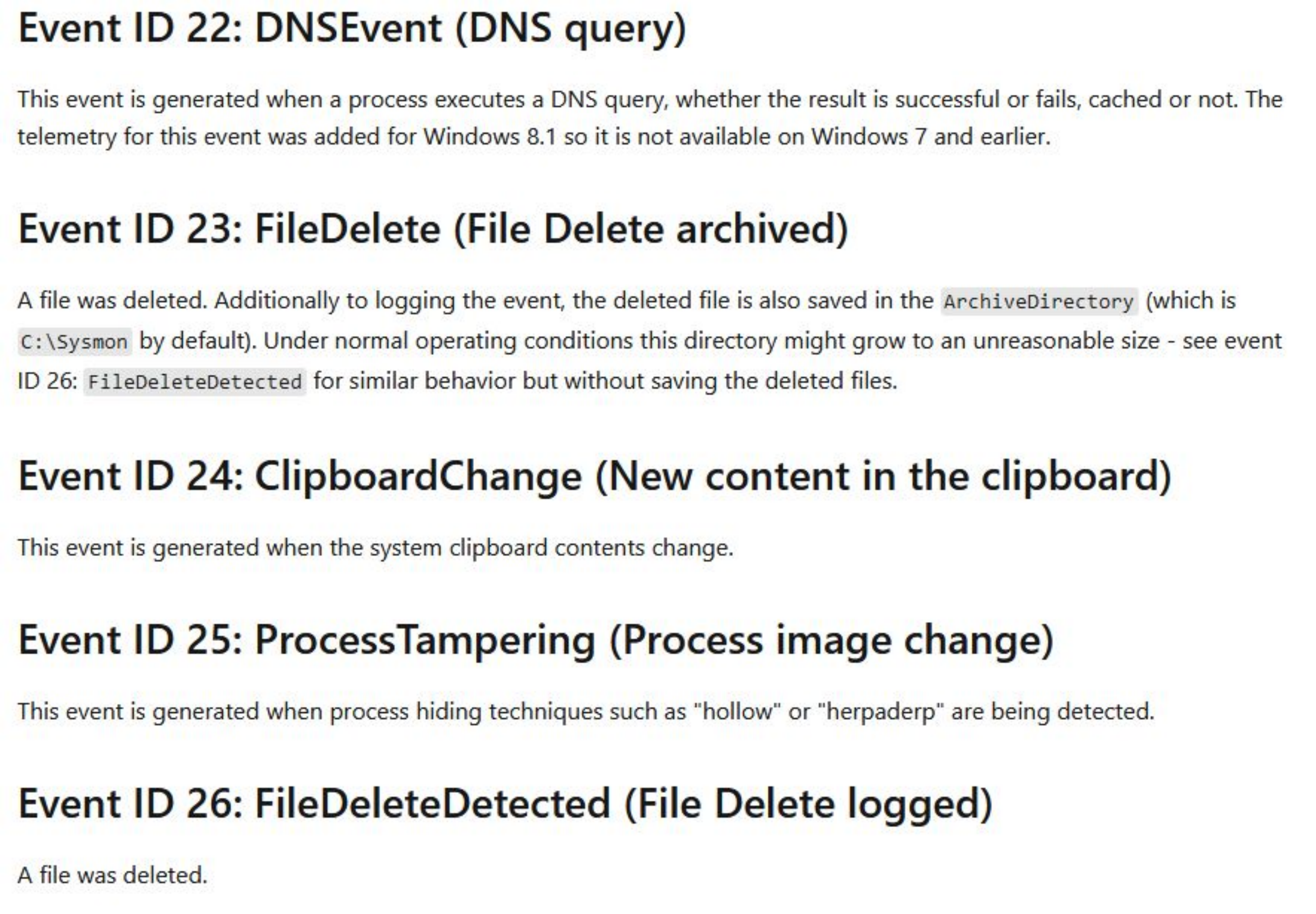
This event logs the registration of WMI consumers, recording the consumer name, log, and destination.

Event ID 21: WmiEvent (WmiEventConsumerToFilter activity detected)

When a consumer binds to a filter, this event logs the consumer name and filter path.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Overview of the Sysmon Events



Event ID 22: DNSEvent (DNS query)

This event is generated when a process executes a DNS query, whether the result is successful or fails, cached or not. The telemetry for this event was added for Windows 8.1 so it is not available on Windows 7 and earlier.

Event ID 23: FileDelete (File Delete archived)

A file was deleted. Additionally to logging the event, the deleted file is also saved in the `ArchiveDirectory` (which is `C:\Sysmon` by default). Under normal operating conditions this directory might grow to an unreasonable size - see event ID 26: `FileDeleteDetected` for similar behavior but without saving the deleted files.

Event ID 24: ClipboardChange (New content in the clipboard)

This event is generated when the system clipboard contents change.

Event ID 25: ProcessTampering (Process image change)

This event is generated when process hiding techniques such as "hollow" or "herpaderp" are being detected.

Event ID 26: FileDeleteDetected (File Delete logged)

A file was deleted.

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

What is the Sysmon Config?

TL;DR

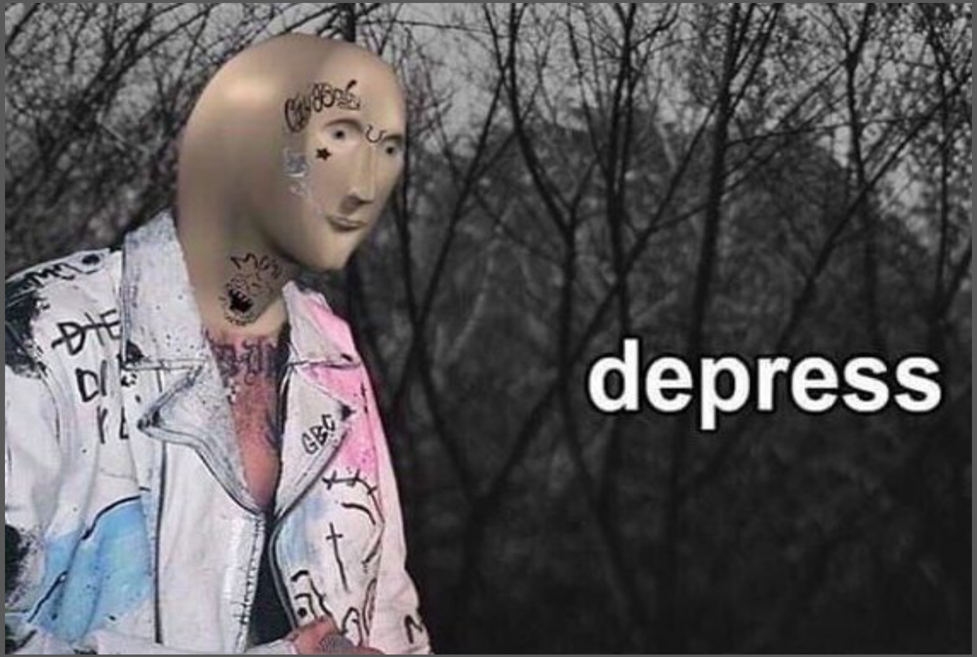
The **Sysmon Config** file, is an XML file that defines what gets ***included*** or ***excluded*** in the Sysmon logs. It’s a big deal.

What is the Sysmon Config?

WHY IS THE
SYSMON CONFIG
SO IMPORTANT?

(Did he just use the IMPACT font? …Yes, I did. Deal with it.)

Why is the Sysmon Config so important?

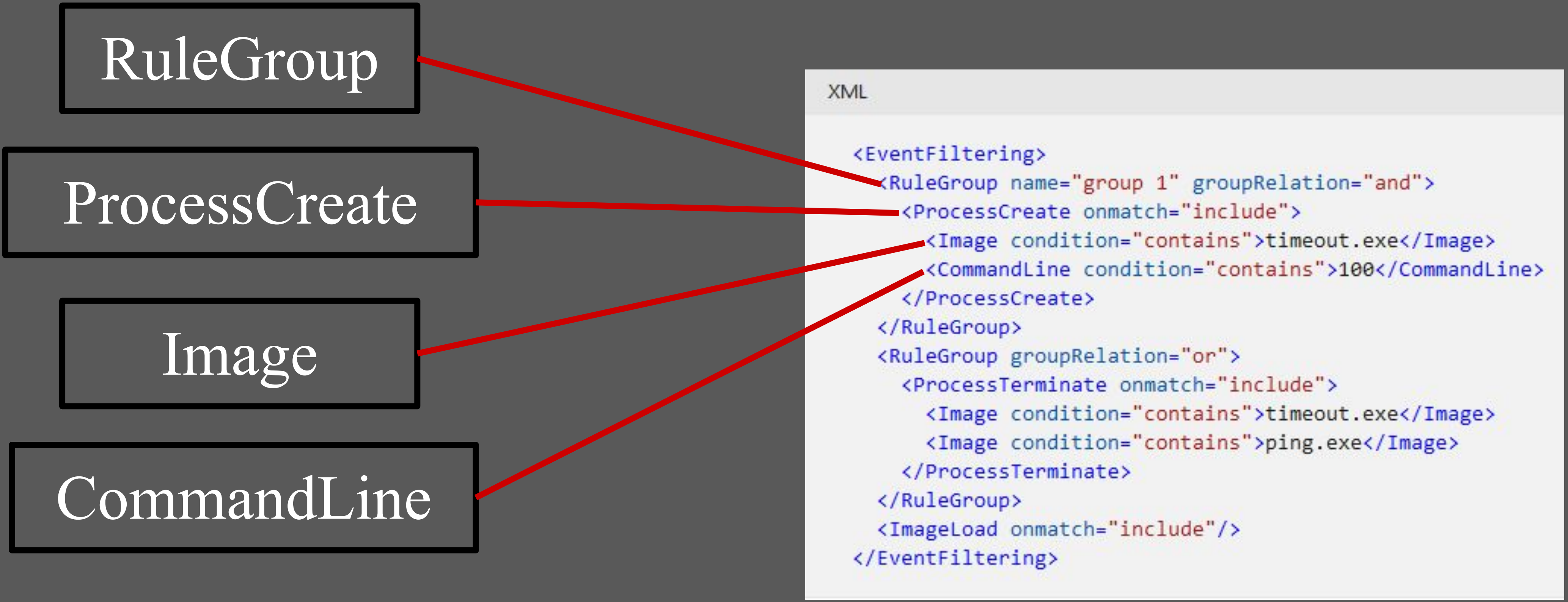


<u>Include</u> too much = *Garbage Data Lake*

Why is the Sysmon Config so important?

Exclude too much = *You won’t see the baddies*

Sysmon Config Example

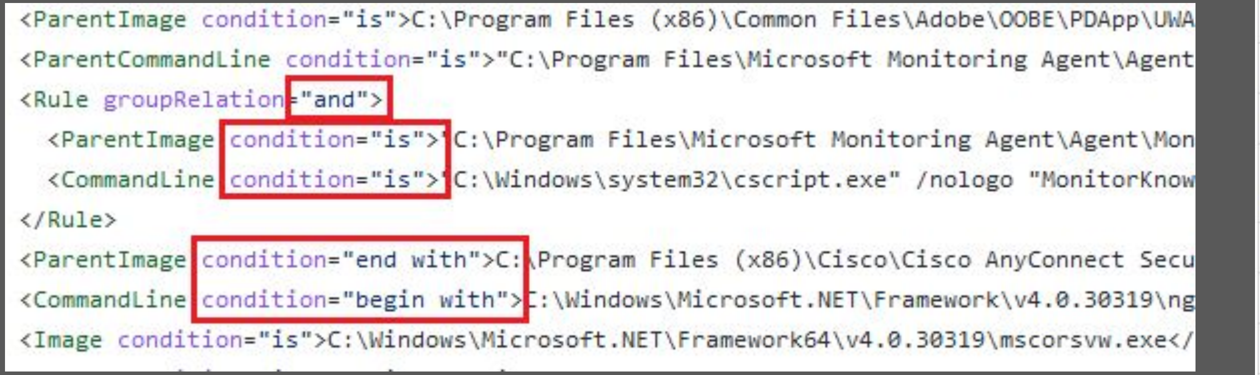


```xml
<EventFiltering>
  <RuleGroup name="group 1" groupRelation="and">
    <ProcessCreate onmatch="include">
      <Image condition="contains">timeout.exe</Image>
      <CommandLine condition="contains">100</CommandLine>
    </ProcessCreate>
  </RuleGroup>
  <RuleGroup groupRelation="or">
    <ProcessTerminate onmatch="include">
      <Image condition="contains">timeout.exe</Image>
      <Image condition="contains">ping.exe</Image>
    </ProcessTerminate>
  </RuleGroup>
  <ImageLoad onmatch="include"/>
</EventFiltering>
```

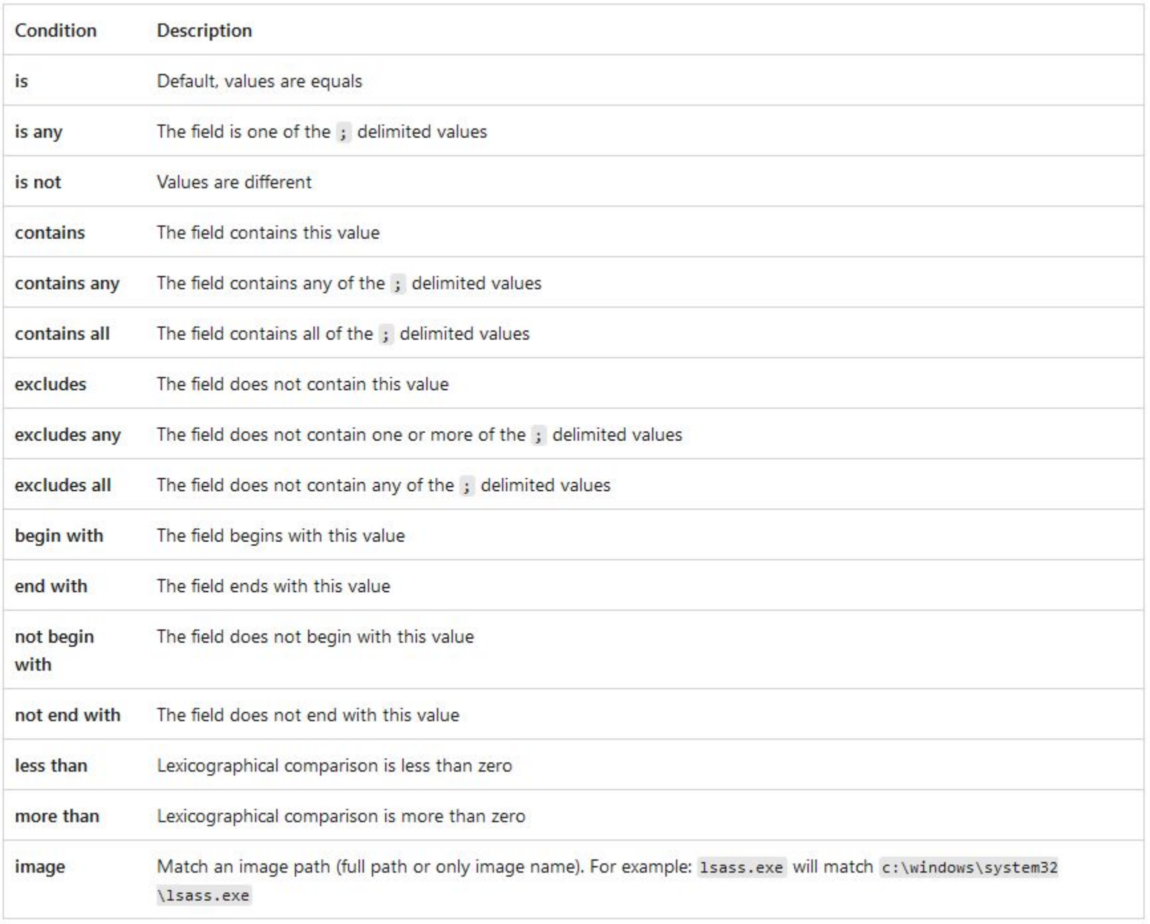
Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

The Sysmon Config

Sysmon Config Conditions



```
<ParentImage condition="is">C:\Program Files (x86)\Common Files\Adobe\OOBE\PDApp\UWA
<ParentCommandLine condition="is">"C:\Program Files\Microsoft Monitoring Agent\Agent
<Rule groupRelation="and">
  <ParentImage condition="is">"C:\Program Files\Microsoft Monitoring Agent\Agent\Mon
  <CommandLine condition="is">"C:\Windows\system32\cscript.exe" /nologo "MonitorKnow
</Rule>
<ParentImage condition="end with">C:\Program Files (x86)\Cisco\Cisco AnyConnect Secu
<CommandLine condition="begin with">C:\Windows\Microsoft.NET\Framework\v4.0.30319\ng
<Image condition="is">C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe</
```



Condition	Description
is	Default, values are equals
is any	The field is one of the `;` delimited values
is not	Values are different
contains	The field contains this value
contains any	The field contains any of the `;` delimited values
contains all	The field contains all of the `;` delimited values
excludes	The field does not contain this value
excludes any	The field does not contain one or more of the `;` delimited values
excludes all	The field does not contain any of the `;` delimited values
begin with	The field begins with this value
end with	The field ends with this value
not begin with	The field does not begin with this value
not end with	The field does not end with this value
less than	Lexicographical comparison is less than zero
more than	Lexicographical comparison is more than zero
image	Match an image path (full path or only image name). For example: `lsass.exe` will match `c:\windows\system32\lsass.exe`

Source: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Pre-Made Sysmon Config?

YOUR BRAIN RIGHT NOW:

*"...so where do I get a good **pre-made** Sysmon Config that I can start with?"*

Great Question

Pre-Made Sysmon Config

"Sup, people?
…I heard you like bad-ass pre-made Sysmon Configs
…Right?"

Note: Olaf Hartong never said this

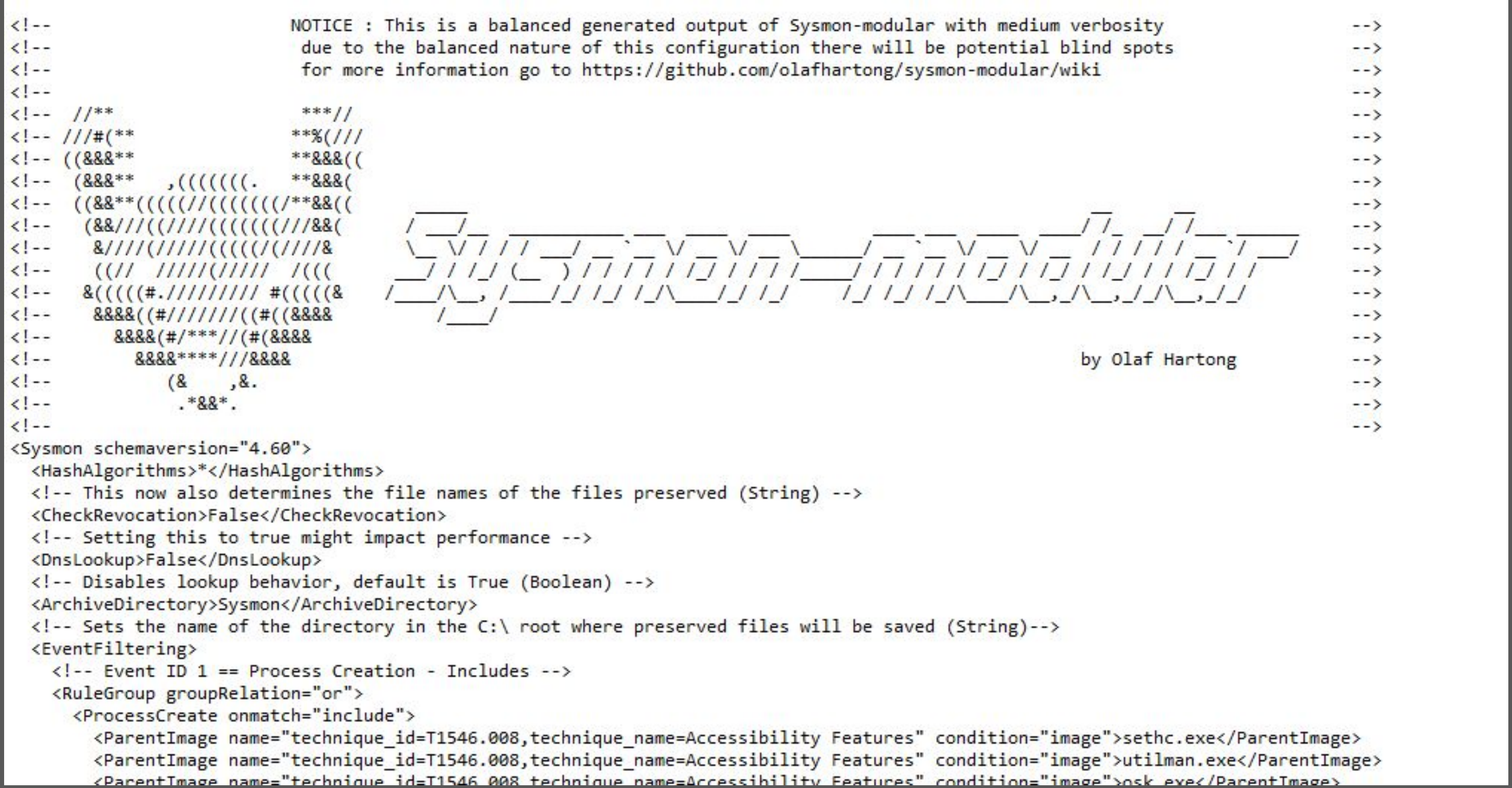
Introducing: "Olaf Hartong"

Source: https://github.com/olafhartong/sysmon-modular

Olaf’s Sysmon Config

In Short:

Olaf’s Sysmon Config Rules



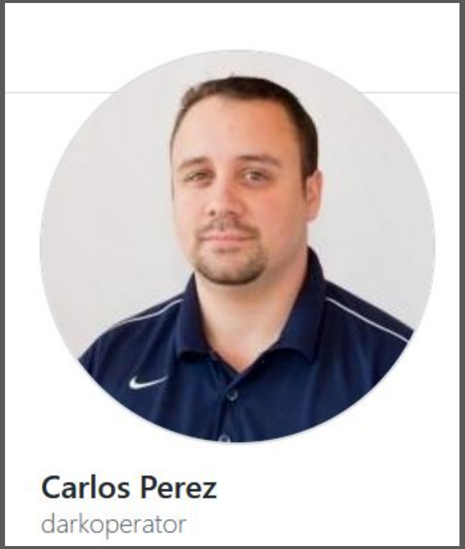
```
<!--                       NOTICE : This is a balanced generated output of Sysmon-modular with medium verbosity                    -->
<!--                        due to the balanced nature of this configuration there will be potential blind spots                   -->
<!--                        for more information go to https://github.com/olafhartong/sysmon-modular/wiki                          -->
<!--                                                                                                                               -->
<!--  //**                  ***//                                                                                                  -->
<!-- ///#(**               **%(///                                                                                                 -->
<!-- ((&&&**               **&&&((                                                                                                 -->
<!--  (&&&**   ,(((((((.   **&&&(                                                                                                  -->
<!--  ((&&**(((((//(((((((/**&&((      _____                                                   __      __                          -->
<!--   (&&///((////(((((((///&&(      / ___/__  ___________ ___  ____  ____        ____ ___  ____  ____/ /_  __/ /___ ______       -->
<!--    &////(/////(((((/(////&       \__ \/ / / / ___/ __ `__ \/ __ \/ __ \______/ __ `__ \/ __ \/ __  / / / / / __ `/ ___/       -->
<!--     ((//  /////(/////  /(((     ___/ / /_/ (__  ) / / / / / /_/ / / / /_____/ / / / / / /_/ / /_/ / /_/ / / /_/ / /           -->
<!--   &(((((#.///////// #(((((&   /____/\__, /____/_/ /_/ /_/\____/_/ /_/     /_/ /_/ /_/\____/\__,_/\__,_/_/\__,_/_/             -->
<!--    &&&&((#///////((#((&&&&          /____/                                                                                    -->
<!--      &&&&(#/***//(#(&&&&                                                                                                      -->
<!--        &&&&****///&&&&                                                                           by Olaf Hartong             -->
<!--           (&    ,&.                                                                                                           -->
<!--            .*&&*.                                                                                                             -->
<!--                                                                                                                               -->
<Sysmon schemaversion="4.60">
  <HashAlgorithms>*</HashAlgorithms>
  <!-- This now also determines the file names of the files preserved (String) -->
  <CheckRevocation>False</CheckRevocation>
  <!-- Setting this to true might impact performance -->
  <DnsLookup>False</DnsLookup>
  <!-- Disables lookup behavior, default is True (Boolean) -->
  <ArchiveDirectory>Sysmon</ArchiveDirectory>
  <!-- Sets the name of the directory in the C:\ root where preserved files will be saved (String)-->
  <EventFiltering>
    <!-- Event ID 1 == Process Creation - Includes -->
    <RuleGroup groupRelation="or">
      <ProcessCreate onmatch="include">
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">sethc.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">utilman.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">osk.exe</ParentImage>
```

Source: https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml

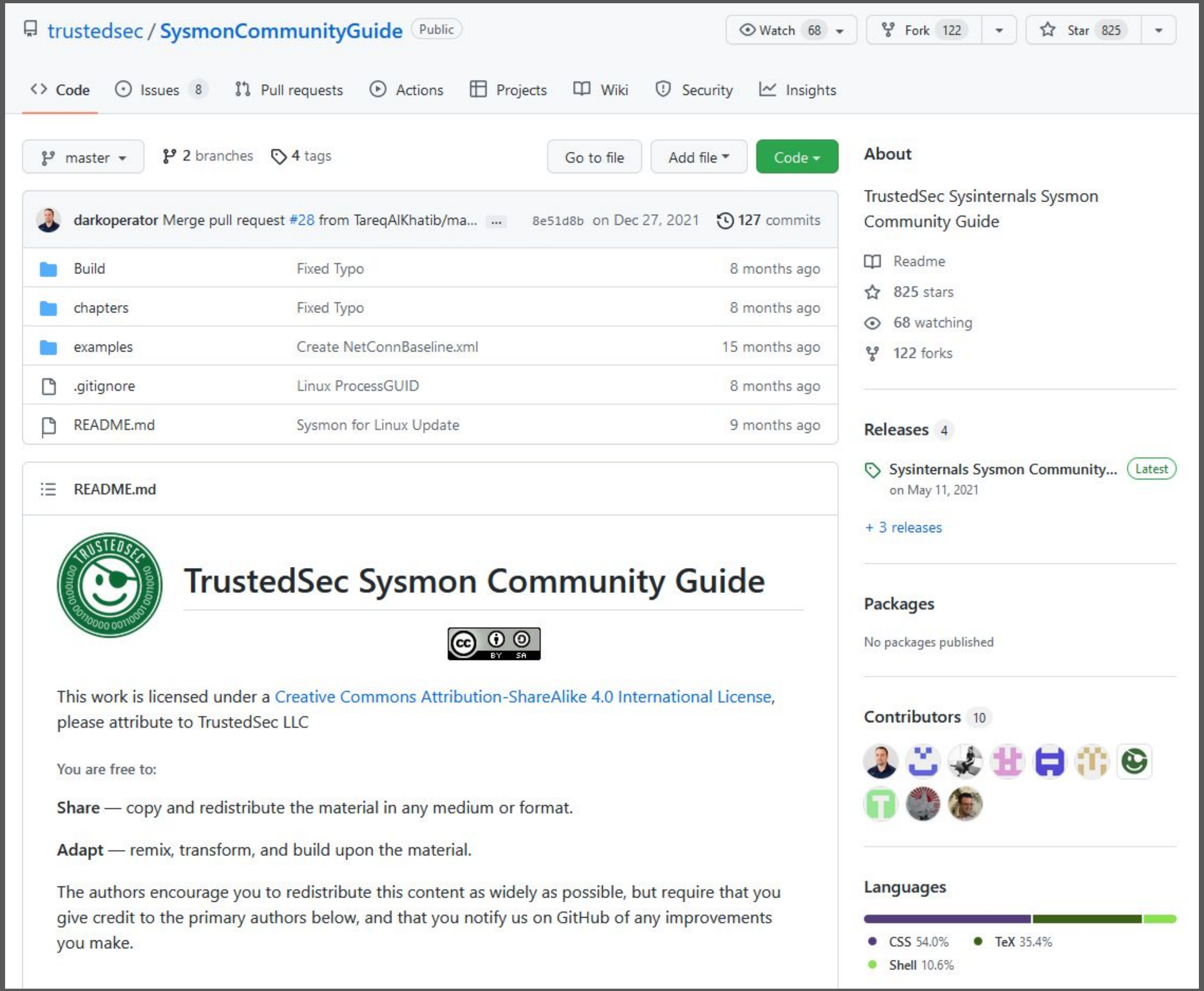
TrustedSec Sysmon Community Guide

TrustedSec has a wonderful Sysmon guide

Written by Carlos Perez



Carlos Perez
darkoperator



darkoperator Merge pull request #28 from TareqAlKhatib/ma... 8e51d8b on Dec 27, 2021 127 commits

Build	Fixed Typo	8 months ago
chapters	Fixed Typo	8 months ago
examples	Create NetConnBaseline.xml	15 months ago
.gitignore	Linux ProcessGUID	8 months ago
README.md	Sysmon for Linux Update	9 months ago

README.md

TrustedSec Sysmon Community Guide

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License, please attribute to TrustedSec LLC

You are free to:

Share — copy and redistribute the material in any medium or format.

Adapt — remix, transform, and build upon the material.

The authors encourage you to redistribute this content as widely as possible, but require that you give credit to the primary authors below, and that you notify us on GitHub of any improvements you make.

About

TrustedSec Sysinternals Sysmon Community Guide

Readme
825 stars
68 watching
122 forks

Releases 4

Sysinternals Sysmon Community... Latest
on May 11, 2021

+ 3 releases

Packages

No packages published

Contributors 10

Languages

CSS 54.0% TeX 35.4%
Shell 10.6%

Source: https://github.com/trustedsec/SysmonCommunityGuide

Installing Sysmon

1 - Download Sysmon, unzip

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

2 - Save Sysmon config to the SAME folder

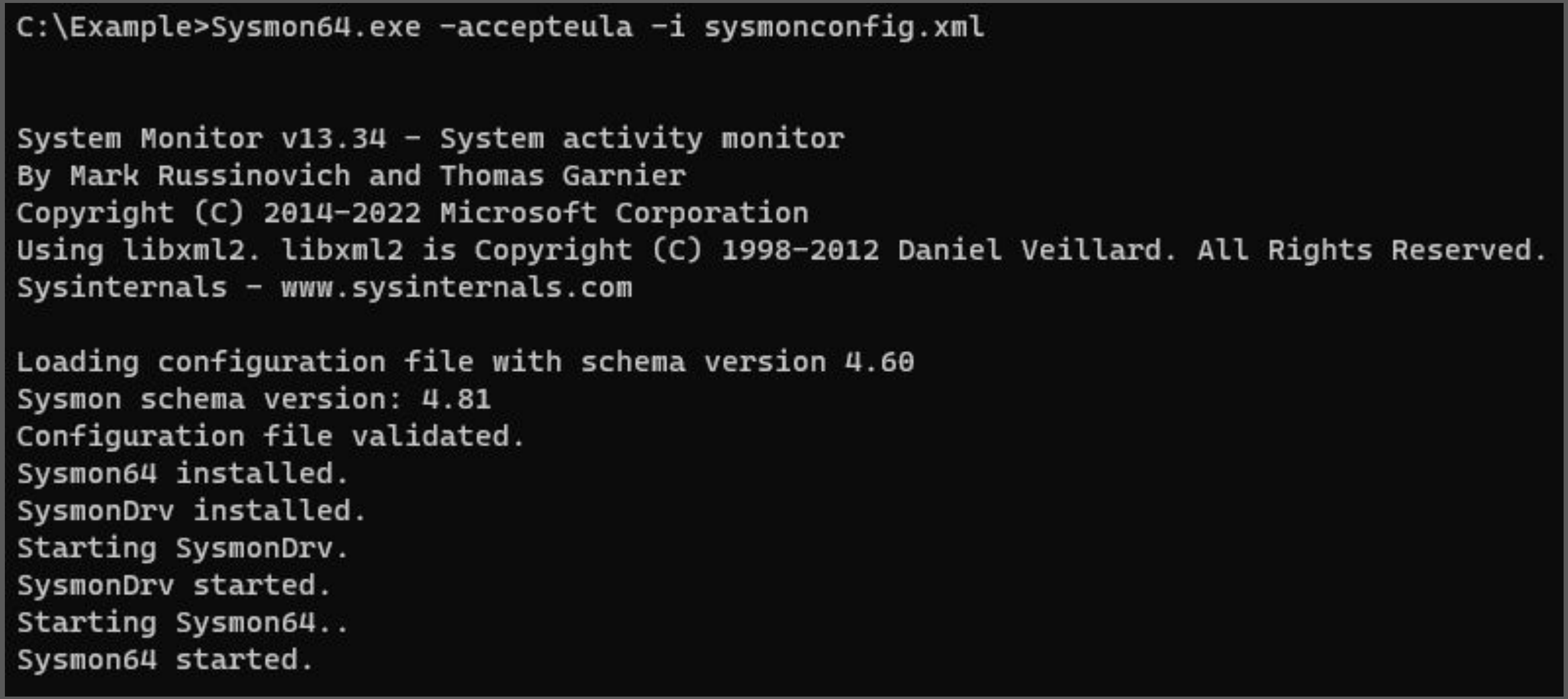
https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml

3 - Run this command:

```
Sysmon64.exe -accepteula -i sysmonconfig.xml
```

Installing Sysmon

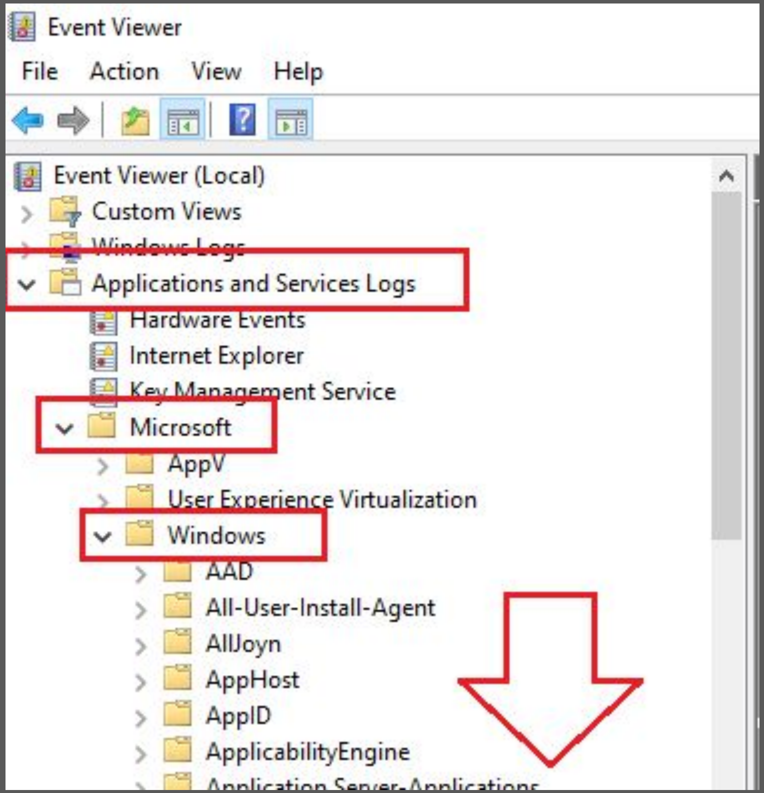
Done

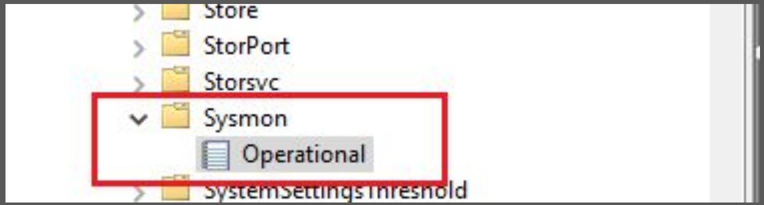


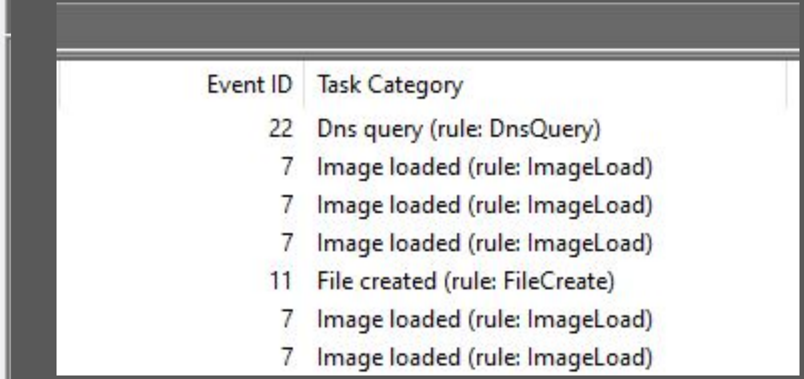
```
C:\Example>Sysmon64.exe -accepteula -i sysmonconfig.xml


System Monitor v13.34 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.60
Sysmon schema version: 4.81
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

Installing Sysmon

To see the Sysmon logs:







Event ID	Task Category
22	Dns query (rule: DnsQuery)
7	Image loaded (rule: ImageLoad)
7	Image loaded (rule: ImageLoad)
7	Image loaded (rule: ImageLoad)
11	File created (rule: FileCreate)
7	Image loaded (rule: ImageLoad)
7	Image loaded (rule: ImageLoad)

Now what?

"OK, I have installed Sysmon ...now what?"

Send Sysmon events to a SIEM!

???

“Wait…what is a SIEM?”

(SIEM) = *Security Information & Event Management*

splunk>

(Paid/Free)

https://www.splunk.com/

Security Onion

(Free)

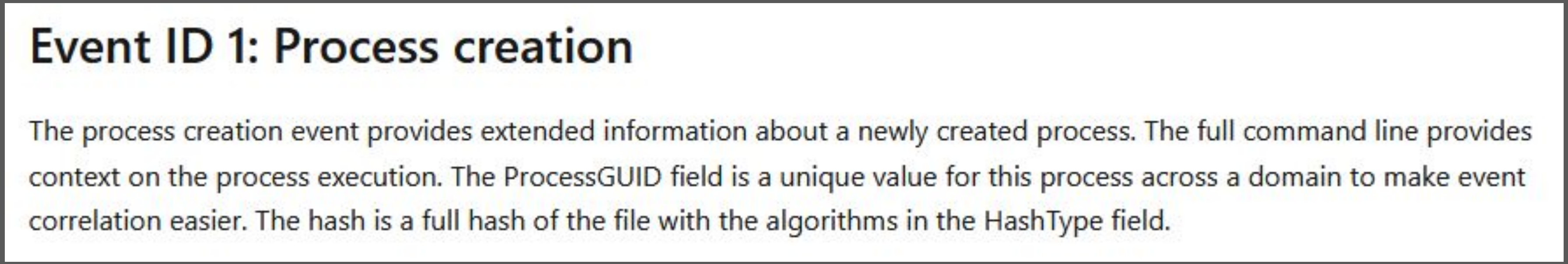
https://securityonionsolutions.com/

elastic stack

(Free)

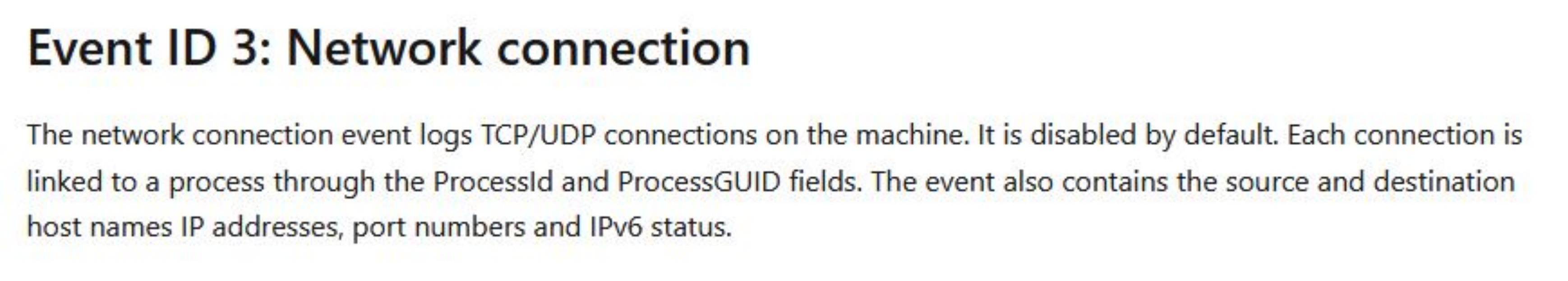
https://www.elastic.co/

Examples of my favorite Sysmon Events



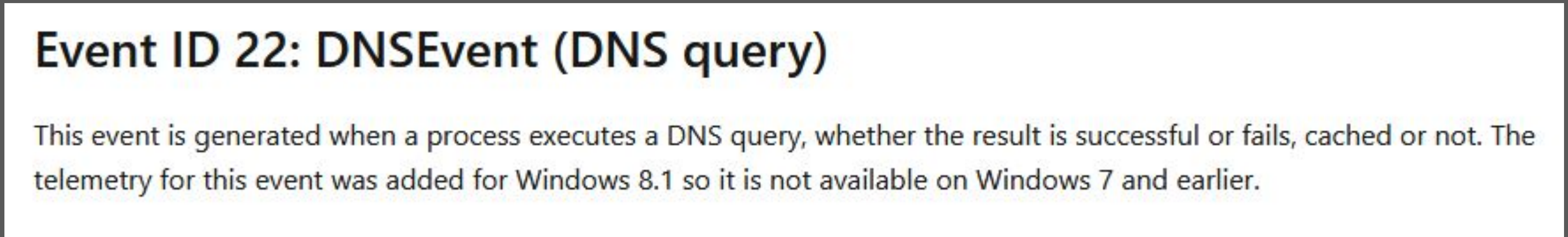
Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.



Event ID 3: Network connection

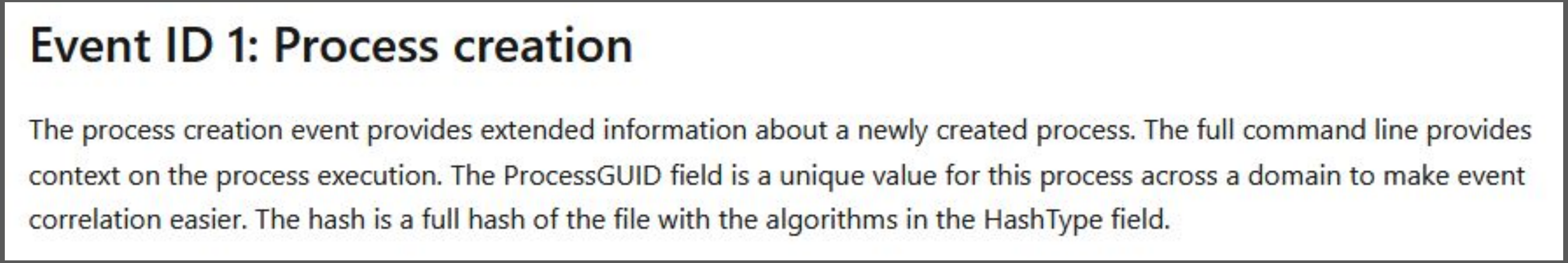
The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.



Event ID 22: DNSEvent (DNS query)

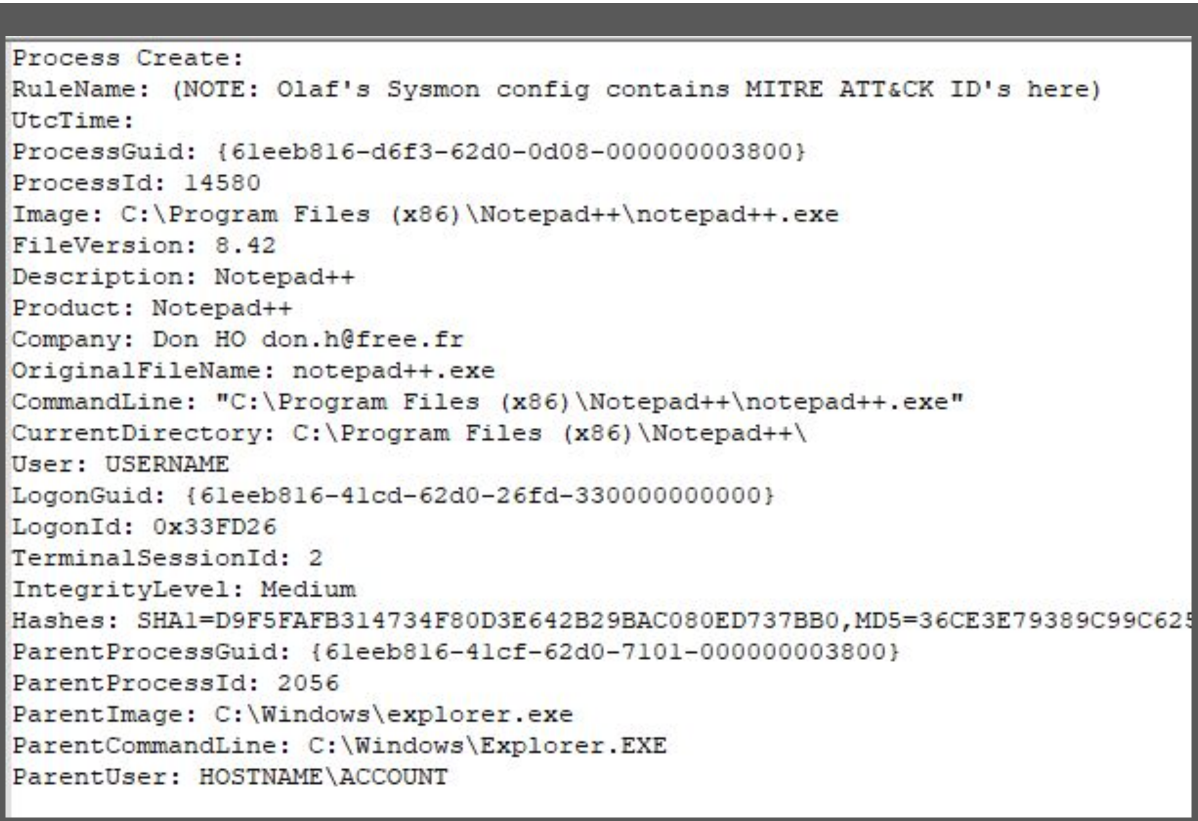
This event is generated when a process executes a DNS query, whether the result is successful or fails, cached or not. The telemetry for this event was added for Windows 8.1 so it is not available on Windows 7 and earlier.

Example: Sysmon Event ID 1



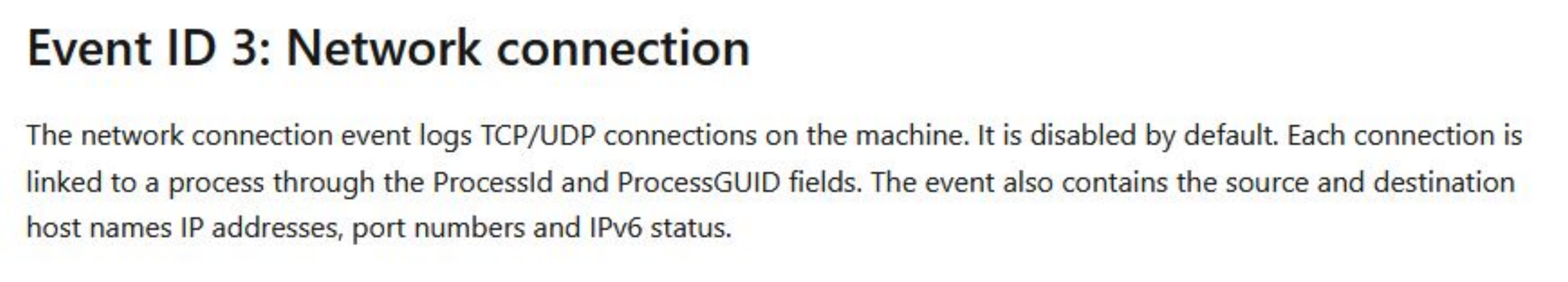
Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.



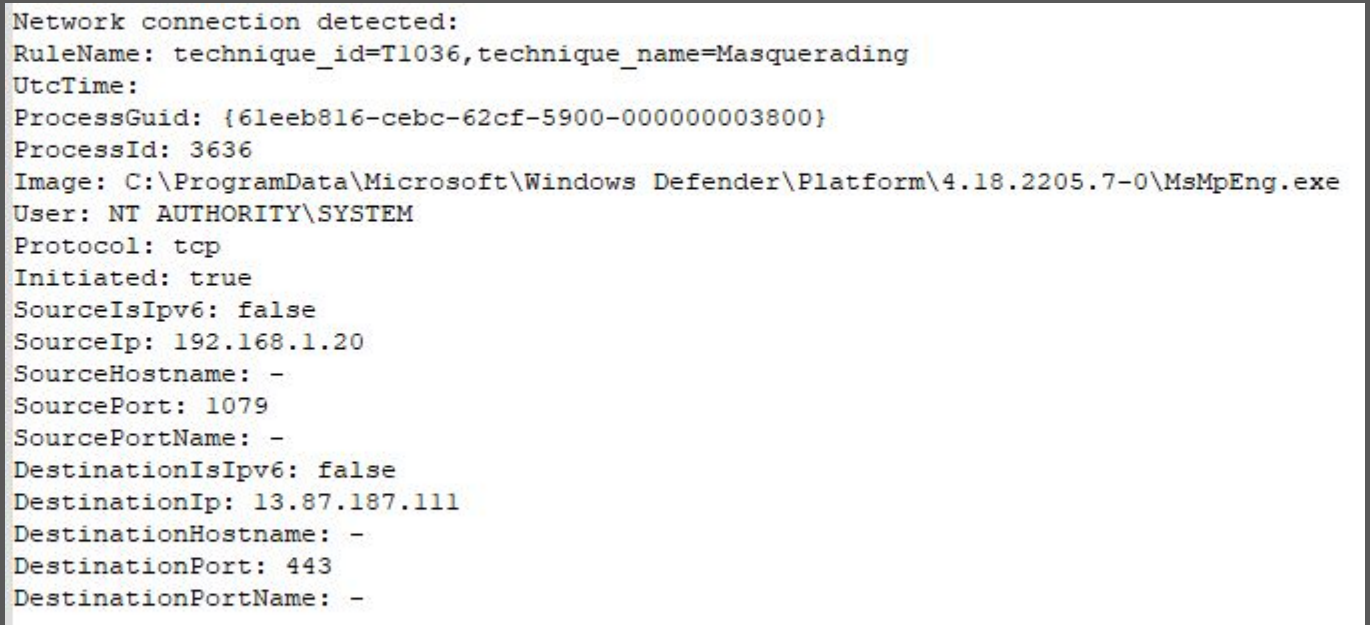
```
Process Create:
RuleName: (NOTE: Olaf's Sysmon config contains MITRE ATT&CK ID's here)
UtcTime:
ProcessGuid: {61eeb816-d6f3-62d0-0d08-000000003800}
ProcessId: 14580
Image: C:\Program Files (x86)\Notepad++\notepad++.exe
FileVersion: 8.42
Description: Notepad++
Product: Notepad++
Company: Don HO don.h@free.fr
OriginalFileName: notepad++.exe
CommandLine: "C:\Program Files (x86)\Notepad++\notepad++.exe"
CurrentDirectory: C:\Program Files (x86)\Notepad++\
User: USERNAME
LogonGuid: {61eeb816-41cd-62d0-26fd-330000000000}
LogonId: 0x33FD26
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA1=D9F5FAFB314734F80D3E642B29BAC080ED737BB0,MD5=36CE3E79389C99C625
ParentProcessGuid: {61eeb816-41cf-62d0-7101-000000003800}
ParentProcessId: 2056
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
ParentUser: HOSTNAME\ACCOUNT
```

Example: Sysmon Event ID 3



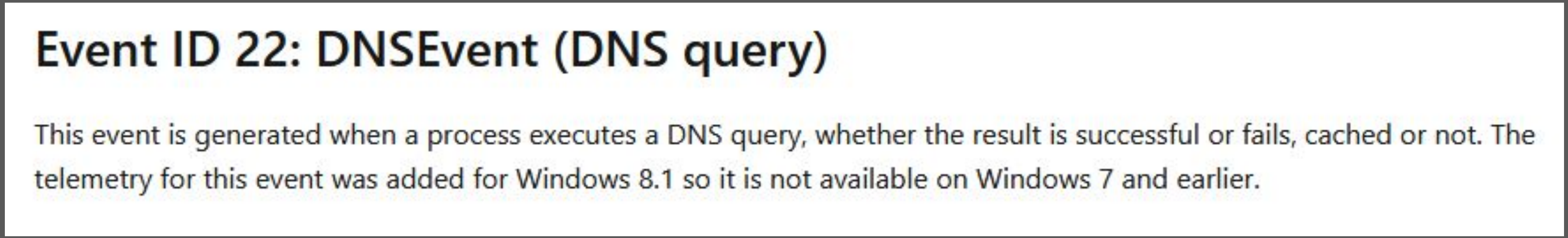
Event ID 3: Network connection

The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.



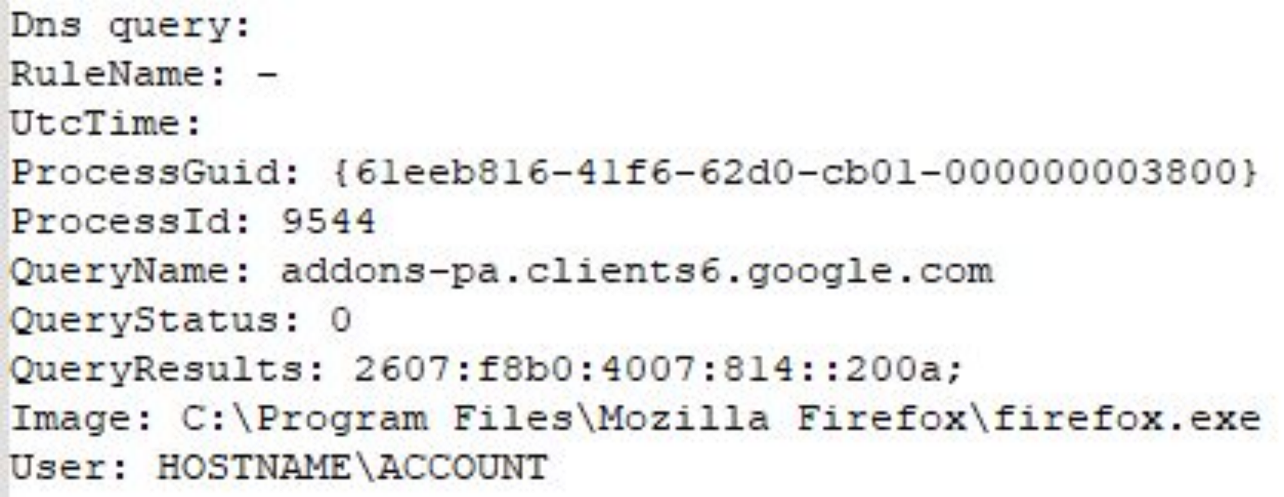
```
Network connection detected:
RuleName: technique_id=T1036,technique_name=Masquerading
UtcTime:
ProcessGuid: {61eeb816-cebc-62cf-5900-000000003800}
ProcessId: 3636
Image: C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2205.7-0\MsMpEng.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.1.20
SourceHostname: -
SourcePort: 1079
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 13.87.187.111
DestinationHostname: -
DestinationPort: 443
DestinationPortName: -
```

Example: Sysmon Event ID 22



Event ID 22: DNSEvent (DNS query)

This event is generated when a process executes a DNS query, whether the result is successful or fails, cached or not. The telemetry for this event was added for Windows 8.1 so it is not available on Windows 7 and earlier.

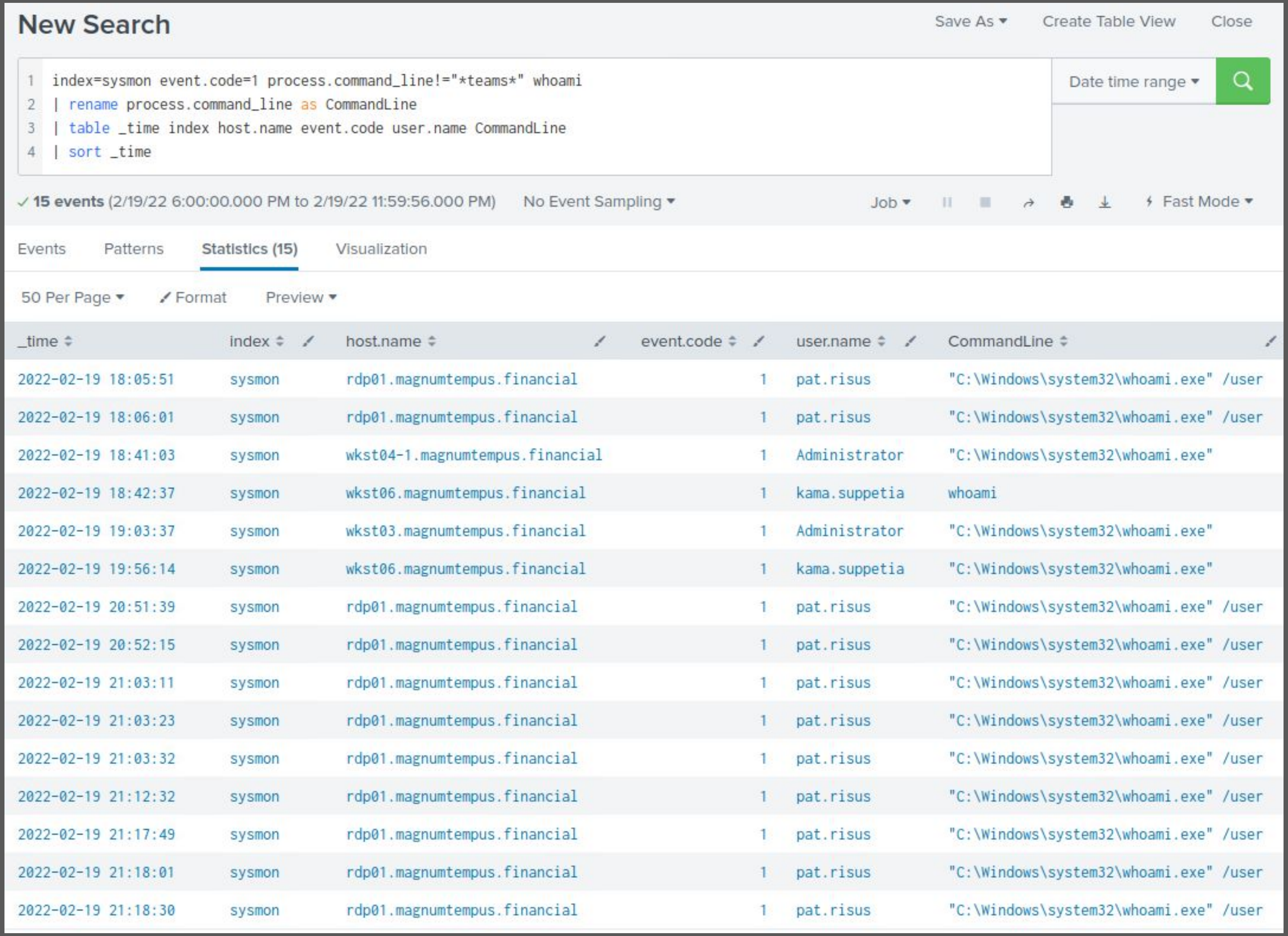


```
Dns query:
RuleName: -
UtcTime:
ProcessGuid: {61eeb816-41f6-62d0-cb01-000000003800}
ProcessId: 9544
QueryName: addons-pa.clients6.google.com
QueryStatus: 0
QueryResults: 2607:f8b0:4007:814::200a;
Image: C:\Program Files\Mozilla Firefox\firefox.exe
User: HOSTNAME\ACCOUNT
```

Sysmon examples during an investigation

Sysmon Event ID 1

“whoami”



```
index=sysmon event.code=1 process.command_line!="*teams*" whoami
| rename process.command_line as CommandLine
| table _time index host.name event.code user.name CommandLine
| sort _time
```

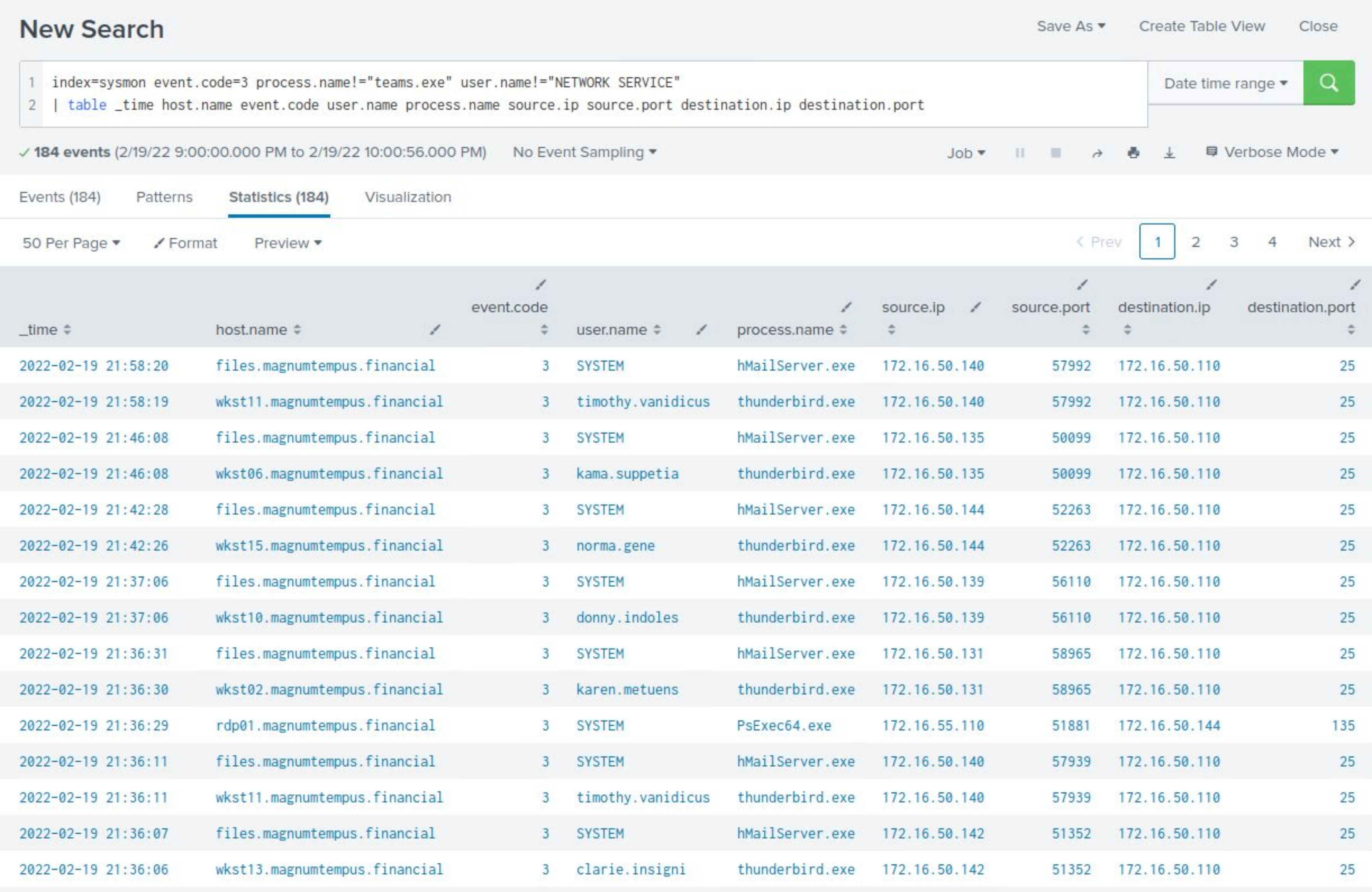
✓ **15 events** (2/19/22 6:00:00.000 PM to 2/19/22 11:59:56.000 PM)

_time	index	host.name	event.code	user.name	CommandLine
2022-02-19 18:05:51	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 18:06:01	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 18:41:03	sysmon	wkst04-1.magnumtempus.financial	1	Administrator	"C:\Windows\system32\whoami.exe"
2022-02-19 18:42:37	sysmon	wkst06.magnumtempus.financial	1	kama.suppetia	whoami
2022-02-19 19:03:37	sysmon	wkst03.magnumtempus.financial	1	Administrator	"C:\Windows\system32\whoami.exe"
2022-02-19 19:56:14	sysmon	wkst06.magnumtempus.financial	1	kama.suppetia	"C:\Windows\system32\whoami.exe"
2022-02-19 20:51:39	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 20:52:15	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:03:11	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:03:23	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:03:32	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:12:32	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:17:49	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:18:01	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:18:30	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user

Sysmon examples during an investigation

Sysmon Event ID 3

"processes"
"sourceIP"
"sourcePort"
"destIP"
"destPort"



```
index=sysmon event.code=3 process.name!="teams.exe" user.name!="NETWORK SERVICE"
| table _time host.name event.code user.name process.name source.ip source.port destination.ip destination.port
```

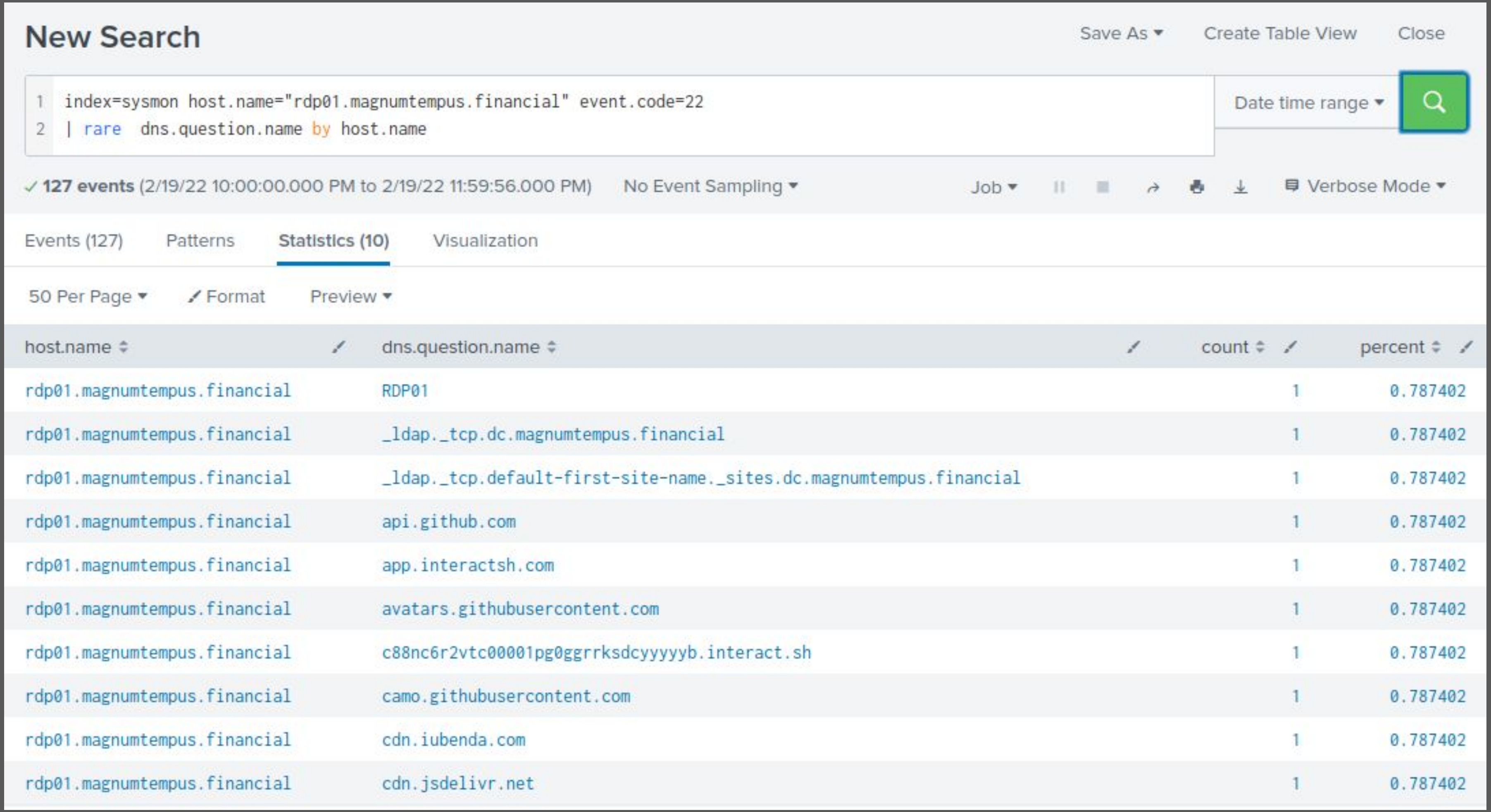
✓ 184 events (2/19/22 9:00:00.000 PM to 2/19/22 10:00:56.000 PM) No Event Sampling ▾

_time	host.name	event.code	user.name	process.name	source.ip	source.port	destination.ip	destination.port
2022-02-19 21:58:20	files.magnumtempus.financial	3	SYSTEM	hMailServer.exe	172.16.50.140	57992	172.16.50.110	25
2022-02-19 21:58:19	wkst11.magnumtempus.financial	3	timothy.vanidicus	thunderbird.exe	172.16.50.140	57992	172.16.50.110	25
2022-02-19 21:46:08	files.magnumtempus.financial	3	SYSTEM	hMailServer.exe	172.16.50.135	50099	172.16.50.110	25
2022-02-19 21:46:08	wkst06.magnumtempus.financial	3	kama.suppetia	thunderbird.exe	172.16.50.135	50099	172.16.50.110	25
2022-02-19 21:42:28	files.magnumtempus.financial	3	SYSTEM	hMailServer.exe	172.16.50.144	52263	172.16.50.110	25
2022-02-19 21:42:26	wkst15.magnumtempus.financial	3	norma.gene	thunderbird.exe	172.16.50.144	52263	172.16.50.110	25
2022-02-19 21:37:06	files.magnumtempus.financial	3	SYSTEM	hMailServer.exe	172.16.50.139	56110	172.16.50.110	25
2022-02-19 21:37:06	wkst10.magnumtempus.financial	3	donny.indoles	thunderbird.exe	172.16.50.139	56110	172.16.50.110	25
2022-02-19 21:36:31	files.magnumtempus.financial	3	SYSTEM	hMailServer.exe	172.16.50.131	58965	172.16.50.110	25
2022-02-19 21:36:30	wkst02.magnumtempus.financial	3	karen.metuens	thunderbird.exe	172.16.50.131	58965	172.16.50.110	25
2022-02-19 21:36:29	rdp01.magnumtempus.financial	3	SYSTEM	PsExec64.exe	172.16.55.110	51881	172.16.50.144	135
2022-02-19 21:36:11	files.magnumtempus.financial	3	SYSTEM	hMailServer.exe	172.16.50.140	57939	172.16.50.110	25
2022-02-19 21:36:11	wkst11.magnumtempus.financial	3	timothy.vanidicus	thunderbird.exe	172.16.50.140	57939	172.16.50.110	25
2022-02-19 21:36:07	files.magnumtempus.financial	3	SYSTEM	hMailServer.exe	172.16.50.142	51352	172.16.50.110	25
2022-02-19 21:36:06	wkst13.magnumtempus.financial	3	clarie.insigni	thunderbird.exe	172.16.50.142	51352	172.16.50.110	25

Sysmon examples during an investigation

Sysmon Event ID 22

“rare DNS”



```
index=sysmon host.name="rdp01.magnumtempus.financial" event.code=22
| rare  dns.question.name by host.name
```

✓ 127 events (2/19/22 10:00:00.000 PM to 2/19/22 11:59:56.000 PM)

host.name	dns.question.name	count	percent
rdp01.magnumtempus.financial	RDP01	1	0.787402
rdp01.magnumtempus.financial	_ldap._tcp.dc.magnumtempus.financial	1	0.787402
rdp01.magnumtempus.financial	_ldap._tcp.default-first-site-name._sites.dc.magnumtempus.financial	1	0.787402
rdp01.magnumtempus.financial	api.github.com	1	0.787402
rdp01.magnumtempus.financial	app.interactsh.com	1	0.787402
rdp01.magnumtempus.financial	avatars.githubusercontent.com	1	0.787402
rdp01.magnumtempus.financial	c88nc6r2vtc00001pg0ggrrksdcyyyyyb.interact.sh	1	0.787402
rdp01.magnumtempus.financial	camo.githubusercontent.com	1	0.787402
rdp01.magnumtempus.financial	cdn.iubenda.com	1	0.787402
rdp01.magnumtempus.financial	cdn.jsdelivr.net	1	0.787402

Some closing thoughts on Sysmon

“Rarely”

“Never”

“Hardly Ever”

“Never”

“Rarely”

“Yes, but not configured to send to the SIEM”

Project Obsidian

THANK YOU!

join the conversation

https://discord.blueteamvillage.org