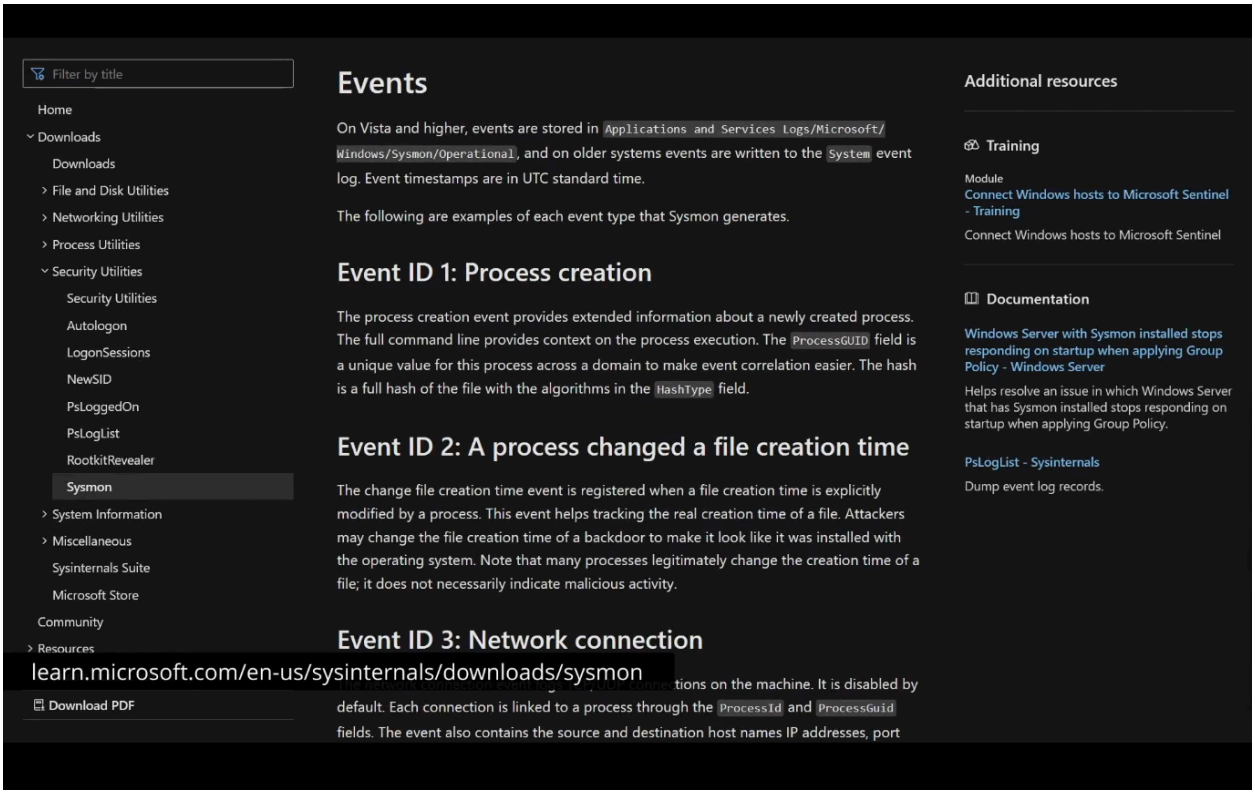
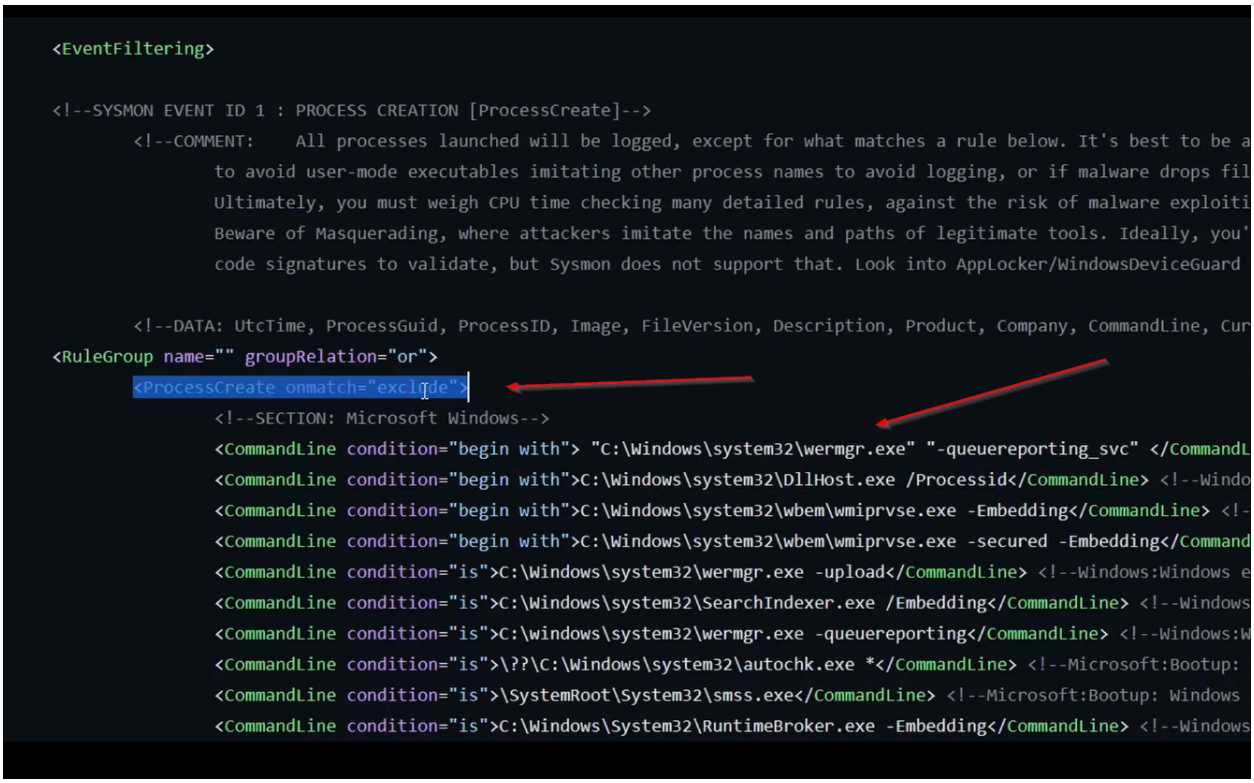
Sysmon uses and methods

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



Unnecessarily file (that official Windows binary)



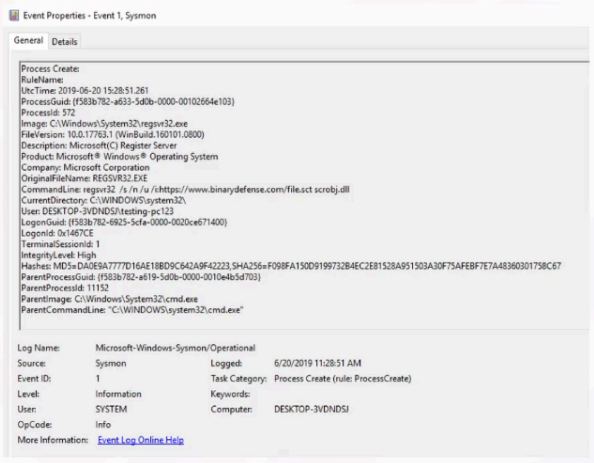
Important Sysmon IDs

⇒ Note: This is not enough, but important,t 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



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

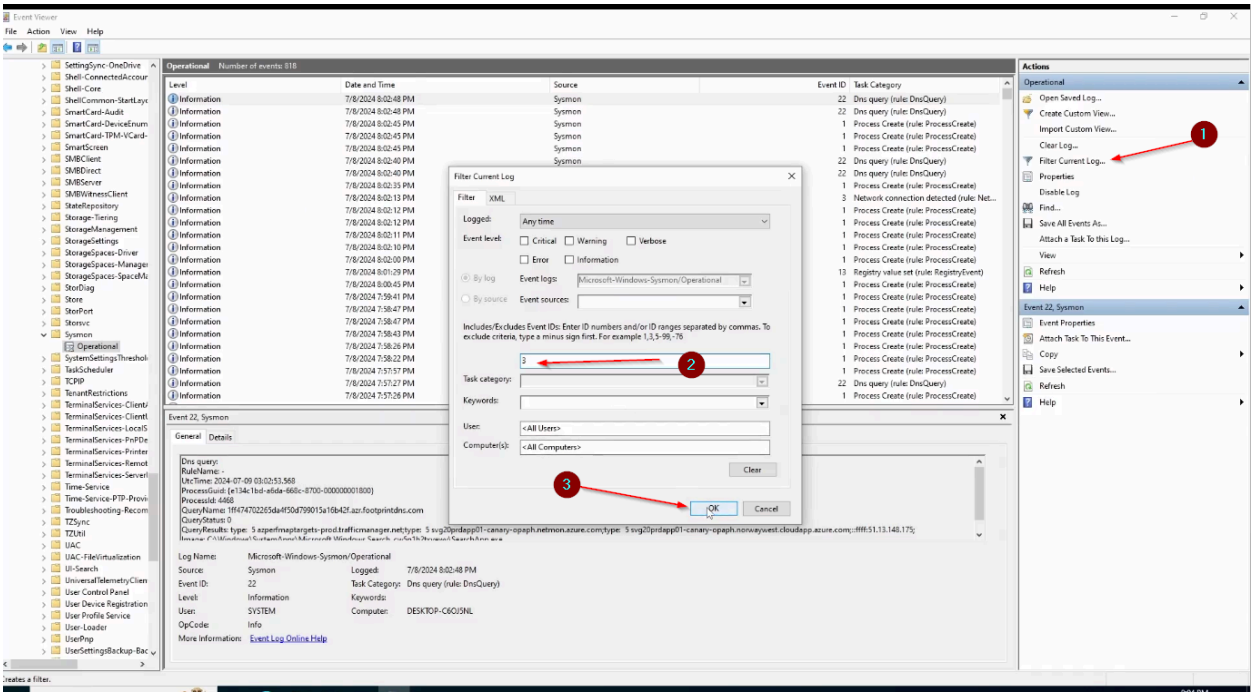
Destination IP ⇒ (reverse shell IP)
Destination port ⇒ (reverse shell port)

Time ⇒ (terminate download any many case time)

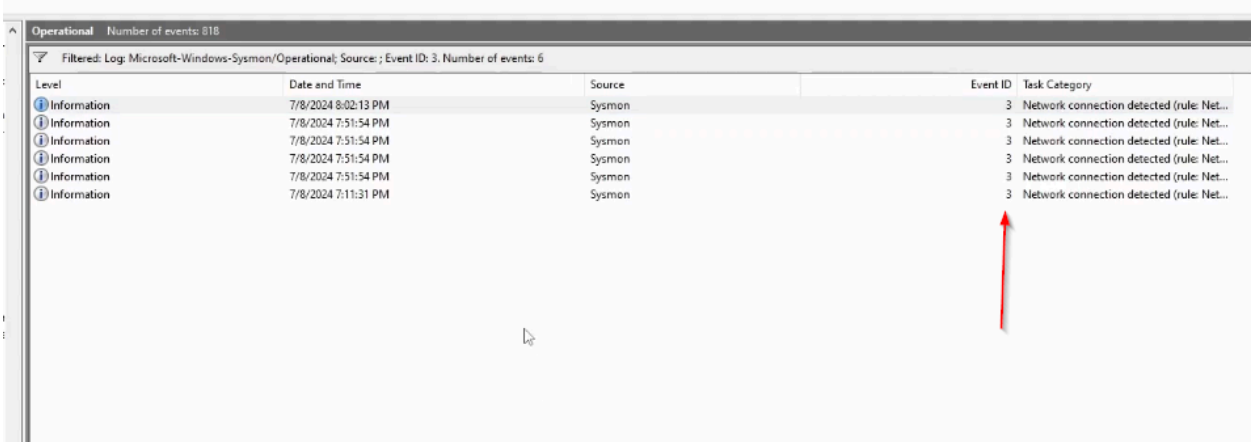
Let's practical Use Sysmon Via Event Viewer:

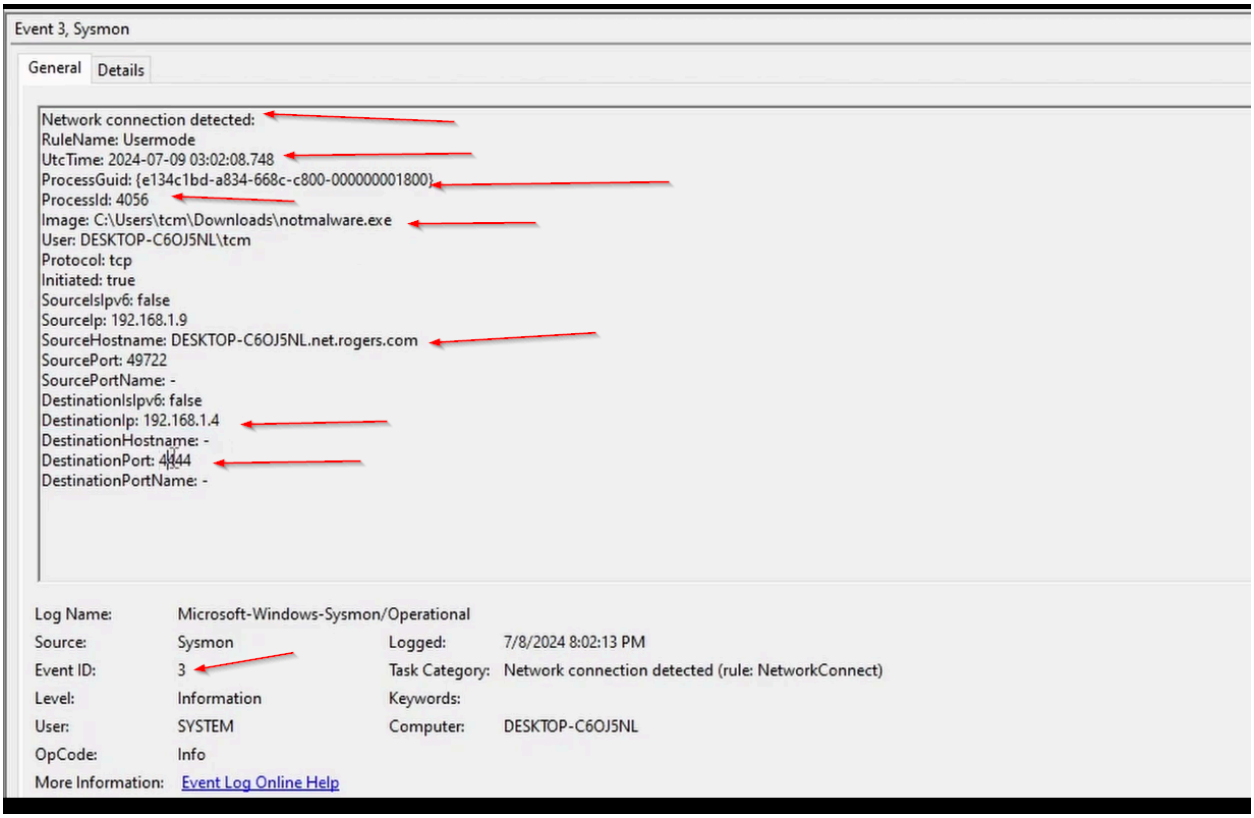
1.) First network event log analysis

⇒ Malware use Metasploit (reference malware create section)



Analysis

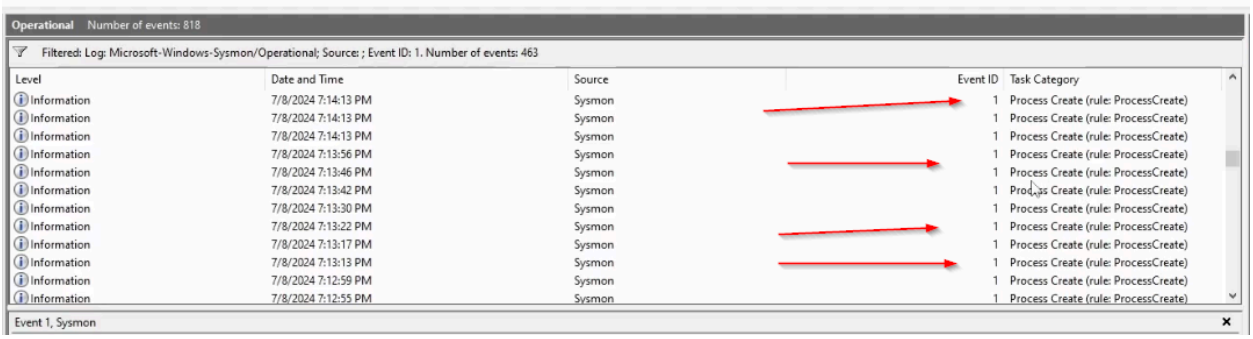




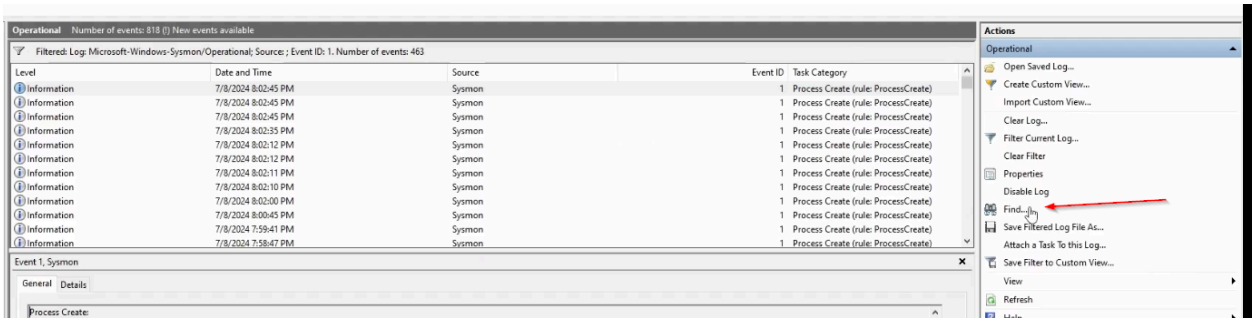
2.) Correlation process (find parent and child process) and use find features on event view tool:

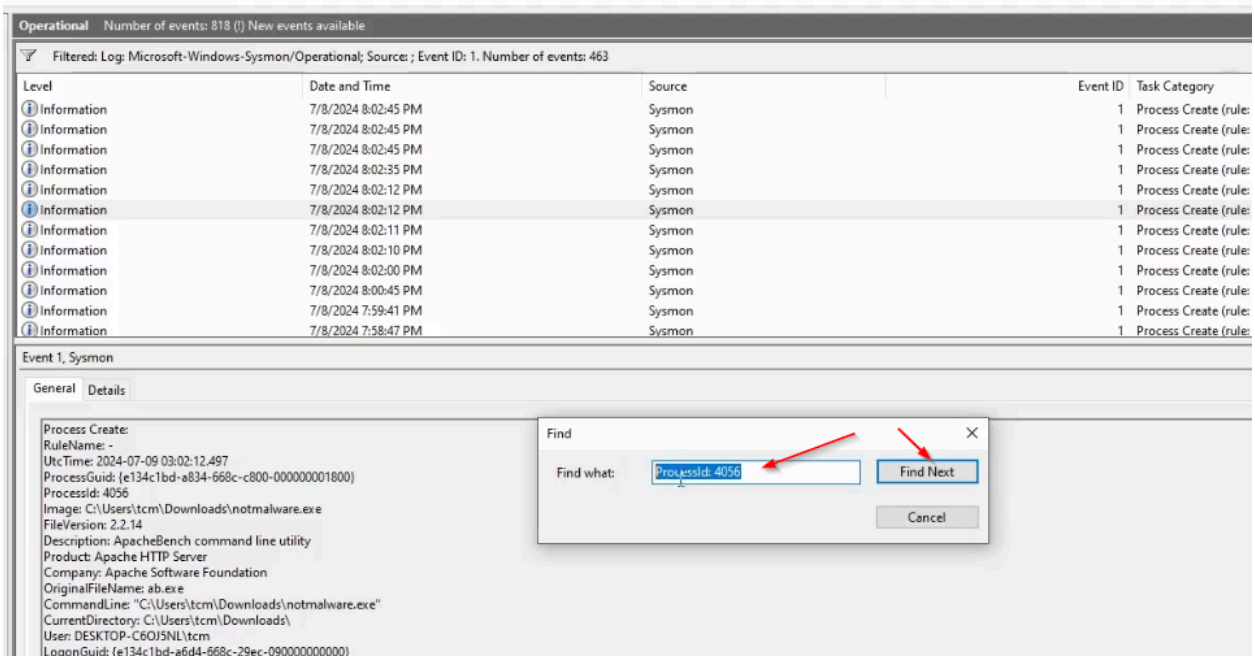
- **Copy PROCESS ID ⇒ 4056**

See my process logs came this place use methodology



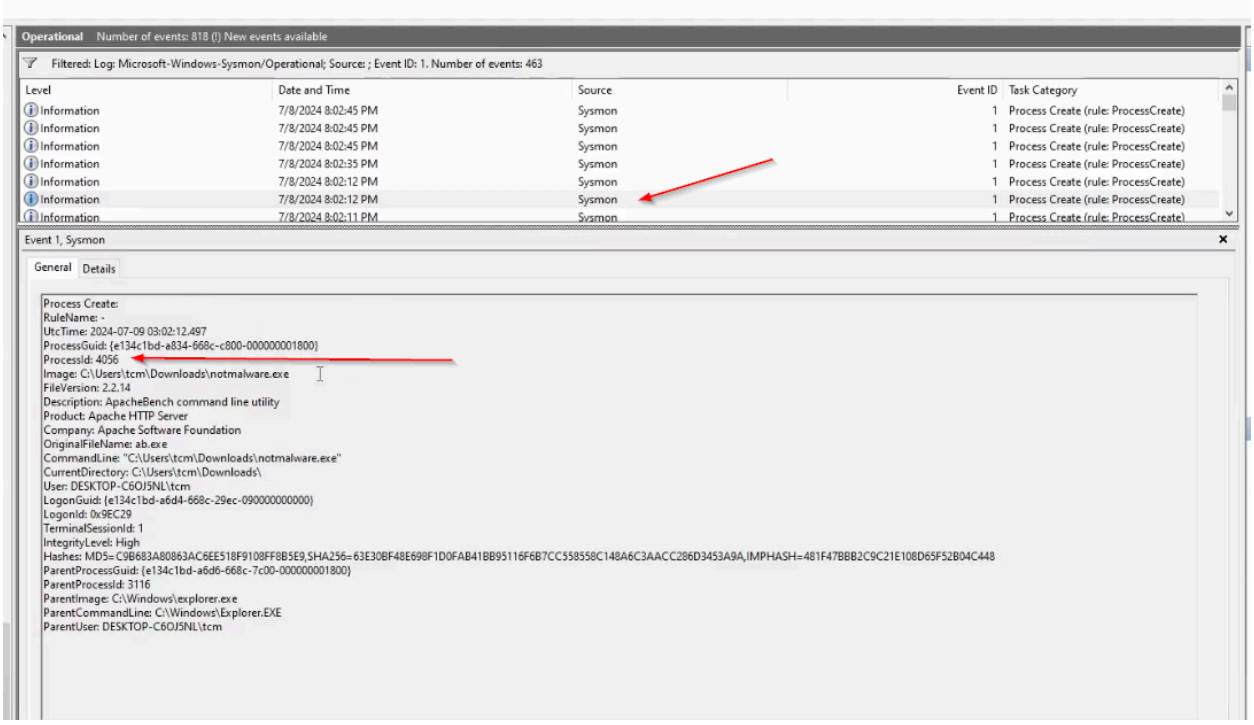
Use find features

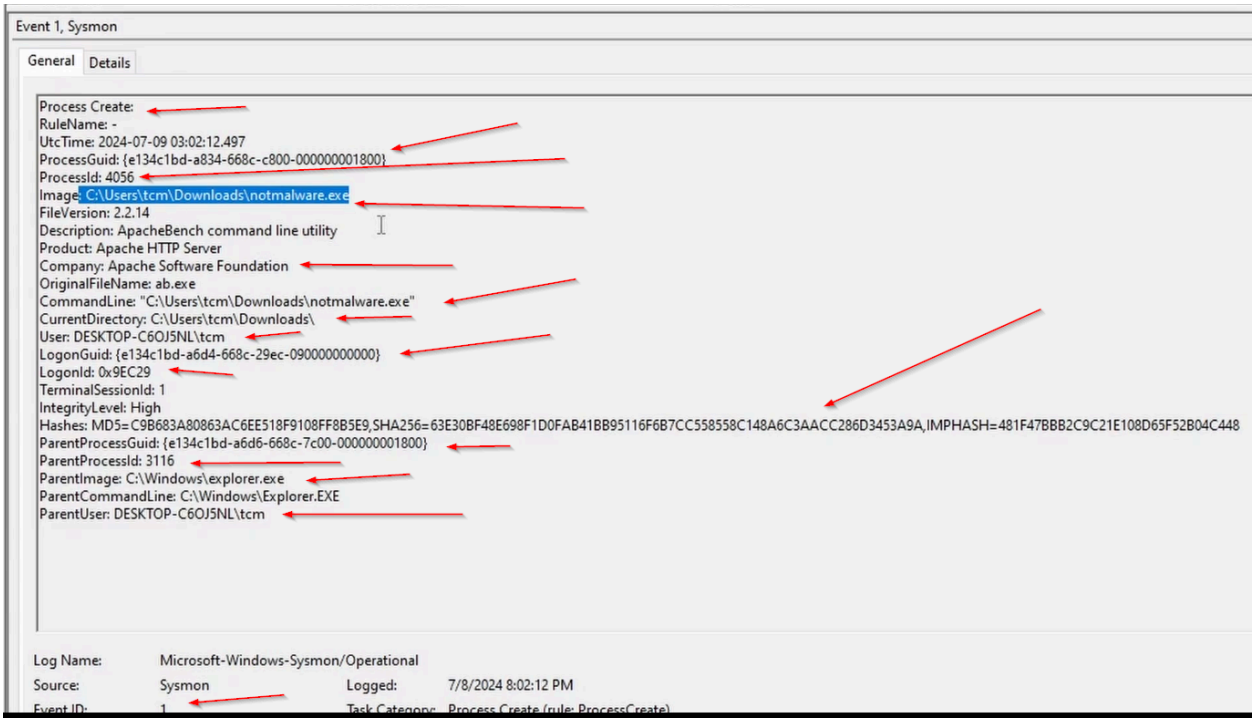




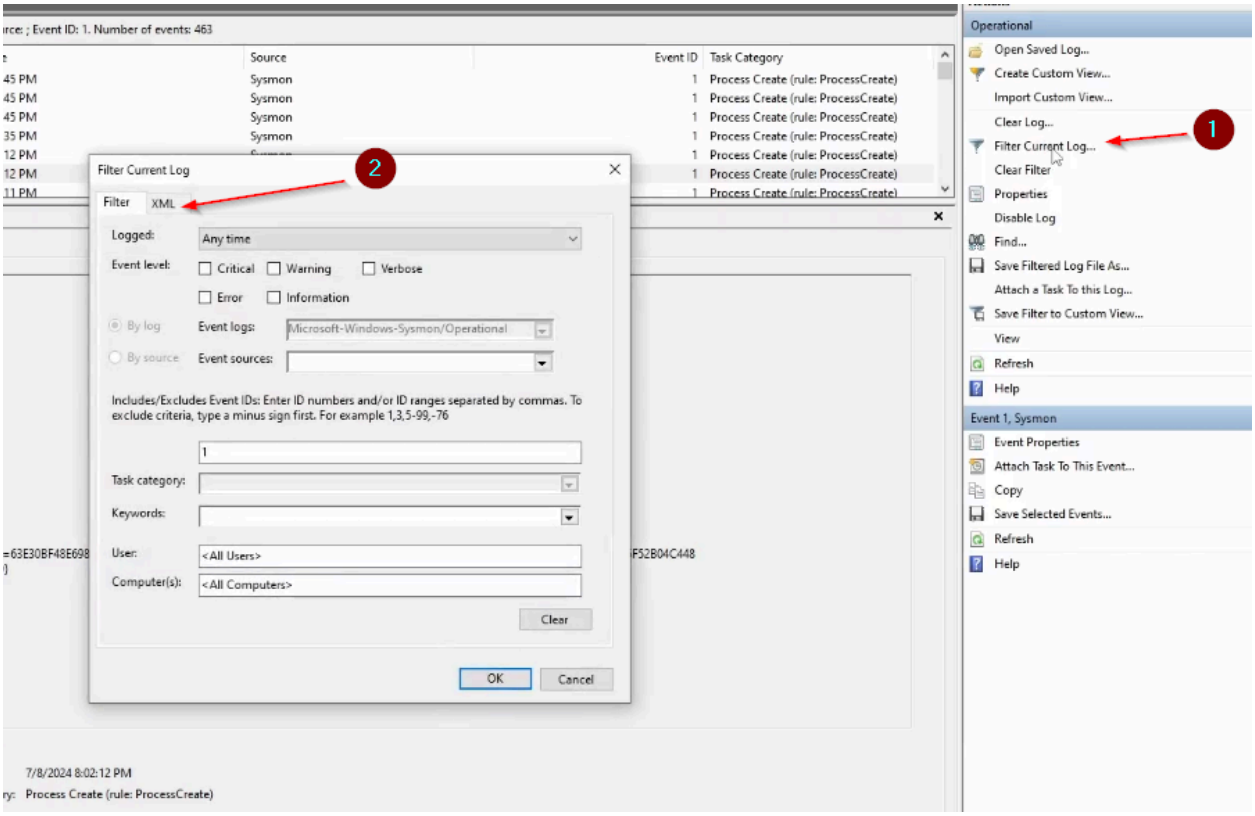
Analysis

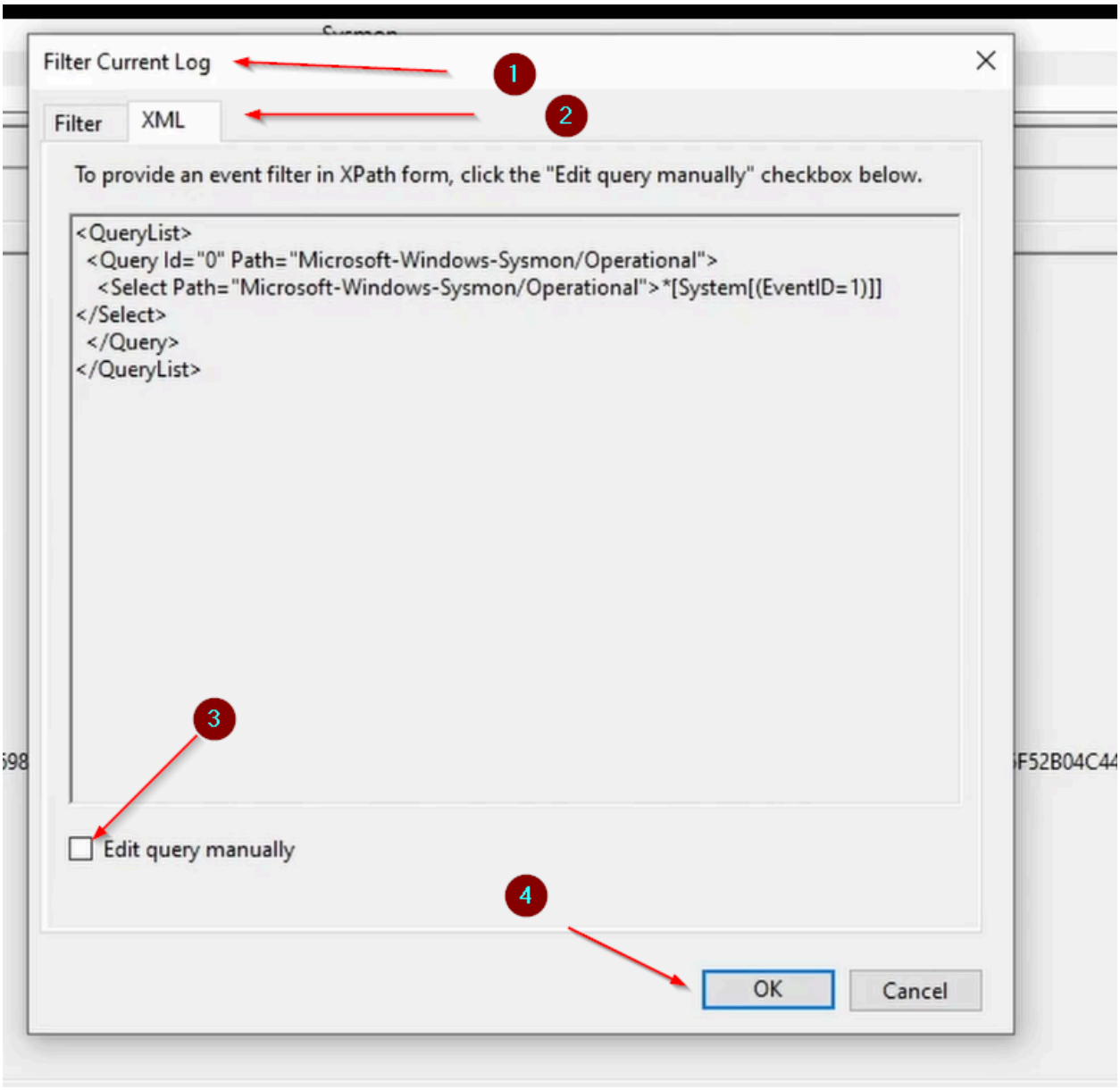
See only extract specific process id


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
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-29ec-090000000000}
LogonId: 0x9EC29
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=C9B683A80863AC6EE518F9108FF8B5E9,SHA256=63E30BF48E698F1D0FAB41BB95116F6B7CC558558C148A6C3AACC286D3453A9A,IMPHASH=481F47BBB2C9C21E108D65F52B04C448
ParentProcessGuid: {e134c1bd-a6d6-668c-7c00-000000001800}
ParentProcessId: 3116
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
ParentUser: DESKTOP-C6OJ5NL\tcm

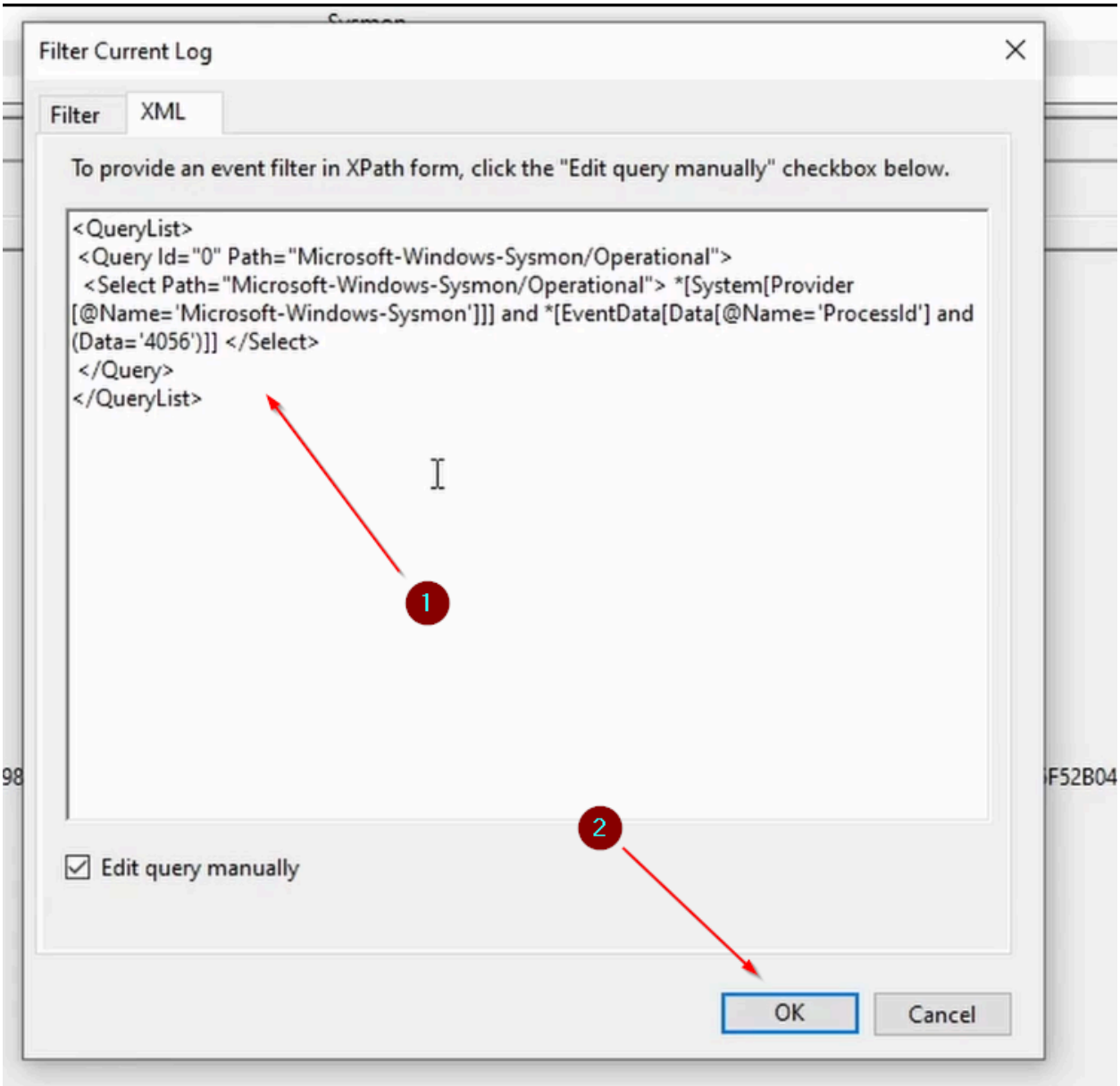

Event 1, Sysmon
General Details
Process Create:
RuleName: -
UtcTime: 2024-07-09 03:02:12.497
ProcessGuid: {e134c1bd-a834-668c-c800-000000001800}
ProcessId: 4056
Image: C:\Users\tcm\Downloads\notmalware.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: 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-29ec-090000000000}
LogonId: 0x9EC29
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=C9B683A80863AC6EE518F9108FF8B5E9,SHA256=63E30BF48E698F1D0FAB41BB95116F6B7CC558558C148A6C3AACC286D3453A9A,IMPHASH=481F47BBB2C9C21E108D65F52B04C448
ParentProcessGuid: {e134c1bd-a6d6-668c-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
Logged: 7/8/2024 8:02:12 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)

More advanced analysis uses XML filter search alter find features:



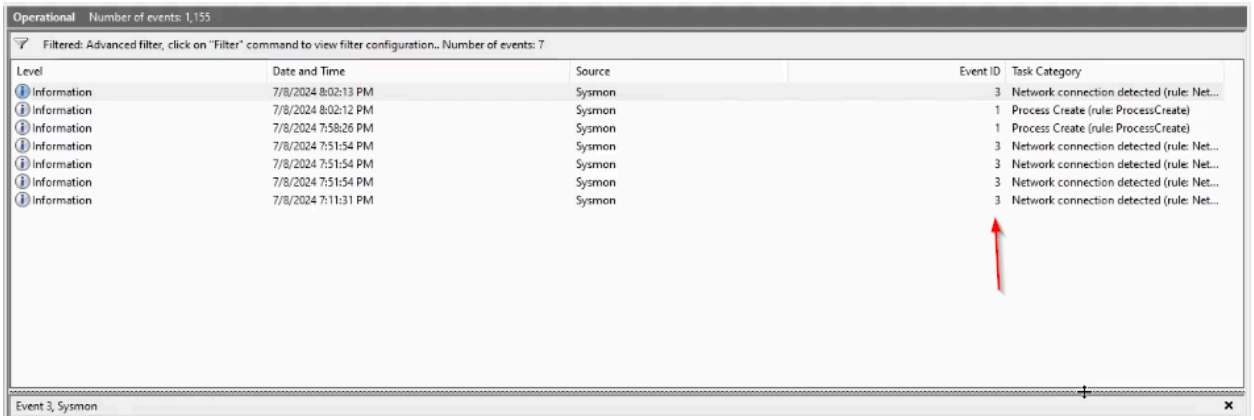


Use advanced search filter XML format query



Result:

⇒ See particular process-related ID execute



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)

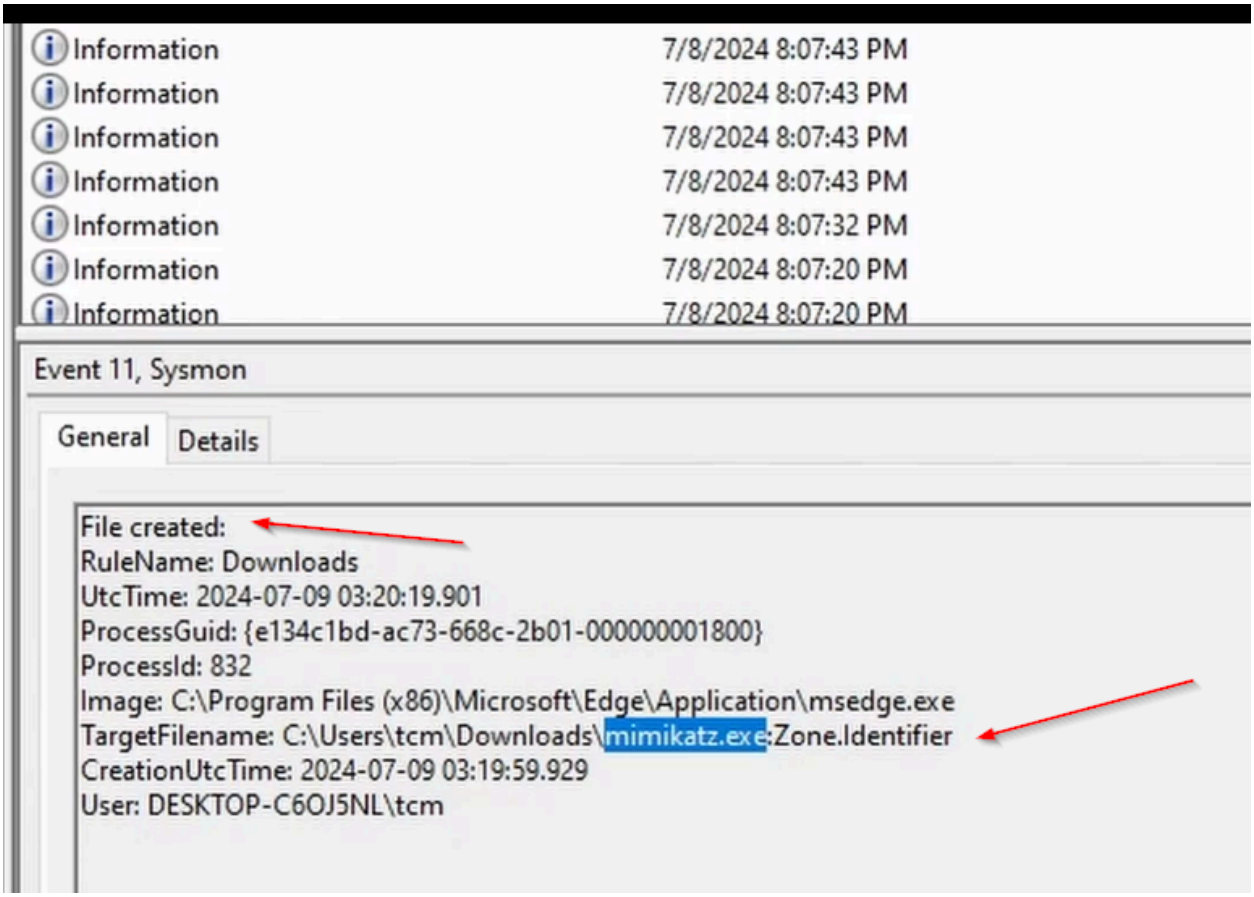
Process terminated:

When the process is terminated, UTC Time is very important

Correlation case process ID and process_GUI is very important

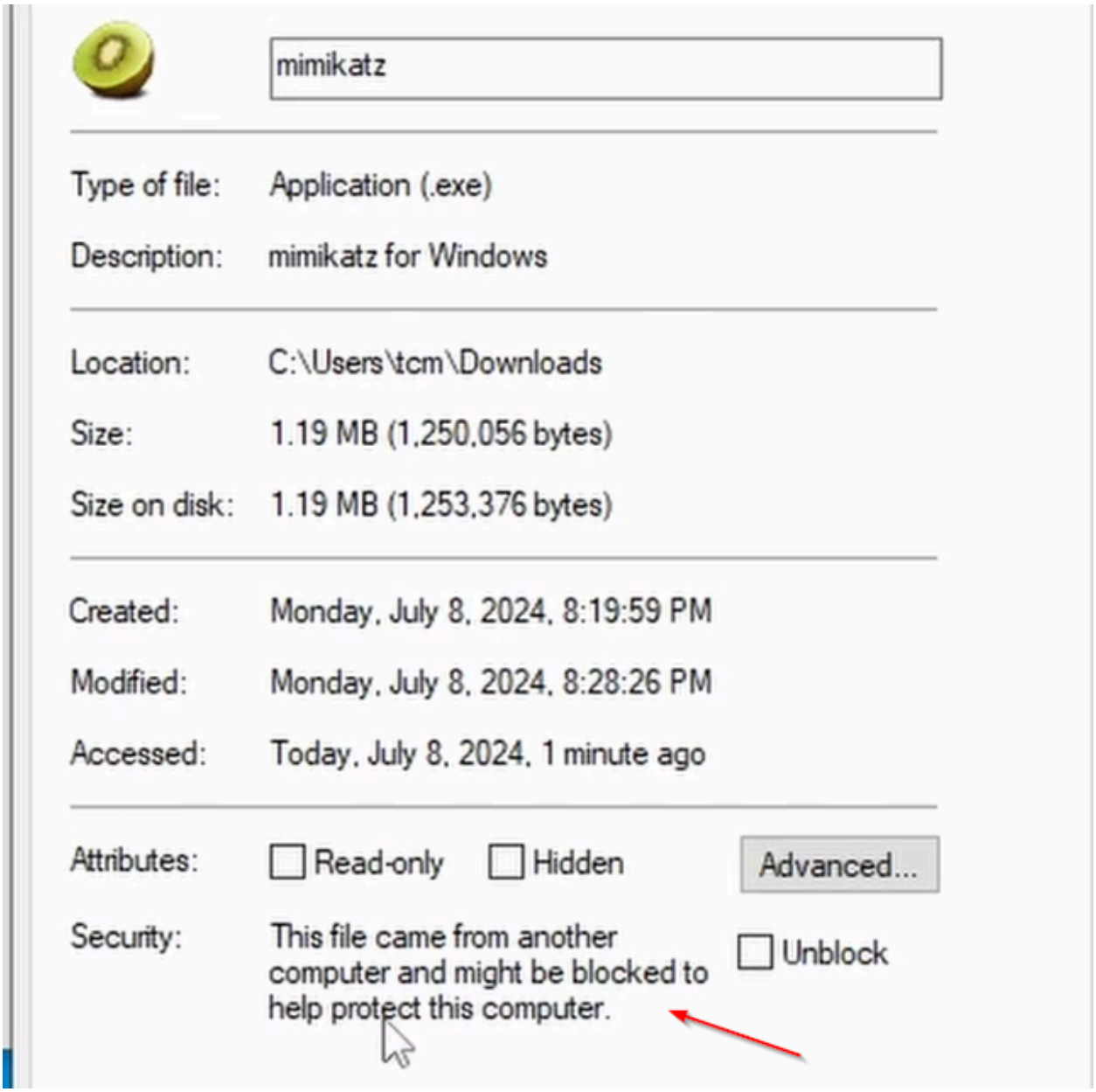
Mark of the web ⇒ MOTW (Use identify, download, potentially indicator, and Windows screen)

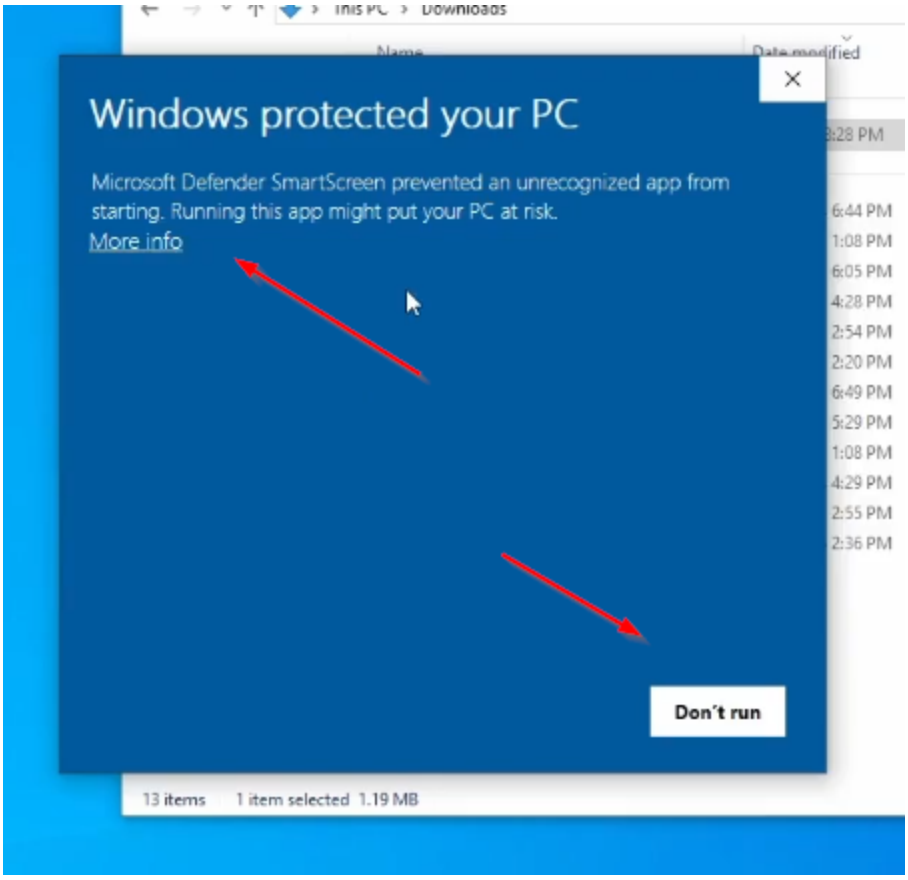
11 file create ⇒ example mimikatz



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

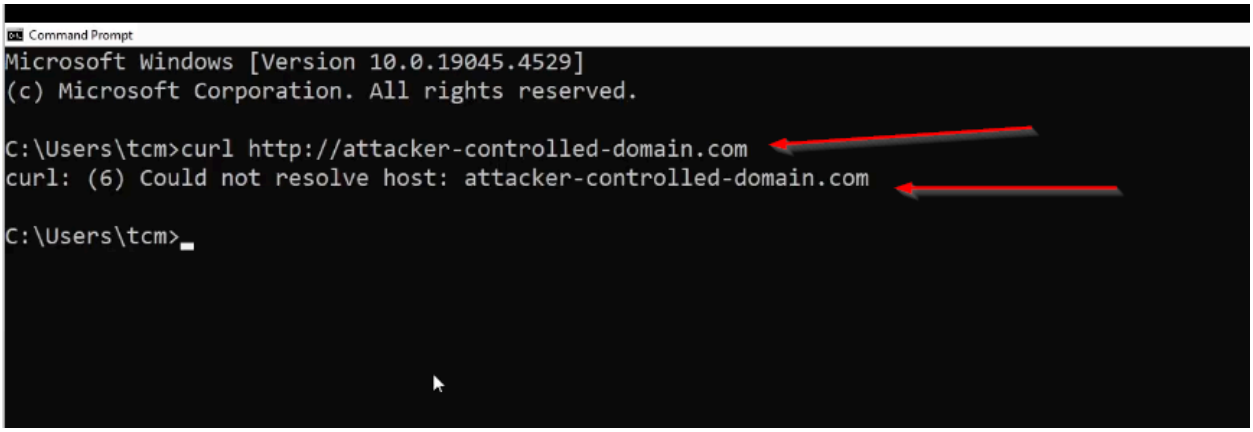
15 file creation stream hash ⇒ This uses find potential file download cases to identify use and Windows screen MOTW (Mark of the Web)


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

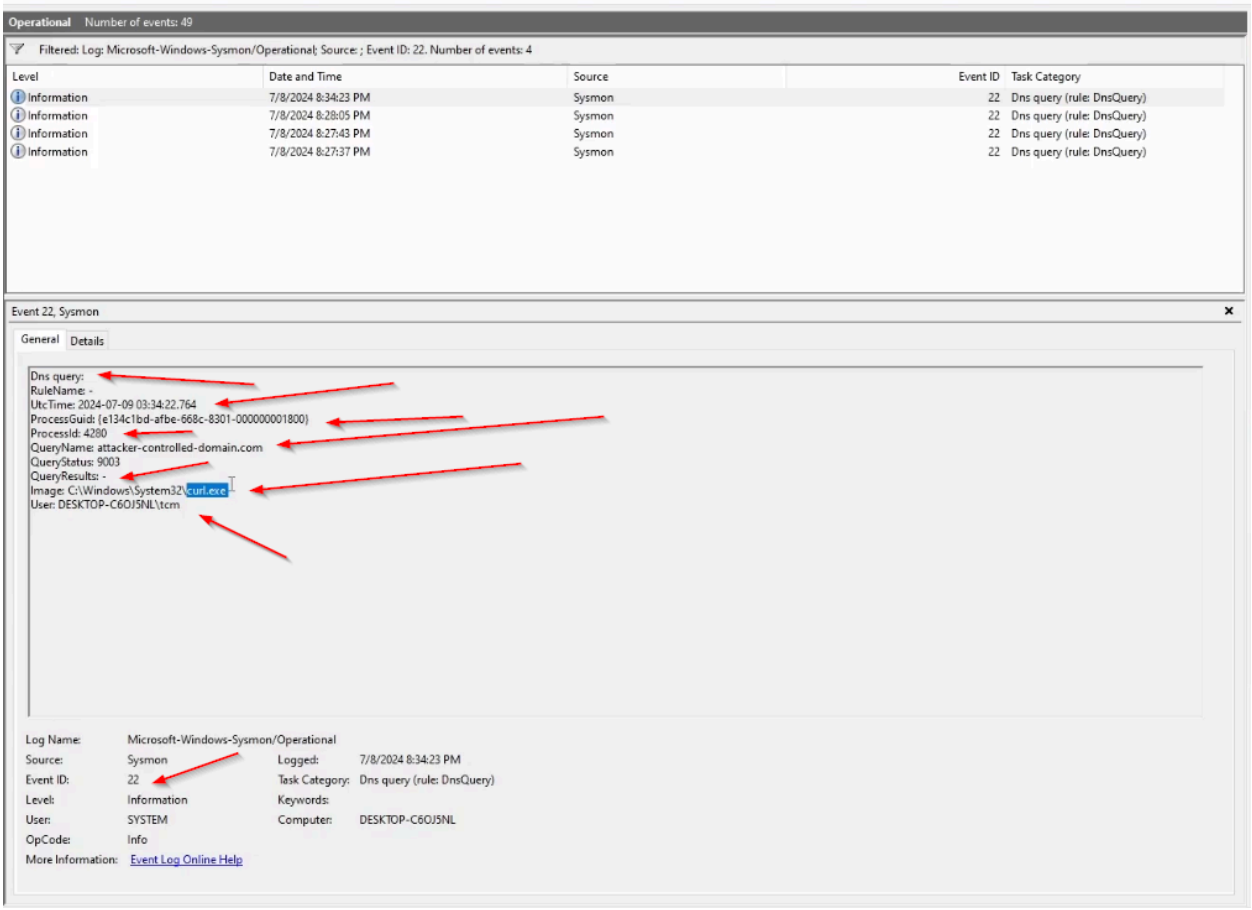

This PC › Downloads
Name
Date modified
Windows protected your PC
Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.
More info
Don't run
13 items
1 item selected 1.19 MB


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=00000000000000000000000000
Contents: [ZoneTransfer] ZoneId=3 HostUrl=https://github.com/
User: DESKTOP-C6OJ5NL\tcm

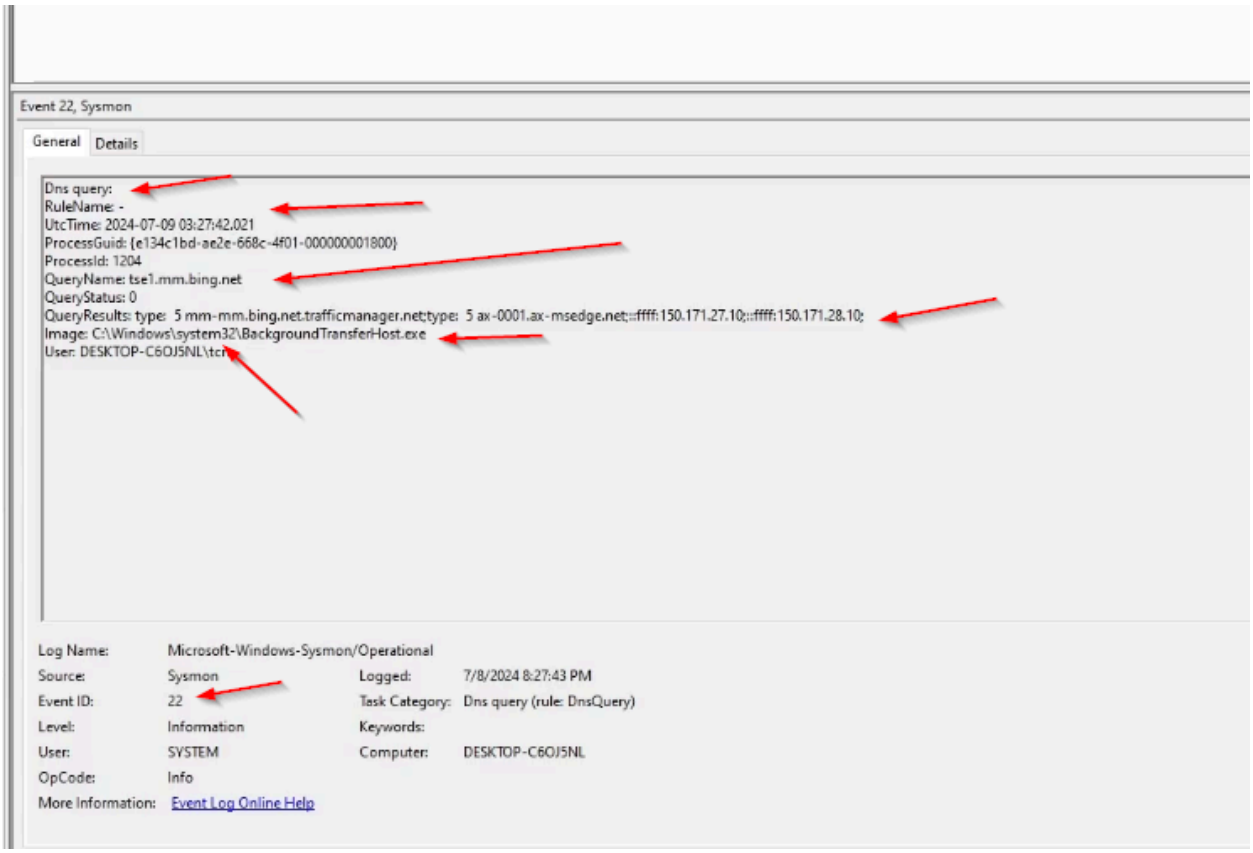
22 DNS events log ⇒ DNS query analysis for malware request case



This image does not contain query results because DNS resolution failed, so not come query results



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



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