TryHackMe: Retracted

The following is a writeup for the new Retracted room hosted on TryHackMe. This room involved using Sysmon logs to investigate a ransomware infection on a machine. You could use cmdlets like Get-WinEvent, although I only used the Event Viewer. It was an enjoyable room and really helped me improve my skills regarding Windows event logs.

Scenario: "So I downloaded and ran an installer for an antivirus program I needed. After a while, I noticed I could no longer open any of my files. And then I saw that my wallpaper was different and contained a terrifying message telling me to pay if I wanted to get my files back. I panicked and got out of the room to call you. But when I came back, everything was back to normal. Except for one message telling me to check my Bitcoin wallet. But I don't even know what a Bitcoin is! Can you help me check if my computer is now fime?"

What is the full path of the text file containing the "message"?

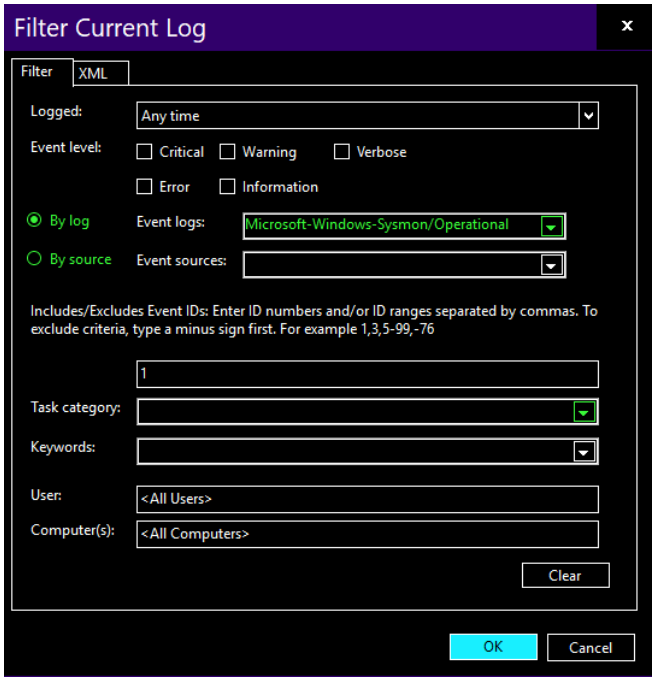
The full path of the text file containing the message is: C:\Users\Sophie\Desktop\SOPHIE.txt.

What program was used to create the text file?

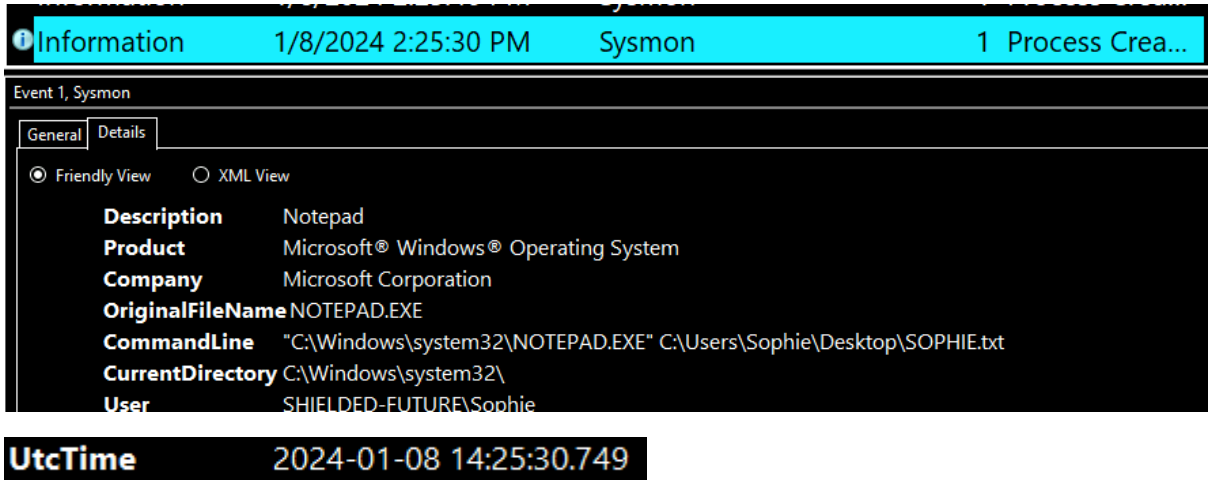
The text file automatically open with notepad.exe which hints at notepad being the program used to create the file.

What is the time of execution of the process that created the text file?

To find the time of execution for when notepad.exe created the file, we first need to open up event viewer. This can be done many ways, I did it by right-clicking the Windows icon on the task bar and selecting event viewer. Then navigate to the Sysmon logs which are located at Applications and Services Logs -> Microsoft -> Windows -> Sysmon -> Operational. You can then filter for the event id 1 which is for process creation:



Once doing so, you can use the find option to search for notepad.exe, the first log found with the string "notepad" is where you can find the answer:



What is the filename of this "installer"? (including the file extension)

In the scenario, we are told that the person tried to download an antivirus, so I simply used the find function to search for "antivirus":

+ System	
- EventData	
RuleName	-
UtcTime	2024-01-08 14:15:00.688
ProcessGuid	{c5d2b969-0364-659c-d500-000000002701}
ProcessId	5992
Image	C:\Users\Sophie\download\antivirus.exe
FileVersion	-
Description	-
Product	-
Company	-
OriginalFileName	-
CommandLine	"C:\Users\Sophie\download\antivirus.exe"
CurrentDirectory	C:\Users\Sophie\download\
User	SHIELDED-FUTURE\Sophie

What is the download location of this installer?

You can see the download location in the image seen below, it is next to the command line and current directory field:

CommandLine	"C:\Users\Sophie\download\antivirus.exe"
CurrentDirectory	C:\Users\Sophie\download\

Note, the answer is not the location including the filename, so use the value for the CurrentDirectory field.

The installer encrypts files and then adds a file extension to the end of the file name. What is this file extension.

To find the new file extension, we can look for Sysmon event ID 11 which is FileCreate. Unbeknownst to myself, the FileCreate event actually logs when a file is overwritten and not just created. If you filter for event ID 11 and use the find function to search for 'antivirus.exe', we can quickly see that the antivirus.exe image keeps editing files that end with .dmp:

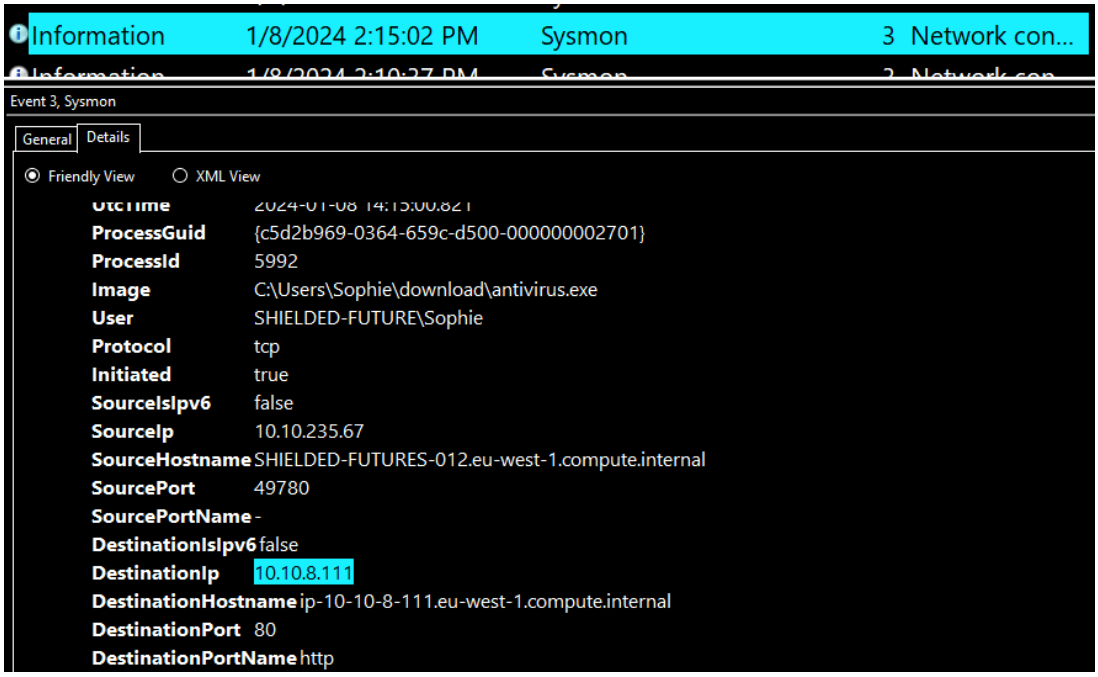
Image	C:\Users\Sophie\download\antivirus.exe
TargetFilename	C:\Users\Sophie\Desktop\Newsletter_JAN2024 - Copy.pptx.dmp

Image	C:\Users\Sophie\download\antivirus.exe
TargetFilename	C:\Users\Sophie\Desktop\Newsletter_DEC2023.pptx.dmp

It becomes clear that the answer is .dmp.

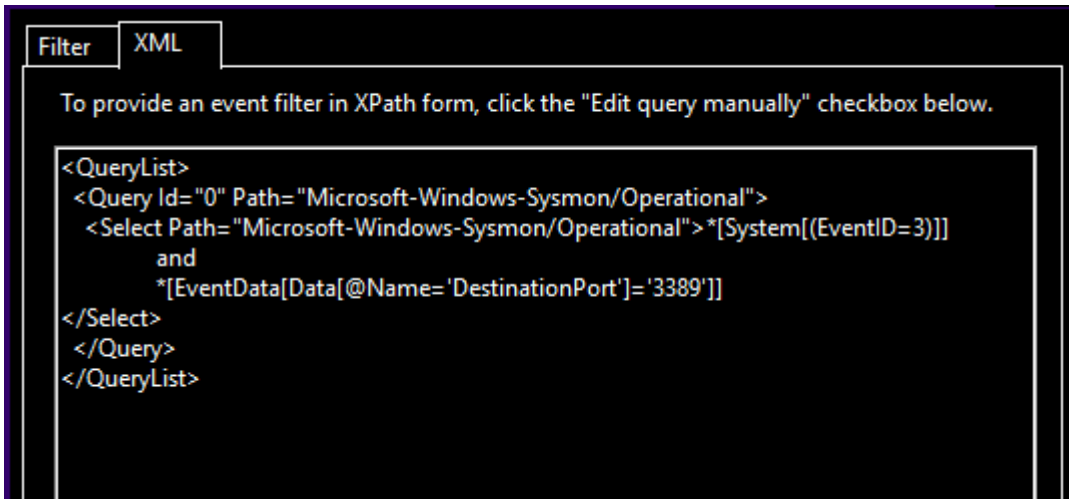
The installer reached out to an IP. What is this IP?

Event ID 3 logs all TCP/UDP connections on a machine. If you filter for event ID 3 and search for the malicious binary we identified, you can find the IP it reached out to in the DestinationIp field:



The threat actor logged in via RDP right after the installer was downloaded. What is the source IP?

To find RDP network connections, we can filter for event ID 3 and for the destination port 3389 which is the default RDP destination port:

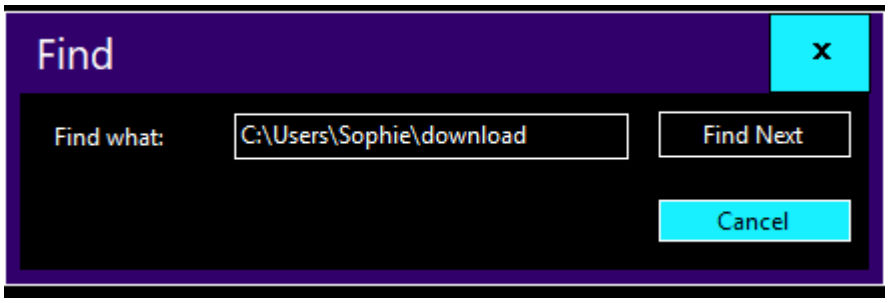


Once you click okay, you should look for logs after the malicious binary was downloaded, from there, we can see the source IP:

RuleName	RDP
UtcTime	2024-07-29 12:47:33.582
ProcessGuid	{c5d2b969-8e98-66a7-1400-000000002a01}
ProcessId	1044
Image	C:\Windows\System32\svchost.exe
User	NT AUTHORITY\NETWORK SERVICE
Protocol	tcp
Initiated	false
SourceIsIpv6	false
SourceIp	10.100.2.58

This other person downloaded a file and ran it. When was this file run?

This took me a while to find the solution, my way is definitely not the most efficient. I first looked for the location of where the first malicious binary (antivirus.exe) was downloaded, I then searched for that path all the while filtering for event ID 1:



This is where we see the following:

UtcTime	2024-01-08 14:24:18.804
ProcessGuid	{c5d2b969-0592-659c-1f01-000000002701}
ProcessId	4544
Image	C:\Users\Sophie\download\decryptor.exe

The value of the UtcTime field is the answer (excluding the milliseconds). Another way to find the answer would be to look for process creation logs after the time of infection which we determined in the 4th question.

The order for the other question is (aka the order of events):

1. Sophia downloaded the malware and ran it.
2. The malware encrypted the files on the computer and showed a ransomware note.
3. Sohpia ran out and reached out to your for help.
4. Someone else logged into Sophie's machine via RDP and started looking around.
5. The intruder downloaded a decryptor and decrypted all the files.
6. A note was created on the desktop telling Sophie to check her Bitcoin.
7. We arrive on the scene to investigate.

The TryHackMe retracted room was an educational exercise focused on using Sysmon logs to investigate a ransomware attack. The scenario describes a user who unwittingly install ransomware disguised as an antivirus program. I was able to correctly answer all questions, but I in no way did it the most efficient way possible. If you have any feedback and tips please reach out to me.