

Sysmon uses and methods

⇒ Sysmon Events logs IDs may have been many, but we learn important IDs

The screenshot shows a web-based documentation interface for Sysmon. On the left is a sidebar with a navigation tree:

- Home
- Downloads
 - Downloads
 - File and Disk Utilities
 - Networking Utilities
 - Process Utilities
 - Security Utilities
 - Security Utilities
 - Autologon
 - LogonSessions
 - NewSID
 - PsLoggedOn
 - PsLogList
 - RootkitRevealer
 - Sysmon
 - System Information
 - Miscellaneous
 - Sysinternals Suite
 - Microsoft Store
- Community
- Resources

Below the sidebar, there's a search bar labeled "Filter by title". The main content area has a dark header "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 is triggered when a process creates a socket connection 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

Additional resources

- Training
 - Module
 - Connect Windows hosts to Microsoft Sentinel - Training
 - Connect Windows hosts to Microsoft Sentinel
- Documentation
 - Windows Server with Sysmon installed stops responding on startup when applying Group Policy - Windows Server
 - Helps resolve an issue in which Windows Server that has Sysmon installed stops responding on startup when applying Group Policy.
- PsLogList - Sysinternals
 - Dump event log records.

Unnecessarily file (that official Windows binary)

```

<EventFiltering>

<!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
<!--COMMENT: All processes launched will be logged, except for what matches a rule below. It's best to be a
to avoid user-mode executables imitating other process names to avoid logging, or if malware drops fil
Ultimately, you must weigh CPU time checking many detailed rules, against the risk of malware exploiti
Beware of Masquerading, where attackers imitate the names and paths of legitimate tools. Ideally, you'
code signatures to validate, but Sysmon does not support that. Look into AppLocker/WindowsDeviceGuard

<!--DATA: UtcTime, ProcessGuid, ProcessID, Image, FileVersion, Description, Product, Company, CommandLine, Cur
<RuleGroup name="" groupRelation="or">
    <ProcessCreate onmatch="exclude"> |----->
        <!--SECTION: Microsoft Windows-->
        <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.exe" "-queueReporting_svc" </CommandL
        <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe /ProcessId</CommandLine> <!--Windo
        <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -Embedding</CommandLine> <!--
        <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding</Command
        <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upload</CommandLine> <!--Windows:Windows e
        <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Embedding</CommandLine> <!--Windows
        <CommandLine condition="is">C:\Windows\system32\wermgr.exe -queueReporting</CommandLine> <!--Windows:W
        <CommandLine condition="is">\??\C:\Windows\system32\autochk.exe *</CommandLine> <!--Microsoft:Bootup:
        <CommandLine condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!--Microsoft:Bootup: Windows
        <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.exe -Embedding</CommandLine> <!--Windows

```

Important Sysmon IDs

⇒ Note: This is not enough, but important, so in more cases, the Microsoft Sysmon event log

Sysmon IDs

Sysmon Event IDs

- **Event ID 1 - Process Creation**
- **Event ID 3 - Network Connection**
- **Event ID 5 - Process Terminated**
- **Event ID 7 - Image Loaded**
- **Event ID 8 - CreateRemoteThread**
- **Event ID 10 - ProcessAccess**
- **Event ID 11 - FileCreate**
- **Event ID 12, 13, 14 - Registry Events**
- **Event ID 15 - FileCreateStreamHash**
- **Event ID 22 - DNSEvent (DNS Query)**
- **Event ID 29 - FileExecutableDetected**

The screenshot shows the Windows Event Viewer interface. A blue Windows logo is in the top right. Below it is a window titled "Event Properties - Event 1, Sysmon". The window has tabs for "General" and "Details". The "General" tab displays event details:

Log Name:	Microsoft-Windows-Sysmon/Operational
Source:	Sysmon
Event ID:	1
Level:	Information
User:	SYSTEM
OpCode:	Info
More Information:	Event Log Online Help

The "Details" tab shows the raw XML event data:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">



Process Create:  
RuleName: UtcTime: 2019-06-20 15:28:51.261  
ProcessGuid: {f583b782-a633-5d0b-0000-00102664e103}  
ProcessId: 1  
Image: C:\Windows\System32\regasm32.exe  
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)  
Description: Microsoft(R) Register Service  
Product: Microsoft(R) Windows 10 Pro Operating System  
Company: Microsoft Corporation  
OriginalFileName: REGASM32.EXE  
CommandLine: regasm32 /s /n /u /https://www.binarydefense.com/file.sct scrobj.dll  
CurrentDirectory: C:\WINDOWS\system32  
User: DESKTOP-3VNDNSI\SYSTEM  
LogonId: {f583b782-4825-5cf4-0000-0020ce671400}  
LogonId: 0x14670CE  
TerminalSessionId: 1  
IntegerValue: 1  
HexValue: 0x1  
Hashes: MD5-D4DE8A777D16AE18BD9C642A9F42223 SHA256-F098FA150D9199732B4EC2E81528A951503A30F75AFEBF7E7A48360301750C67  
ParentProcessGuid: {f583b782-a619-5d0b-0000-0010ef45d703}  
ParentProcessId: 11152  
ParentImage: C:\Windows\System32\cmd.exe  
ParentCommandLine: "C:\Windows\system32\cmd.exe"
```

Methodology

Note ⇒ Many processes come in even the Sysmon use case, but we find malicious indicators, so using the methodology is very important

Event logs important columns

Subject

Processid ⇒ (Very important correlation case like parent-child)

Processgui id

Hashs

Computer name ⇒ (malware computer name)

Image path

Destination IP ⇒ (reverse shell IP)

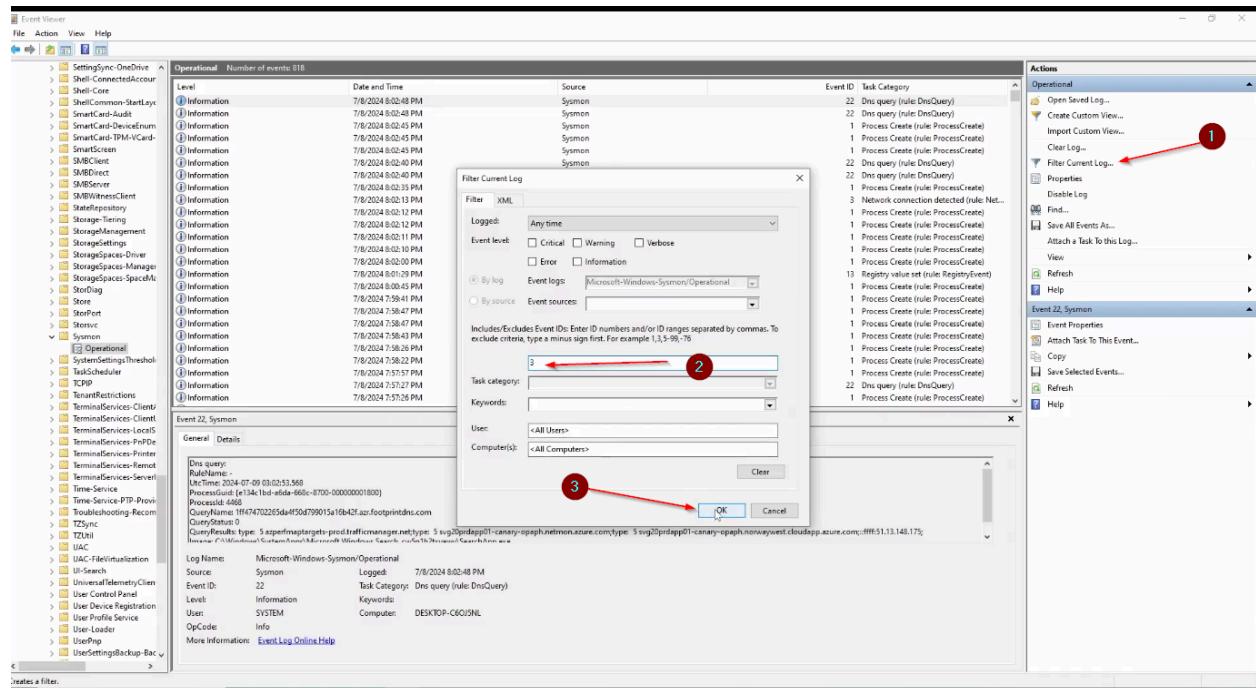
Destination port ⇒ (reverse shell port)

Time ⇒ (terminate download any many case time)

Let's practical Use Sysmon Via Event Viewer:

1.) First network event log analysis

⇒ Malware use Metasploit (reference malware create section)



Analysis

Operational Number of events: 818			
Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 3. Number of events: 6			
Level	Date and Time	Source	Event ID Task Category
Information	7/8/2024 8:02:13 PM	Sysmon	3 Network connection detected (rule: Net...)
Information	7/8/2024 7:51:54 PM	Sysmon	3 Network connection detected (rule: Net...)
Information	7/8/2024 7:51:54 PM	Sysmon	3 Network connection detected (rule: Net...)
Information	7/8/2024 7:51:54 PM	Sysmon	3 Network connection detected (rule: Net...)
Information	7/8/2024 7:51:54 PM	Sysmon	3 Network connection detected (rule: Net...)
Information	7/8/2024 7:51:54 PM	Sysmon	3 Network connection detected (rule: Net...)

Event 3, Sysmon	
General	Details
Network connection detected: RuleName: Usermode UtcTime: 2024-07-09 03:02:08.748 ProcessGuid: {e134c1bd-a834-668c-c800-000000001800} ProcessId: 4056 Image: C:\Users\tcm\Downloads\notmalware.exe User: DESKTOP-C6OJ5NL\tcm Protocol: tcp Initiated: true SourceIsIPv6: false SourceIP: 192.168.1.9 SourceHostname: DESKTOP-C6OJ5NL.net.rogers.com SourcePort: 49722 SourcePortName: - DestinationIsIPv6: false DestinationIP: 192.168.1.4 DestinationHostname: - DestinationPort: 444 DestinationPortName: -	
Log Name:	Microsoft-Windows-Sysmon/Operational
Source:	Sysmon
Event ID:	3
Level:	Information
User:	SYSTEM
OpCode:	Info
More Information:	Event Log Online Help

2.) Correlation process (find parent and child process) and use find features on event view tool:

- Copy PROCESS ID ⇒ 4056

See my process logs came this place use methodology

Operational Number of events: 818

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 463

Level	Date and Time	Source	Event ID	Task Category
(i) Information	7/8/2024 7:14:13 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:14:13 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:14:13 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:13:56 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:13:46 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:13:42 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:13:30 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:13:22 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:13:17 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:13:13 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:12:59 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:12:55 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

Use find features

Operational Number of events: 818 (0) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 463

Level	Date and Time	Source	Event ID	Task Category
(i) Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:35 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:12 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:12 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:11 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:10 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:02:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 8:00:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:59:41 PM	Sysmon	1	Process Create (rule: ProcessCreate)
(i) Information	7/8/2024 7:58:47 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

Actions

- Operational
 - Open Saved Log...
 - Create Custom View...
 - Import Custom View...
 - Clear Log...
 - Filter Current Log...
 - Clear Filter
 - Properties
 - Disable Log
 - Find...
 - Save Filtered Log File As...
 - Attach a Task To this Log...
 - Save Filter to Custom View...
 - View
 - Refresh

Operational Number of events: 818 (!) New events available

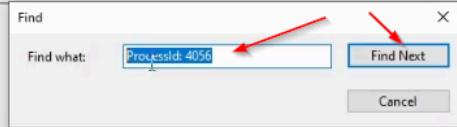
Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 463

Level	Date and Time	Source	Event ID	Task Category
(i) Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:35 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:12 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:12 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:11 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:10 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:02:00 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 8:00:45 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 7:59:41 PM	Sysmon	1	Process Create (rule)
(i) Information	7/8/2024 7:58:47 PM	Sysmon	1	Process Create (rule)

Event 1, Sysmon

General Details

Process Create:
 RuleName: -
 UtcTime: 2024-07-09 03:02:12.497
 ProcessGuid: {e134c1bd-a834-668c-c800-000000001800}
 ProcessId: 4056
 Image: C:\Users\tcm\Downloads\notmalware.exe
 FileVersion: 2.2.14
 Description: ApacheBench command line utility
 Product: Apache HTTP Server
 Company: Apache Software Foundation
 OriginalFileName: ab.exe
 CommandLine: "C:\Users\tcm\Downloads\notmalware.exe"
 CurrentDirectory: C:\Users\tcm\Downloads\
 User: DESKTOP-C60J5NL\tcm
 LoonanGuid: {e134c1bd-a6d4-668c-29ec-090000000000}



Analysis

See only extract specific process id

Operational Number of events: 818 (0) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 463

Level	Date and Time	Source	Event ID	Task Category
Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 8:02:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 8:02:35 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 8:02:12 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 8:02:12 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 8:02:11 PM	Sysmon	1	Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

```

Process Create:
RuleName: -
UtcTime: 2024-07-09 03:02:12.497
ProcessGuid: {e134c1bd-a834-668c-c800-000000001800}
ProcessId: 4056
Image: C:\Users\tcm\Downloads\notmalware.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\tcm\Downloads\notmalware.exe"
CurrentDirectory: C:\Users\tcm\Downloads\
User: DESKTOP-C6OJ5NL\tcm
LogonGuid: {e134c1bd-a6d4-668c-7c00-000000001800}
LogonId: 0x9EC29
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=C9B683A80863AC6EE518F9108FF8B5E9,SHA256=63E30BF48E698F1D0FAB41BB95116F6B7CC558558C148A6C3AACCB286D3453A9A,IMPHASH=481F47BBB2C9C21E108D65F52B04C448
ParentProcessGuid: {e134c1bd-a6d4-668c-7c00-000000001800}
ParentProcessId: 3116
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
ParentUser: DESKTOP-C6OJ5NL\tcm

```

Event 1, Sysmon

General Details

```

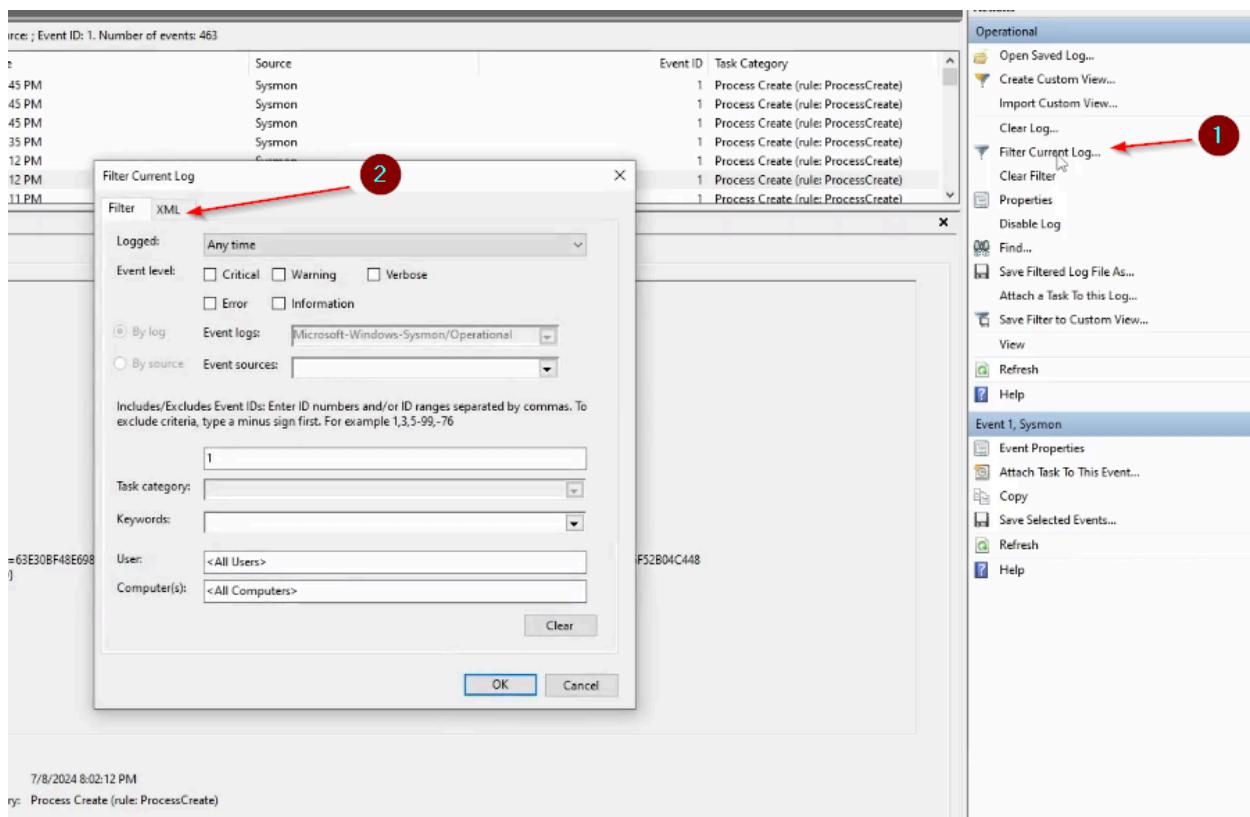
Process Create: ←
RuleName: - ←
UtcTime: 2024-07-09 03:02:12.497 ←
ProcessGuid: {e134c1bd-a834-668c-c800-000000001800} ←
ProcessId: 4056 ←
Image: C:\Users\tcm\Downloads\notmalware.exe ←
FileVersion: 2.2.14 ←
Description: ApacheBench command line utility ←
Product: Apache HTTP Server ←
Company: Apache Software Foundation ←
OriginalFileName: ab.exe ←
CommandLine: "C:\Users\tcm\Downloads\notmalware.exe" ←
CurrentDirectory: C:\Users\tcm\Downloads\ ←
User: DESKTOP-C6OJ5NL\tcm ←
LogonGuid: {e134c1bd-a6d4-668c-7c00-000000001800} ←
LogonId: 0x9EC29 ←
TerminalSessionId: 1 ←
IntegrityLevel: High ←
Hashes: MD5=C9B683A80863AC6EE518F9108FF8B5E9,SHA256=63E30BF48E698F1D0FAB41BB95116F6B7CC558558C148A6C3AACCB286D3453A9A,IMPHASH=481F47BBB2C9C21E108D65F52B04C448 ←
ParentProcessGuid: {e134c1bd-a6d4-668c-7c00-000000001800} ←
ParentProcessId: 3116 ←
ParentImage: C:\Windows\explorer.exe ←
ParentCommandLine: C:\Windows\Explorer.EXE ←
ParentUser: DESKTOP-C6OJ5NL\tcm ←

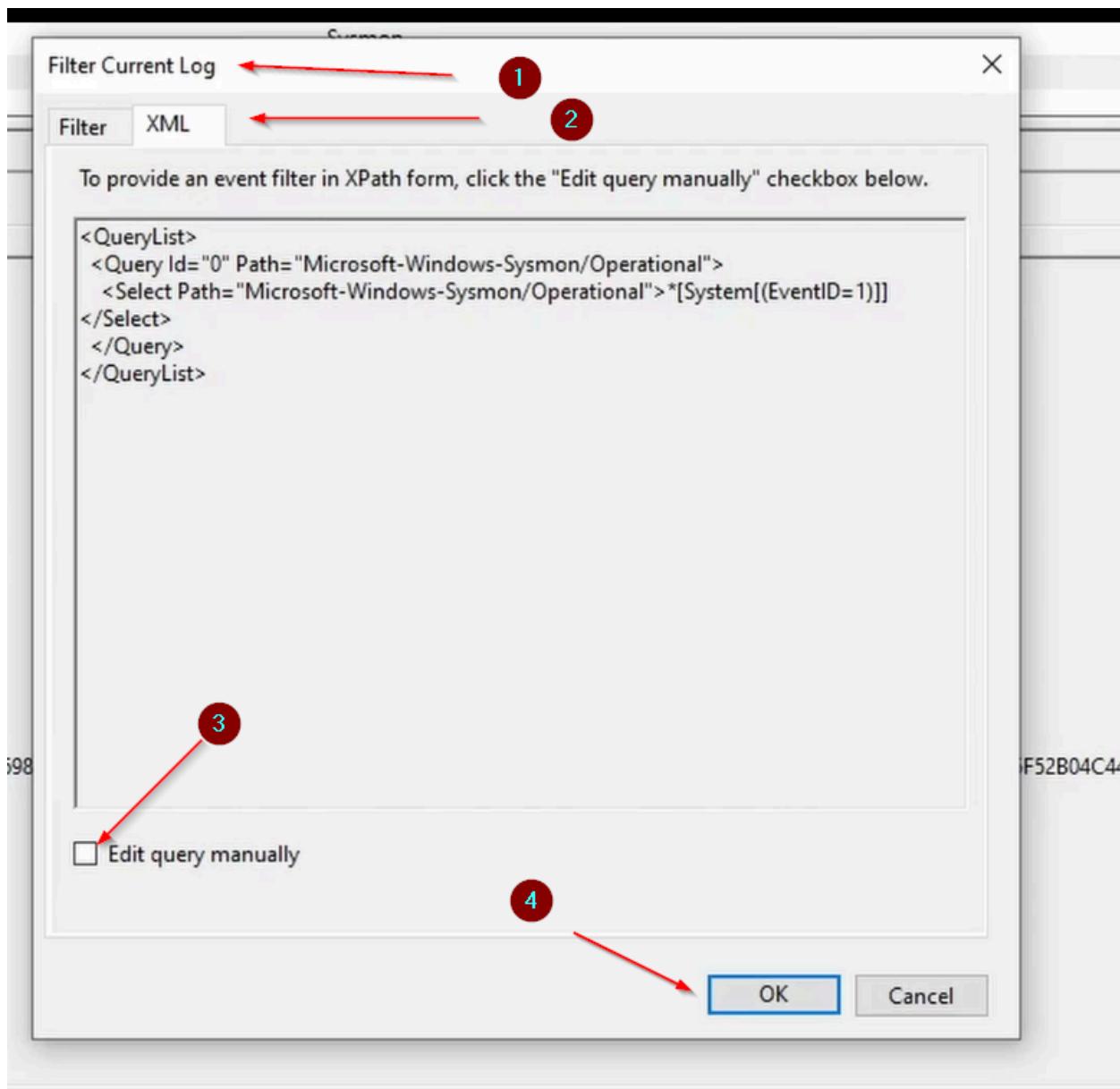
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1

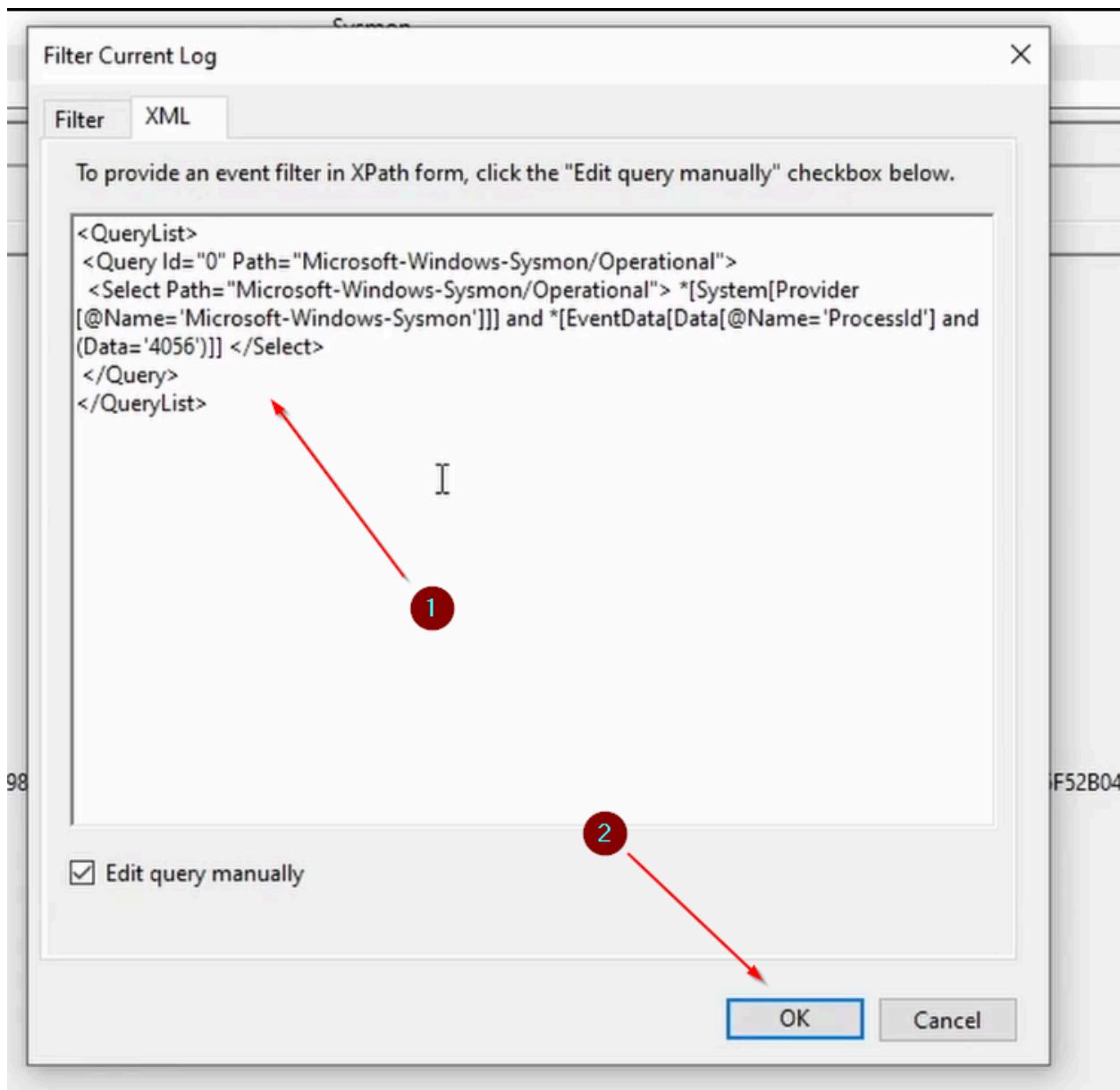
Logged: 7/8/2024 8:02:12 PM
Task Category: Process Create (rule: ProcessCreate)

More advanced analysis uses XML filter search alter find features:





Use advanced search filter XML format query



Result:

⇒ See particular process-related ID execute

Operational Number of events: 1,155

Filtered: Advanced filter, click on 'Filter' command to view filter configuration.. Number of events: 7

Level	Date and Time	Source	Event ID	Task Category
Information	7/8/2024 8:02:13 PM	Sysmon	3	Network connection detected (rule: Net...)
Information	7/8/2024 8:02:12 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 7:58:26 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	7/8/2024 7:51:54 PM	Sysmon	3	Network connection detected (rule: Net...)
Information	7/8/2024 7:51:54 PM	Sysmon	3	Network connection detected (rule: Net...)
Information	7/8/2024 7:51:54 PM	Sysmon	3	Network connection detected (rule: Net...)
Information	7/8/2024 7:11:31 PM	Sysmon	3	Network connection detected (rule: Net...)

Event 3, Sysmon

Advance filter search query:

Event Viewer: Process ID XML Query

```
<QueryList>
<Query Id="0" Path="Microsoft-Windows-Sysmon/Operational">
<Select Path="Microsoft-Windows-Sysmon/Operational"> *
[System[Provider[@Name='Microsoft-Windows-Sysmon']] and *
[EventData[Data[@Name='ProcessId'] and (Data='<ENTER YOUR PID HERE>')]]
</Select>
</Query>
</QueryList>
```

Event Viewer: Process ID XML Query - Process Creation Events

```
<QueryList>
<Query Id="0" Path="Microsoft-Windows-Sysmon/Operational">
<Select Path="Microsoft-Windows-Sysmon/Operational">
*[System[Provider[@Name='Microsoft-Windows-Sysmon'] and (EventID=1)]]
and
*[EventData[Data[@Name='ProcessId'] and (Data='<ENTER YOUR PID HERE>')]]
```

```
</Select>
</Query>
</QueryList>
```

Let's practical Use Sysmon Via Power shell analysis:

PowerShell: Get-WinEvent

```
$ Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational"
```

```
$ Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-
Sysmon/Operational"; id=1}
```

```
$ Get-WinEvent -FilterHashtable @{logname="Microsoft-Windows-
Sysmon/Operational"; id=3} -MaxEvents 1 | Format-List *
```

```
$ Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -FilterXPath
"*[System/EventID=3 and EventData[Data[@Name='DestinationPort']='4444']]"
| Format-List *
```

```
$ Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -FilterXPath
"*[System/EventID=1]"
```

```
$ Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' -FilterXPath
"*[System/EventID=1 and EventData[Data[@Name='ProcessId']='<ENTER YOUR
PID HERE>']]"
| Format-List *
```

References:

<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

<https://github.com/SwiftOnSecurity/sysmon-config>

<https://github.com/ParrotSec/mimikatz>

<https://github.com/PeterDaveHello/top-1m-domains>

Common knowledge:

process creation:

Important columns process id (unique execution id),hash

Network connection:

subject

processid

processgui id

image path

destination IP

hostname

destination port

Methodology:

correlation ⇒ process is important

Ex ⇒ malicious network event log save that analysis case note process id next correlate process creation (use find options)

More advanced methods:

Use filter current log features (use custom XML processid query for correlating all process find case) and (use custom XML event id and processid query for correlating all process find case)

Process terminated:

When the process is terminated, UTC Time is very important

Correlation case process ID and process_GUI is very important

Mark of the web ⇒ MOTW (Use identify, download, potentially indicator, and Windows screen)

11 file create ⇒ example mimikatz

The screenshot shows a list of Sysmon events and a detailed view of one specific event. The list of events shows multiple 'Information' level entries with various timestamps. Below this, a specific event is selected, labeled 'Event 11, Sysmon'. This event is detailed as follows:

File created:	
RuleName:	Downloads
UtcTime:	2024-07-09 03:20:19.901
ProcessGuid:	{e134c1bd-ac73-668c-2b01-000000001800}
ProcessId:	832
Image:	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
TargetFilename:	C:\Users\tcm\Downloads\mimikatz.exe
CreationUtcTime:	2024-07-09 03:19:59.929
User:	DESKTOP-C6OJ5NL\tcm

A red arrow points from the text 'File created:' to the 'File created:' header in the event details. Another red arrow points from the word 'mimikatz.exe' in the TargetFilename field to the word 'mimikatz.exe' in the text above.

12 , 14 Registry event ⇒ This Registry event logs but specific (12 creation and deletion 14 read and rename operations on the registry)

15 file creation stream hash ⇒ This uses find potential file download cases to identify use and Windows screen MOTW (Mark of the Web)



mimikatz

Type of file: Application (.exe)

Description: mimikatz for Windows

Location: C:\Users\tcm\Downloads

Size: 1.19 MB (1,250,056 bytes)

Size on disk: 1.19 MB (1,253,376 bytes)

Created: Monday, July 8, 2024, 8:19:59 PM

Modified: Monday, July 8, 2024, 8:28:26 PM

Accessed: Today, July 8, 2024, 1 minute ago

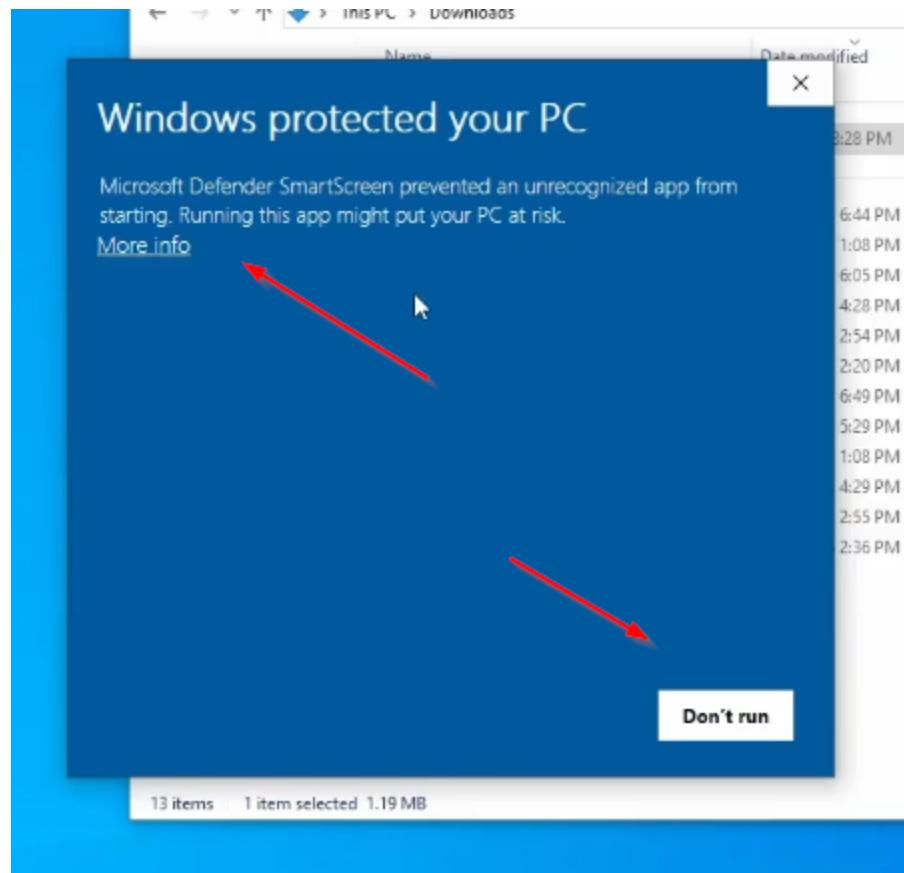
Attributes: Read-only Hidden

[Advanced...](#)

Security: This file came from another
computer and might be blocked to
help protect this computer.

Unblock



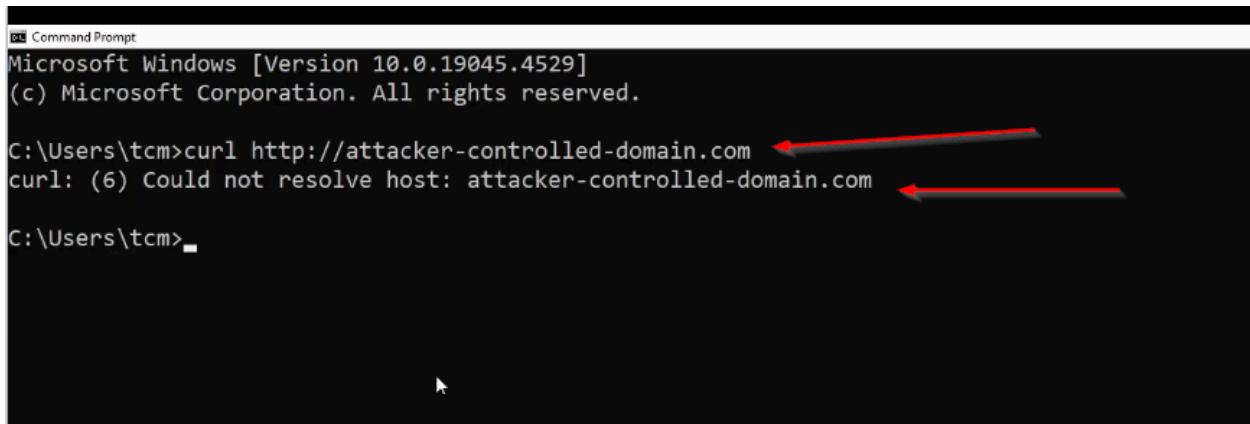


Event 15, Sysmon

General | Details

File stream created: ←
RuleName: -
UtcTime: 2024-07-09 03:28:26.157
ProcessGuid: {e134c1bd-ae59-668c-7501-000000001800} ←
ProcessId: 6032 ←
Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe ←
TargetFilename: C:\Users\tcm\Downloads\mimikatz.exe:Zone.Identifier ←
CreationUtcTime: 2024-07-09 03:19:59.929
Hash: MD5=0F98A5550ABE0FB880568B1480C96A1C,SHA256=2DFB5F4B33E4CF8237B732C02B1F2B1192FFE4B83114BCF821F489BBF48C6AA1,IMPHASH=00000000000000000000000000000000
Contents: [ZoneTransfer] ZoneId=3 HostUrl=https://github.com/
User: DESKTOP-C60J5NL\tcm

22 DNS events log ⇒ DNS query analysis for malware request case



A screenshot of a Microsoft Windows Command Prompt window. The window title is "Command Prompt". The text inside the window reads:

```
Microsoft Windows [Version 10.0.19045.4529]
(c) Microsoft Corporation. All rights reserved.

C:\Users\tcm>curl http://attacker-controlled-domain.com
curl: (6) Could not resolve host: attacker-controlled-domain.com
```

Two red arrows point from the right side of the slide towards the error message "curl: (6) Could not resolve host: attacker-controlled-domain.com".

This image does not contain query results because DNS resolution failed, so no come query results

Operational Number of events: 49

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 22. Number of events: 4

Level	Date and Time	Source	Event ID	Task Category
(i) Information	7/8/2024 8:34:23 PM	Sysmon	22	Dns query (rule: DnsQuery)
(i) Information	7/8/2024 8:28:05 PM	Sysmon	22	Dns query (rule: DnsQuery)
(i) Information	7/8/2024 8:27:43 PM	Sysmon	22	Dns query (rule: DnsQuery)
(i) Information	7/8/2024 8:27:37 PM	Sysmon	22	Dns query (rule: DnsQuery)

Event 22, Sysmon

General Details

Dns query:
 RuleName: -
 UtcTime: 2024-07-09 03:34:22.764
 ProcessGuid: {e134c1bd-afbe-668c-8301-000000001800}
 ProcessId: 4280
 QueryName: attacker-controlled-domain.com
 QueryStatus: 9003
 QueryResults: -
 Image: C:\Windows\System32\curl.exe
 User: DESKTOP-C60J5NL\tcm

Log Name: Microsoft-Windows-Sysmon/Operational
 Source: Sysmon Logged: 7/8/2024 8:34:23 PM
 Event ID: 22 Task Category: Dns query (rule: DnsQuery)
 Level: Information Keywords:
 User: SYSTEM Computer: DESKTOP-C60J5NL
 OpCode: Info
 More Information: [Event Log Online Help](#)

But in this case Query result comes because the DNS resolution is successful

Event 22, Sysmon

General Details

Dns query:
RuleName: -
UtcTime: 2024-07-09 03:27:42,021
ProcessGuid: {e134c1bd-ae2e-668c-4f01-000000001800}
ProcessId: 1204
QueryName: tse1.mm.bing.net
QueryStatus: 0
QueryResults: type: 5 mm-mm.bing.net.trafficmanager.net/type: 5 ax-0001.ax-msedge.net::ffff:150.171.27.10::ffff:150.171.28.10;
Image: C:\Windows\system32\BackgroundTransferHost.exe
User: DESKTOP-C6OJ5NL\tcr

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 22
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

27 Event ⇒ This event ID uses the DLL and PE file block and deletes that file creation

Note ⇒ This is not enough, so learn more. Event IDs refer to Microsoft Sysmon event IDs, like file deletion events, clipboard changes, or different pipe events on the system, so refer to Microsoft Sysmon