HTB- Sherlocks: Unit42 – Level: Very Easy
Amit Persky

Table of Contents

Intro

In this Sherlock, you will familiarize yourself with Sysmon logs and various useful EventIDs for identifying and analyzing malicious activities on a Windows system. Palo Alto's Unit42 recently conducted research on an UltraVNC campaign, wherein attackers utilized a backdoored version of UltraVNC to maintain access to systems. This lab is inspired by that campaign and guides participants through the initial access stage of the campaign.

For this Sherlock I also used Microsoft's website that explains about sysmon Events ID'S, which helped me to understand the tasks that need to be performed in a better way.

You can watch it here:

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

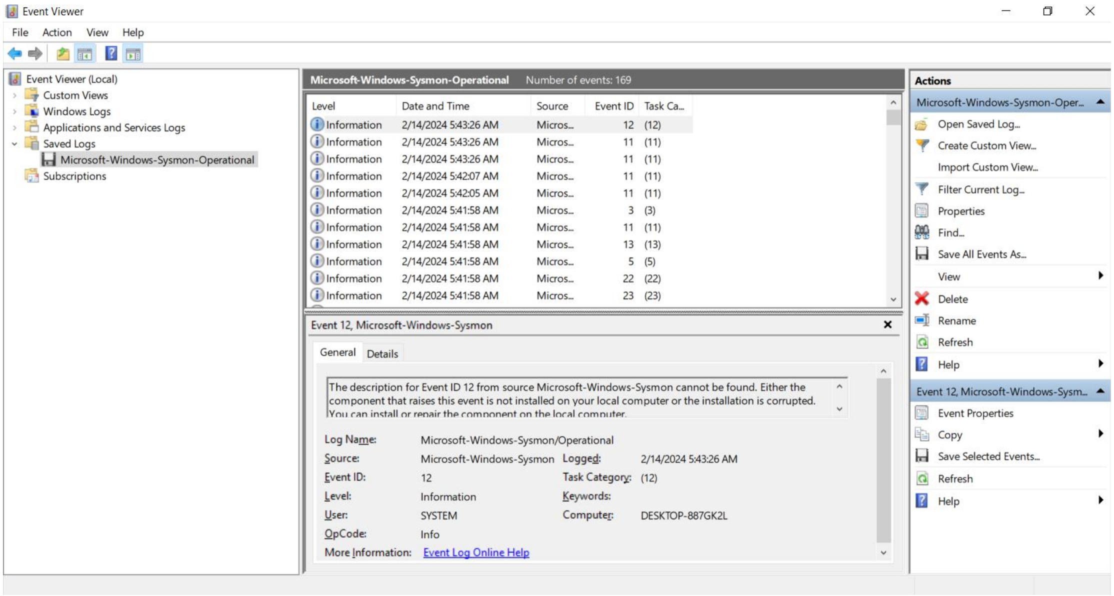
HTB- Sherlocks: Unit42 – Level: Very Easy
Amit Persky

Task 1:

How many Event logs are there with Event ID 11?

Ok so we are got a Windows Event Log file which including sysmon logs.

We are opening the Sysmon log file and we can see that:



Microsoft-Windows-Sysmon-Operational Number of events: 169

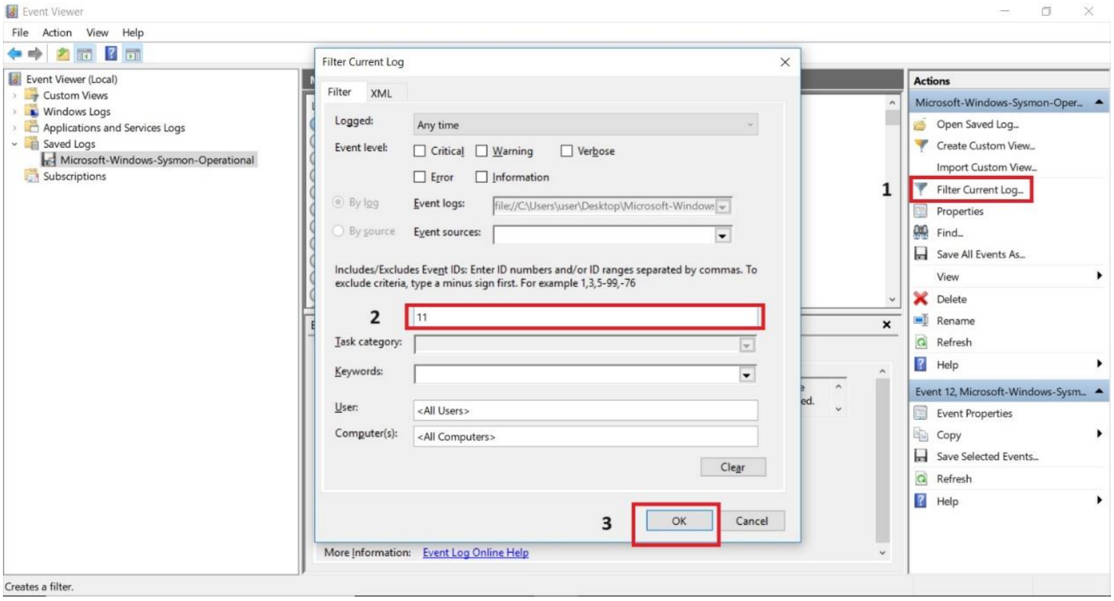
Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:43:26 AM	Micros...	12	(12)
Information	2/14/2024 5:43:26 AM	Micros...	11	(11)
Information	2/14/2024 5:43:26 AM	Micros...	11	(11)
Information	2/14/2024 5:42:07 AM	Micros...	11	(11)
Information	2/14/2024 5:42:05 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	3	(3)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	13	(13)
Information	2/14/2024 5:41:58 AM	Micros...	5	(5)
Information	2/14/2024 5:41:58 AM	Micros...	22	(22)
Information	2/14/2024 5:41:58 AM	Micros...	23	(23)

Event 12, Microsoft-Windows-Sysmon

The description for Event ID 12 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 2/14/2024 5:43:26 AM
Event ID: 12 Task Category: (12)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-887GK2L
OpCode: Info
More Information: Event Log Online Help

So for finding the count of the event ID 11 we need to follow this steps:



Logged: Any time
Event level: □ Critical □ Warning □ Verbose □ Error □ Information
● By log Event logs: file://C:\Users\user\Desktop\Microsoft-Windows
○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

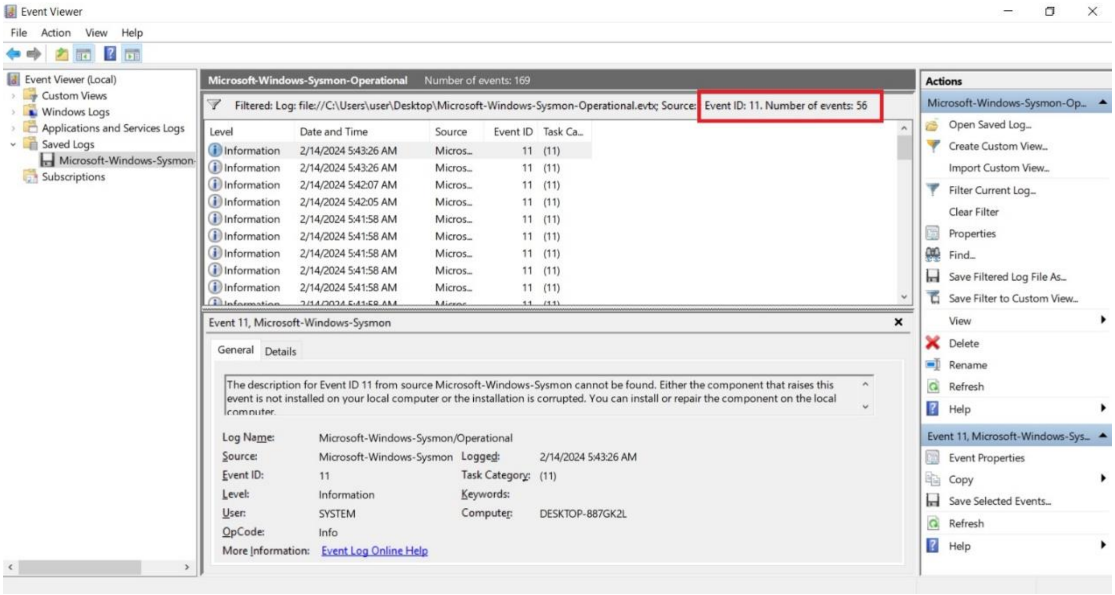
11

Task category:
Keywords:
User: <All Users>
Computer(s): <All Computers>

Creates a filter.

Filter Current Log…> 11 (the event ID we are looking) > ok

And we will find the number..



Microsoft-Windows-Sysmon-Operational Number of events: 169

Filtered: Log: file://C:\Users\user\Desktop\Microsoft-Windows-Sysmon-Operational.evtx; Source: Event ID: 11. Number of events: 56

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:43:26 AM	Micros...	11	(11)
Information	2/14/2024 5:43:26 AM	Micros...	11	(11)
Information	2/14/2024 5:42:07 AM	Micros...	11	(11)
Information	2/14/2024 5:42:05 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)

Event 11, Microsoft-Windows-Sysmon

General Details

The description for Event ID 11 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 2/14/2024 5:43:26 AM
Event ID: 11 Task Category: (11)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-887GK2L
OpCode: Info
More Information: Event Log Online Help

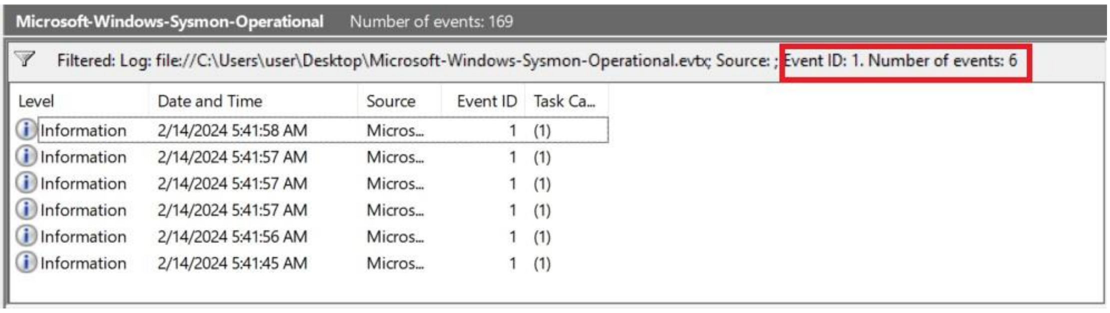
Answer:

56

Task 2 :

Whenever a process is created in memory, an event with Event ID 1 is recorded with details such as command line, hashes, process path, parent process path, etc. This information is very useful for an analyst because it allows us to see all programs executed on a system, which means we can spot any malicious processes being executed. What is the malicious process that infected the victim's system?

Ok so I used the same method from question for filtering Event ID 1 and got 6 results.

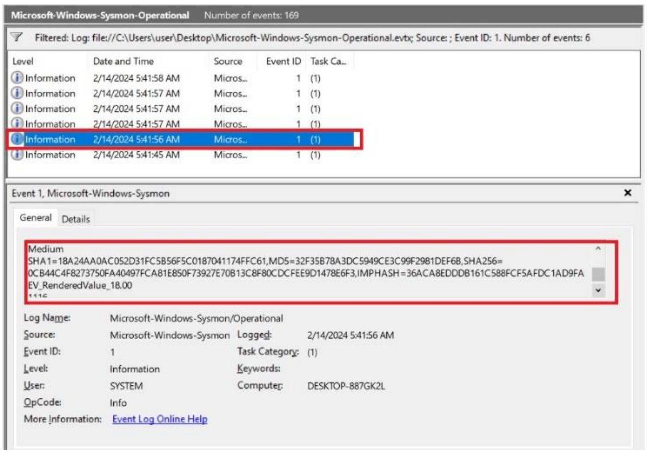

Microsoft-Windows-Sysmon-Operational Number of events: 169

Filtered: Log: file://C:\Users\user\Desktop\Microsoft-Windows-Sysmon-Operational.evtx; Source: ; Event ID: 1. Number of events: 6

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	1	(1)
Information	2/14/2024 5:41:57 AM	Micros...	1	(1)
Information	2/14/2024 5:41:57 AM	Micros...	1	(1)
Information	2/14/2024 5:41:57 AM	Micros...	1	(1)
Information	2/14/2024 5:41:56 AM	Micros...	1	(1)
Information	2/14/2024 5:41:45 AM	Micros...	1	(1)

I thought to my self how to determine which one is malicious?

I decided to check each Hash value virustotal for findings and I got that this one is not ok:

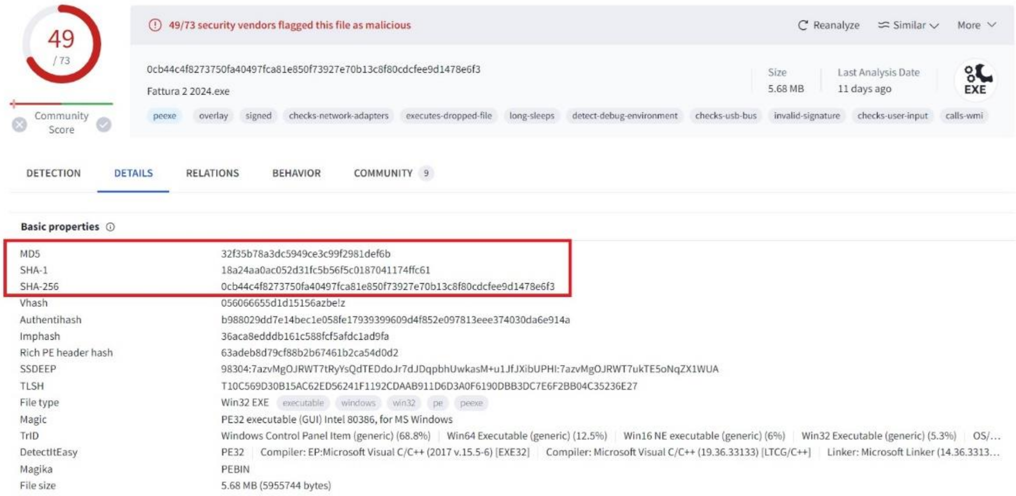


```
Microsoft-Windows-Sysmon-Operational    Number of events: 169
Filtered: Log: file://C:\Users\user\Desktop\Microsoft-Windows-Sysmon-Operational.evtx; Source: ; Event ID: 1. Number of events: 6
Level         Date and Time           Source    Event ID  Task Ca...
Information   2/14/2024 5:41:58 AM    Micros...        1  (1)
Information   2/14/2024 5:41:57 AM    Micros...        1  (1)
Information   2/14/2024 5:41:57 AM    Micros...        1  (1)
Information   2/14/2024 5:41:57 AM    Micros...        1  (1)
Information   2/14/2024 5:41:56 AM    Micros...        1  (1)
Information   2/14/2024 5:41:45 AM    Micros...        1  (1)
```

Event 1, Microsoft-Windows-Sysmon

```
Medium
SHA1=18A24AA0AC052D31FC5B56F5C0187041174FFC61,MD5=32F35B78A3DC5949CE3C99F2981DEF6B,SHA256=
0CB44C4F8273750FA40497FCA81E850F73927E70B13C8F80CDCFEE9D1478E6F3,IMPHASH=36ACA8EDDDB161C588FCF5AFDC1AD9FA
EV_RenderedValue_18.00
```

```
Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Microsoft-Windows-Sysmon  Logged:         2/14/2024 5:41:56 AM
Event ID:          1                         Task Category:  (1)
Level:             Information               Keywords:
User:              SYSTEM                    Computer:       DESKTOP-887GK2L
OpCode:            Info
More Information:  Event Log Online Help
```



49/73 security vendors flagged this file as malicious

0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3

Fattura 2 2024.exe

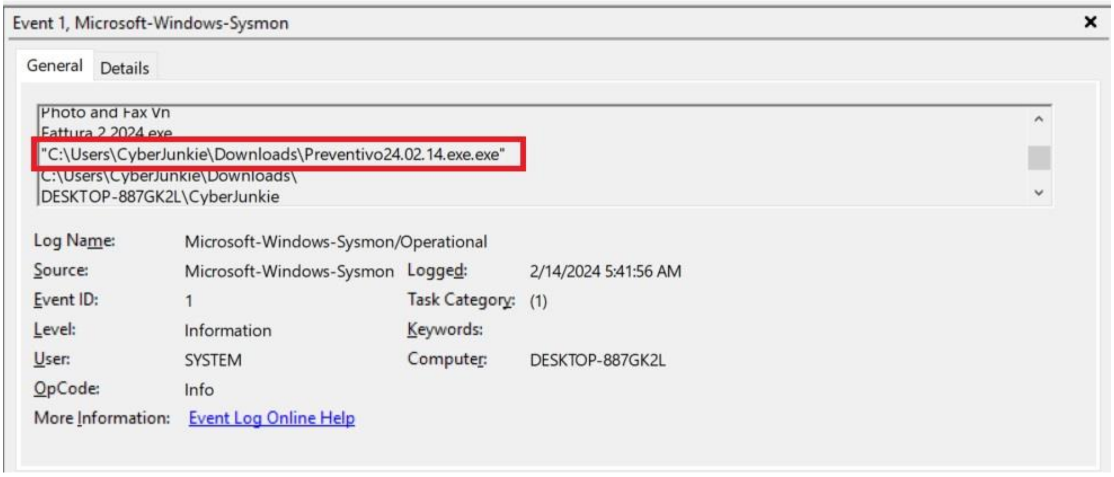
Size 5.68 MB

Last Analysis Date 11 days ago

Basic properties

```
MD5                 32f35b78a3dc5949ce3c99f2981def6b
SHA-1               18a24aa0ac052d31fc5b56f5c0187041174ffc61
SHA-256             0cb44c4f8273750fa40497fca81e850f73927e70b13c8f80cdcfee9d1478e6f3
Vhash               056066655d1d15156azbe!z
Authentihash        b988029dd7e14bec1e058fe17939399609d4f852e097813eee374030da6e914a
Imphash             36aca8edddb161c588fcf5afdc1ad9fa
Rich PE header hash 63adeb8d79cf88b2b67461b2ca54d0d2
SSDEEP              98304:7azvMgOJRWT7tRyYsQdTEDdoJr7dJDqpbhUwkasM+u1JfJXibUPHI:7azvMgOJRWT7ukTE5oNqZX1WUA
TLSH                T10C569D30B15AC62ED56241F1192CDAAB911D6D3A0F6190DBB3DC7E6F2BB04C35236E27
File type           Win32 EXE  executable  windows  win32  pe  peexe
Magic               PE32 executable (GUI) Intel 80386, for MS Windows
TrID                Windows Control Panel Item (generic) (68.8%) | Win64 Executable (generic) (12.5%) | Win16 NE executable (generic) (6%) | Win32 Executable (generic) (5.3%) | OS/...
DetectItEasy        PE32 | Compiler: EP:Microsoft Visual C/C++ (2017 v.15.5-6) [EXE32] | Compiler: Microsoft Visual C/C++ (19.36.33133) [LTCG/C++] | Linker: Microsoft Linker (14.36.3313...
Magika              PEBIN
File size           5.68 MB (5955744 bytes)
```

This one was the only one with some findings so I inspected him more:



Event 1, Microsoft-Windows-Sysmon

```
Photo and Fax Vn
Fattura 2 2024.exe
"C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe"
C:\Users\CyberJunkie\Downloads\
DESKTOP-887GK2L\CyberJunkie
```

```
Log Name:          Microsoft-Windows-Sysmon/Operational
Source:            Microsoft-Windows-Sysmon  Logged:         2/14/2024 5:41:56 AM
Event ID:          1                         Task Category:  (1)
Level:             Information               Keywords:
User:              SYSTEM                    Computer:       DESKTOP-887GK2L
OpCode:            Info
More Information:  Event Log Online Help
```

And this is what we looked for. This is the malicious processes being executed. We can observe and see that he had double "exe" and its not normal.

Answer:

C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe

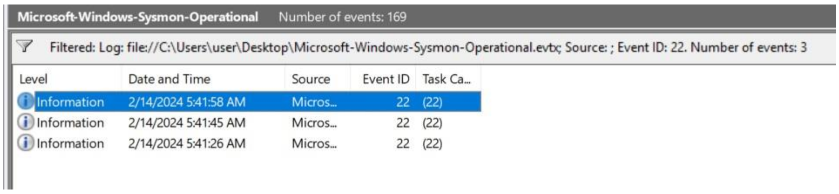
<u>Task 3:</u>

<u>Which Cloud drive was used to distribute the malware?</u>

so I checked the hint of HTB for help:

<u>Event ID 22 can be used to look for any DNS Queries made by the system. Do not filter for any specific event ID; start analyzing the events from the oldest available event. If you see events related to the malicious file being created, look for an Event ID 22 event surrounding that event.</u>

So I filtered event ID 22

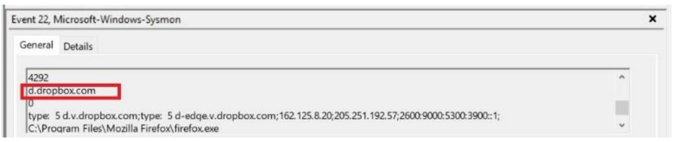


Microsoft-Windows-Sysmon-Operational Number of events: 169

Filtered: Log: file://C:\Users\user\Desktop\Microsoft-Windows-Sysmon-Operational.evtx; Source: ; Event ID: 22. Number of events: 3

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	22	(22)
Information	2/14/2024 5:41:45 AM	Micros...	22	(22)
Information	2/14/2024 5:41:26 AM	Micros...	22	(22)

I inspected inside and saw this:



Event 22, Microsoft-Windows-Sysmon

```
4292
d.dropbox.com
0
type:  5 d.v.dropbox.com;type:  5 d-edge.v.dropbox.com;162.125.8.20;205.251.192.57;2600:9000:5300:3900::1;
C:\Program Files\Mozilla Firefox\firefox.exe
```

We can conclude from this that dropbox is the cloud service that was involved in spreading the malware.

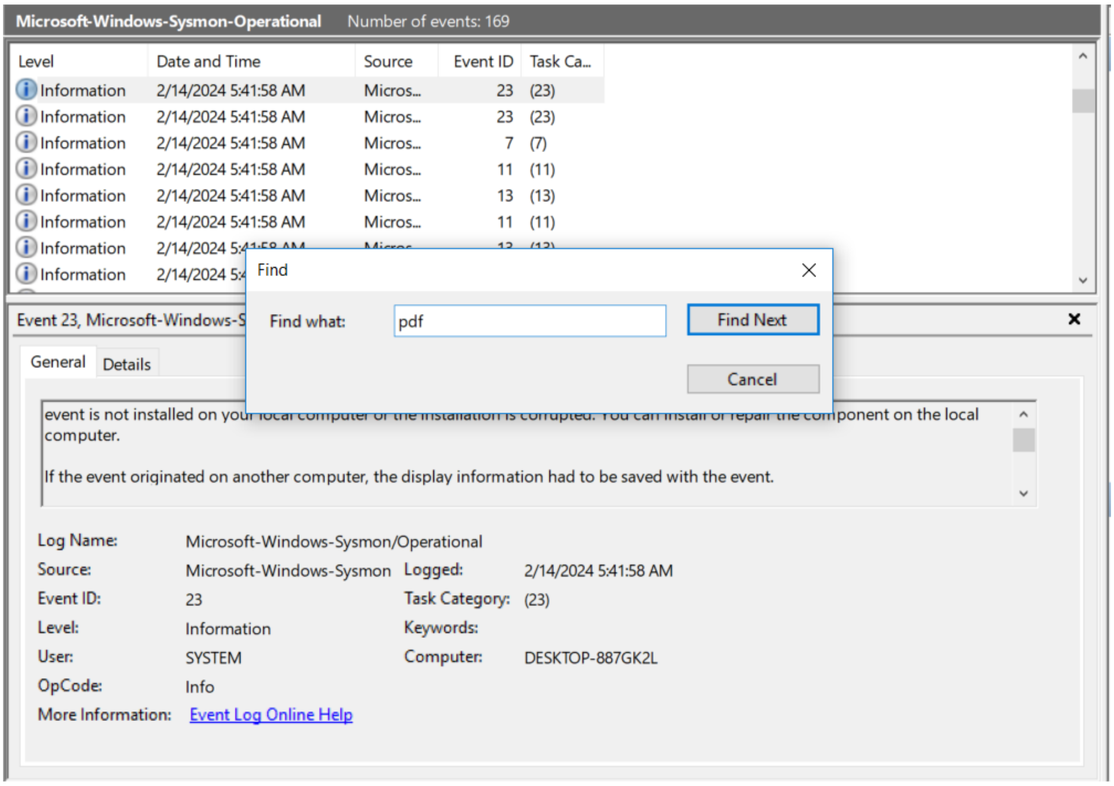
Answer:

dropbox

Task 4:

The initial malicious file time-stamped (a defense evasion technique, where the file creation date is changed to make it appear old) many files it created on disk. What was the timestamp changed to for a PDF file?

So I searched "pdf" in the search :



Microsoft-Windows-Sysmon-Operational Number of events: 169

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	23	(23)
Information	2/14/2024 5:41:58 AM	Micros...	23	(23)
Information	2/14/2024 5:41:58 AM	Micros...	7	(7)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	13	(13)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	13	(13)
Information	2/14/2024 5:			

Event 23, Microsoft-Windows-S

Find what: pdf

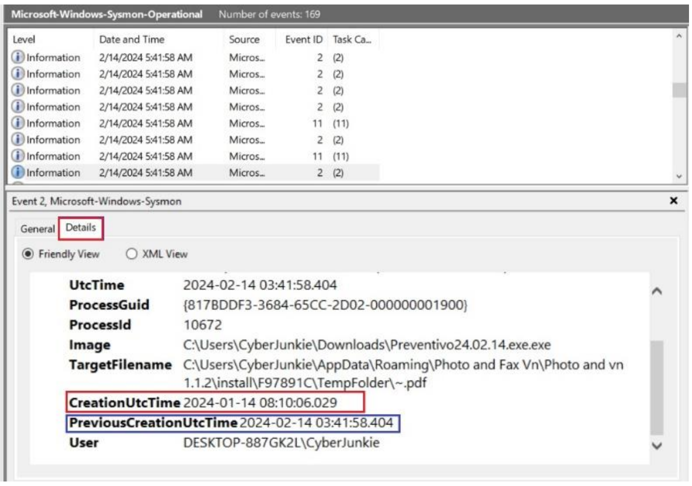
event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon
Logged: 2/14/2024 5:41:58 AM
Event ID: 23
Task Category: (23)
Level: Information
Keywords:
User: SYSTEM
Computer: DESKTOP-887GK2L
OpCode: Info
More Information: Event Log Online Help

I found 2 files that is contain pdf.

I inspected this two file more closely in the details tab and saw this on one of them:



Microsoft-Windows-Sysmon-Operational Number of events: 169

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	2	(2)
Information	2/14/2024 5:41:58 AM	Micros...	2	(2)
Information	2/14/2024 5:41:58 AM	Micros...	2	(2)
Information	2/14/2024 5:41:58 AM	Micros...	2	(2)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	2	(2)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	2	(2)

Event 2, Microsoft-Windows-Sysmon

● Friendly View ○ XML View

```
UtcTime               2024-02-14 03:41:58.404
ProcessGuid           {817BDDF3-3684-65CC-2D02-000000001900}
ProcessId             10672
Image                 C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
TargetFilename        C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn
                      1.1.2\install\F97891C\TempFolder\~.pdf
CreationUtcTime       2024-01-14 08:10:06.029
PreviousCreationUtcTime 2024-02-14 03:41:58.404
User                  DESKTOP-887GK2L\CyberJunkie
```

We can see that one of them had another time of creation. Previouscreationutctime. Its mean that the timestep changed. So we can be sure this is the file we are talking about. We can see now the CreationUtcTime that the file is now and this is what we looked.

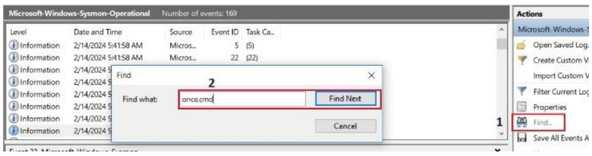
Answer:

2024-01-14 08:10:06

Task 5:

The malicious file dropped a few files on disk. Where was "once.cmd" created on disk? Please answer with the full path along with the filename.

To answer on this question I searched "once.cmd" in the find:



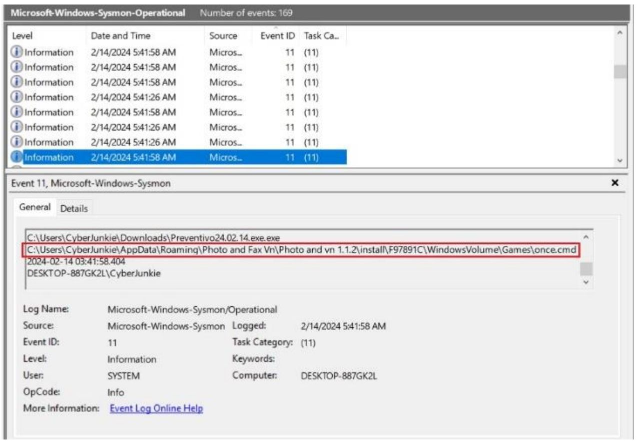
Microsoft-Windows-Sysmon-Operational Number of events: 169

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	5	(5)
Information	2/14/2024 5:41:58 AM	Micros...	22	(22)
Information	2/14/2024 5			
Information	2/14/2024 5			
Information	2/14/2024 5			
Information	2/14/2024 5			
Information	2/14/2024 5			
Information	2/14/2024 5			

Find

Find what: once.cmd

After that I sorted the events by Event ID and searched for Event ID 11 for files created (tnx to the hint)



Microsoft-Windows-Sysmon-Operational Number of events: 169

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:26 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)
Information	2/14/2024 5:41:26 AM	Micros...	11	(11)
Information	2/14/2024 5:41:26 AM	Micros...	11	(11)
Information	2/14/2024 5:41:58 AM	Micros...	11	(11)

Event 11, Microsoft-Windows-Sysmon

```
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd
2024-02-14 03:41:58.404
DESKTOP-887GK2L\CyberJunkie
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Microsoft-Windows-Sysmon Logged: 2/14/2024 5:41:58 AM
Event ID: 11 Task Category: (11)
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-887GK2L
OpCode: Info
More Information: Event Log Online Help

As we can see I found the full path to once.cmd

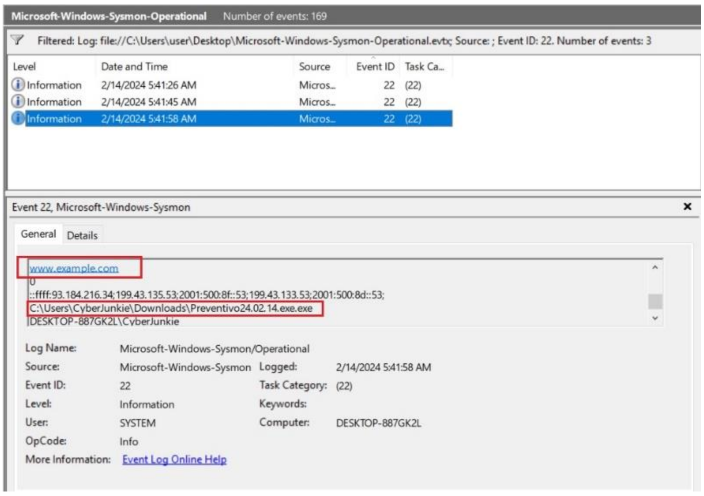
Answer:

C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd

Task 6:

The malicious file attempted to reach a dummy domain, most likely to check the internet connection status. What domain name did it try to connect to?

to answer this question I checked and got the info the Event ID 22 represent the DNS query so I filtered by Event ID 22, found 3 events and I looked on their inside. One of them show you this:



Microsoft-Windows-Sysmon-Operational   Number of events: 169

Filtered: Log: file://C:\Users\user\Desktop\Microsoft-Windows-Sysmon-Operational.evtx; Source: ; Event ID: 22. Number of events: 3

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:26 AM	Micros...	22	(22)
Information	2/14/2024 5:41:45 AM	Micros...	22	(22)
Information	2/14/2024 5:41:58 AM	Micros...	22	(22)

Event 22, Microsoft-Windows-Sysmon

```
www.example.com
0
::ffff:93.184.216.34;199.43.135.53;2001:500:8f::53;199.43.133.53;2001:500:8d::53;
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Microsoft-Windows-Sysmon	Logged:	2/14/2024 5:41:58 AM
Event ID:	22	Task Category:	(22)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-887GK2L
OpCode:	Info		
More Information:	Event Log Online Help		

As we can see, there is a valid domain here, and we can see also the malicious file that we know from before.

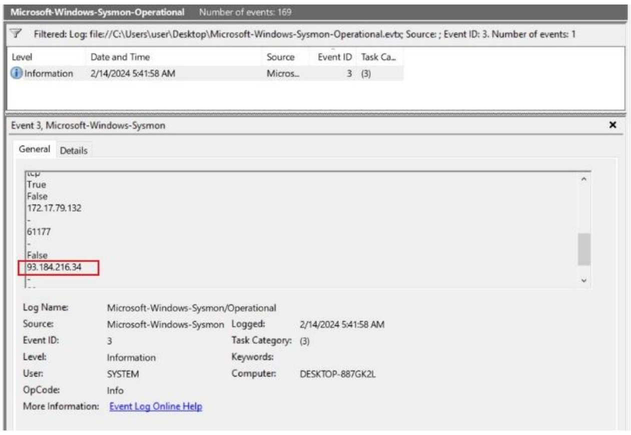
Answer:

www.example.com

Task 7:

Which IP address did the malicious process try to reach out to?

for that question I knew that If a process tried to reach a network connection, it means Event ID 3 (you can verify on the Microsoft web). I filtered Event ID 3 to see only 1 event:



Microsoft-Windows-Sysmon-Operational   Number of events: 169

Filtered: Log: file://C:\Users\user\Desktop\Microsoft-Windows-Sysmon-Operational.evtx; Source: ; Event ID: 3. Number of events: 1

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	3	(3)

Event 3, Microsoft-Windows-Sysmon

```
tcp
True
False
172.17.79.132
-
61177
-
False
93.184.216.34
-
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Microsoft-Windows-Sysmon	Logged:	2/14/2024 5:41:58 AM
Event ID:	3	Task Category:	(3)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-887GK2L
OpCode:	Info		
More Information:	Event Log Online Help		

As you can see there is 2 IP'S I tried them both and the last one is the answer.

Answer:

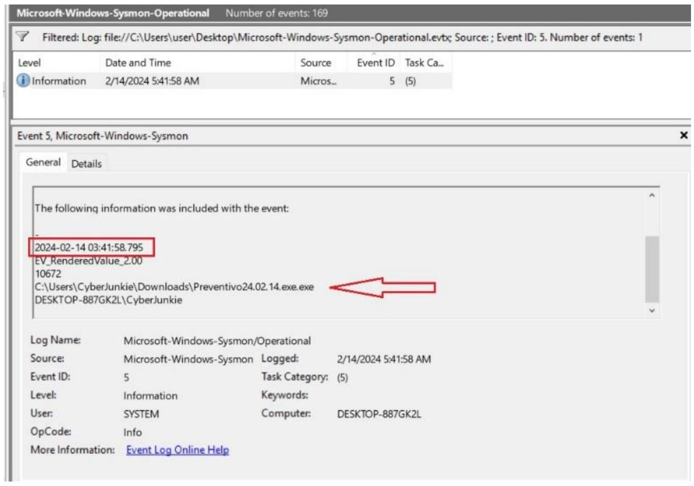
93.184.216.34

Task 8:

The malicious process terminated itself after infecting the PC with a backdoored variant of UltraVNC. When did the process terminate itself?

Ok so for this question I looked at the hint and it says "go for Event ID 5"

I looked more on Microsoft web and I understood that this is Event when process terminates. I filtered Event ID 5:



Microsoft-Windows-Sysmon-Operational Number of events: 169

Filtered: Log: file://C:\Users\user\Desktop\Microsoft-Windows-Sysmon-Operational.evtx; Source: ; Event ID: 5. Number of events: 1

Level	Date and Time	Source	Event ID	Task Ca...
Information	2/14/2024 5:41:58 AM	Micros...	5	(5)

Event 5, Microsoft-Windows-Sysmon

```
The following information was included with the event:

-
2024-02-14 03:41:58.795
EV_RenderedValue_2.00
10672
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Microsoft-Windows-Sysmon	Logged:	2/14/2024 5:41:58 AM
Event ID:	5	Task Category:	(5)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-887GK2L
OpCode:	Info		
More Information:	Event Log Online Help		

As we can see there is one event here with time stamp, and we can see that he is related to our malicious process.

Answer:

2024-02-14 03:41:58