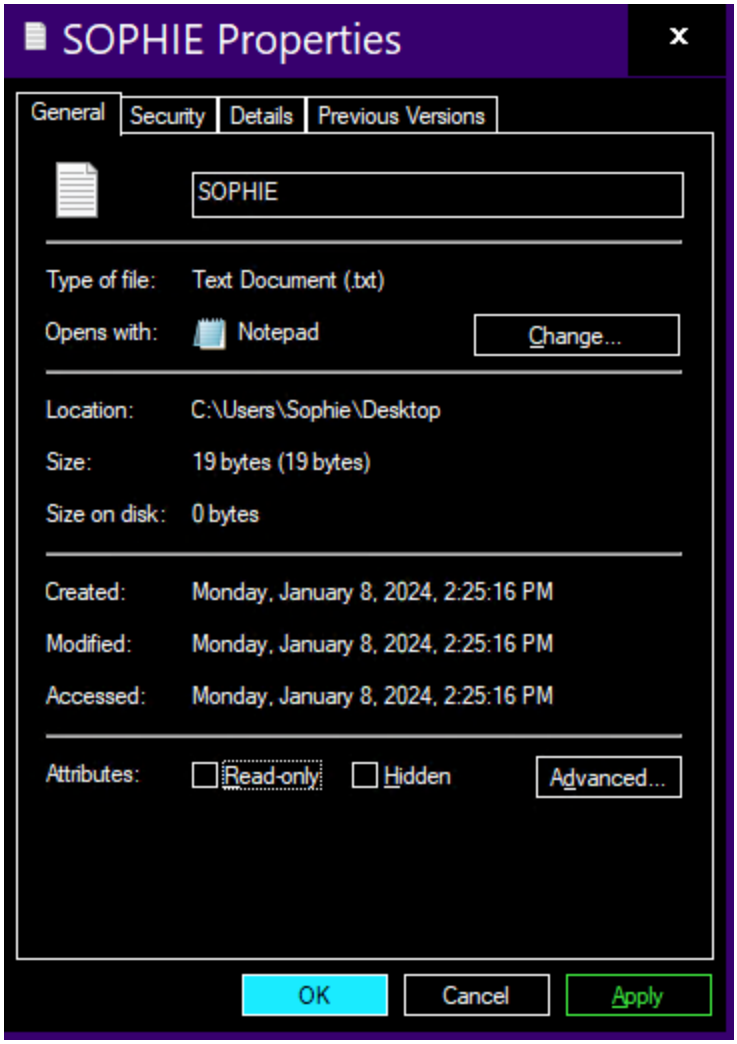
Retracted - ransomware room

Created	@August 6, 2025 5:25 PM
Tags	

Task 2: The Message

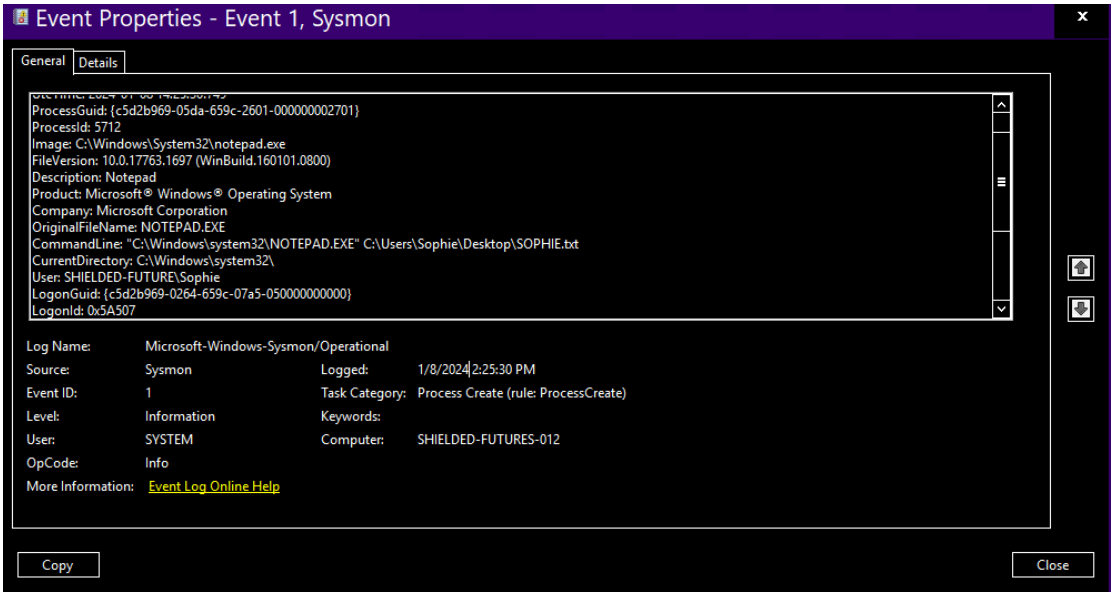
Q: What is the full path of the text file containing the "message"?
There's a file named "SOPHIE" on the desktop. By right-clicking it and choose "Properties", we can see the full path of the file.



Answer: C:\Users\Sophie\Desktop\SOPHIE.txt

Q: What program was used to create the text file?
A: notepad.exe - since file type is text document (.txt).

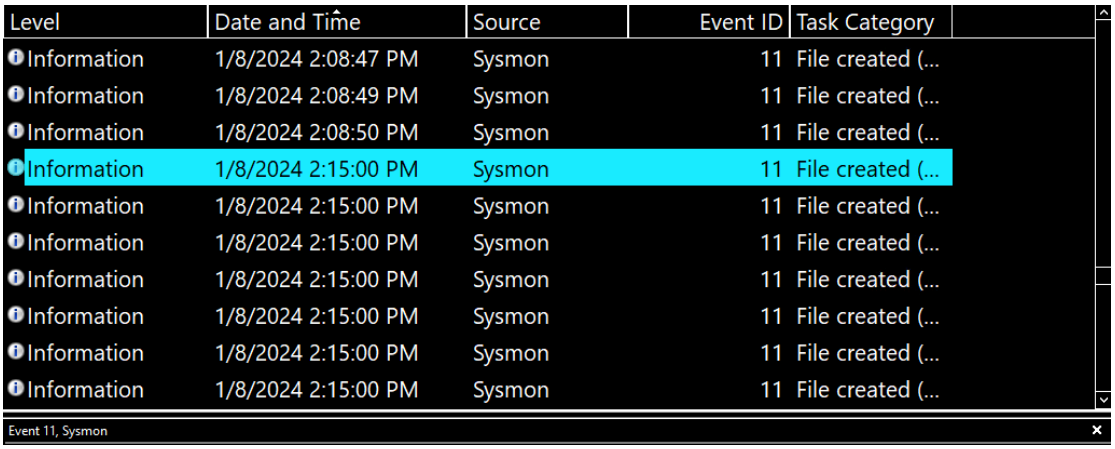
Q: What is the time of execution of the process that created the text file? Timezone UTC (Format YYYY-MM-DD hh:mm:ss)
Using “Event Viewer” with Event ID 1 (Process creation) and find “sophie.txt”, we are able to get the log for the process creation linking to the text file.

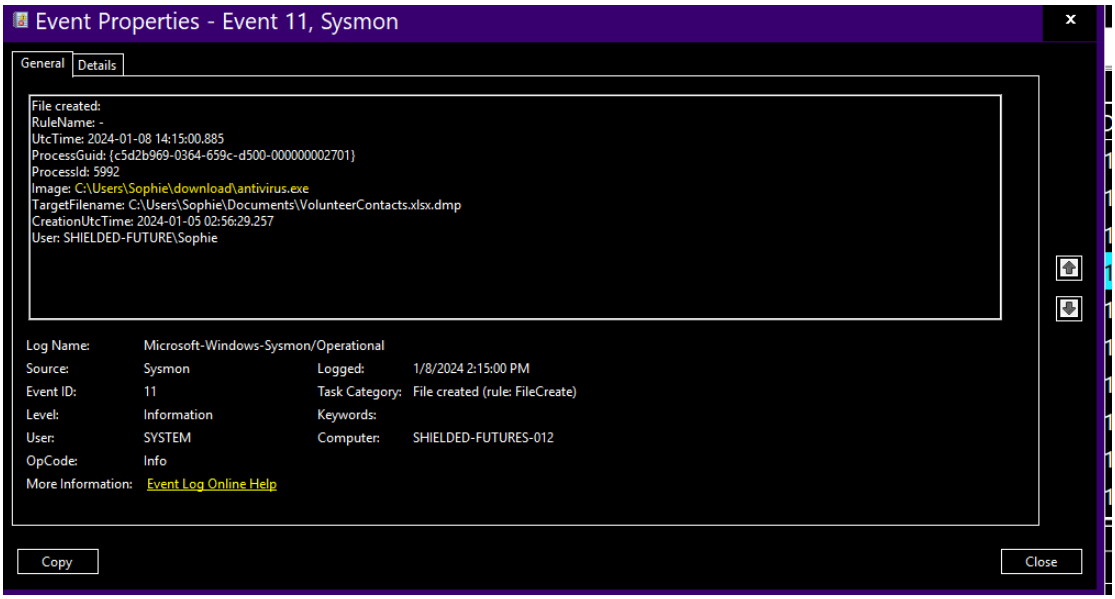


Answer: 2024-01-08 14:25:30

Task 3: Something Wrong

Q: What is the filename of this "installer"? (Including the file extension)
Using Event ID 11 (File Create operation) around the time that the text file above was created, I was able to find a fishy “antivirus program” that Sophie mentioned earlier, and it seems to be the one as it was encrypting other files from the log.



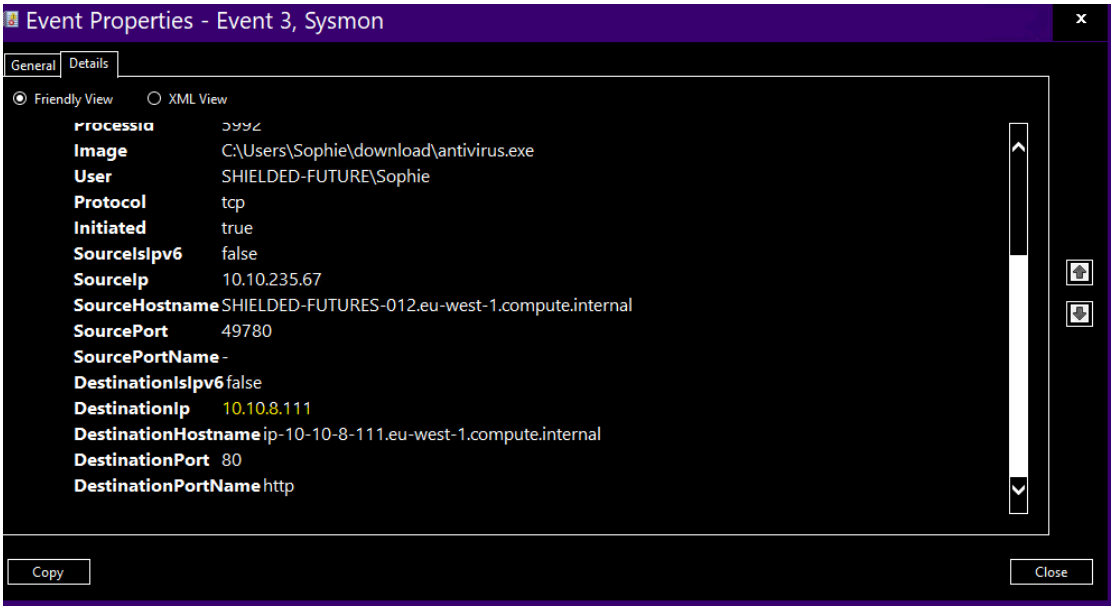


A: antivirus.exe

Q: What is the download location of this installer?
A: C:\Users\Sophie\download - as seen on the above screenshot.

Q: The installer encrypts files and then adds a file extension to the end of the file name. What is this file extension?
A: .dmp - also from the above screenshot.

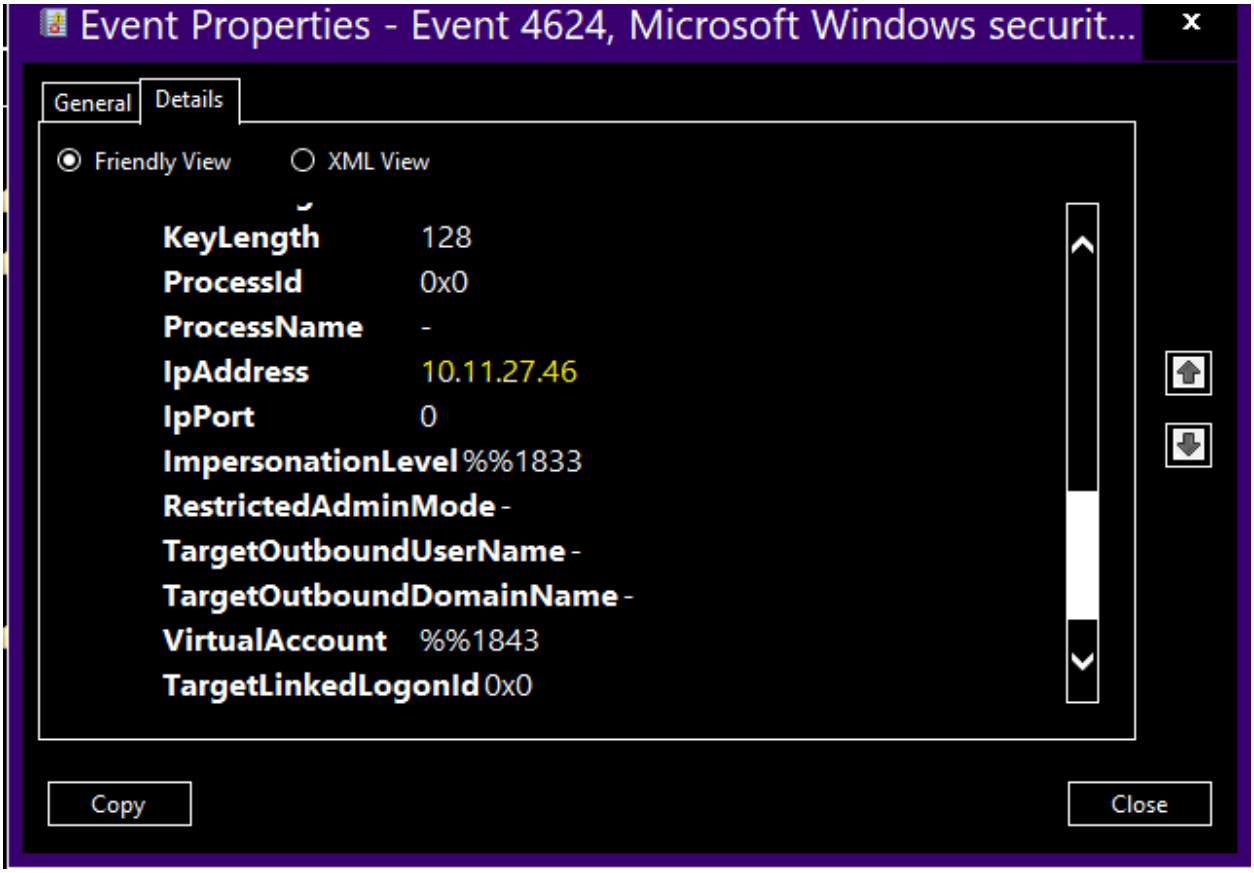
Q: The installer reached out to an IP. What is this IP?
By using Event ID 3, I was able to filter the logs to network connection created by processes, and searching for “antivirus.exe” really did the trick.



Ans: 10.10.8.111

Task 4: Back to Normal

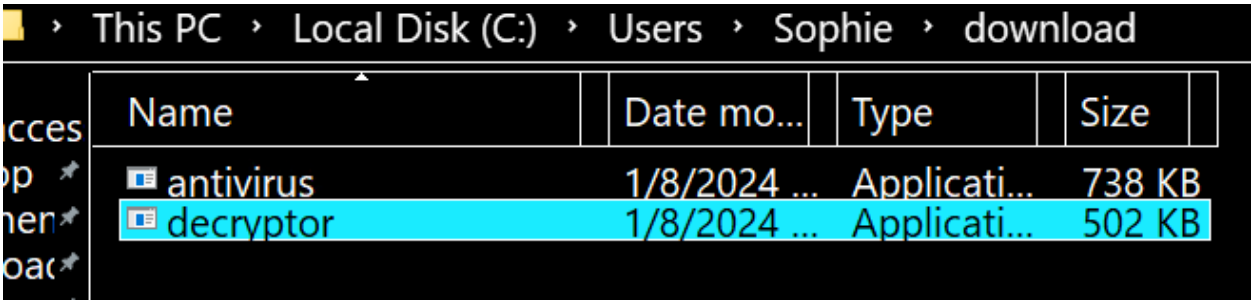
Q: The threat actor logged in via RDP right after the “installer” was downloaded. What is the source IP?
With the prior knowledge that the “antivirus” ransomware was run at 2:15 PM on August 1st 2024, I checked the Security tab in Event Viewer with event ID **4624** (successful logon), and I was able to find the logon at 2:19 PM with a weird IP.

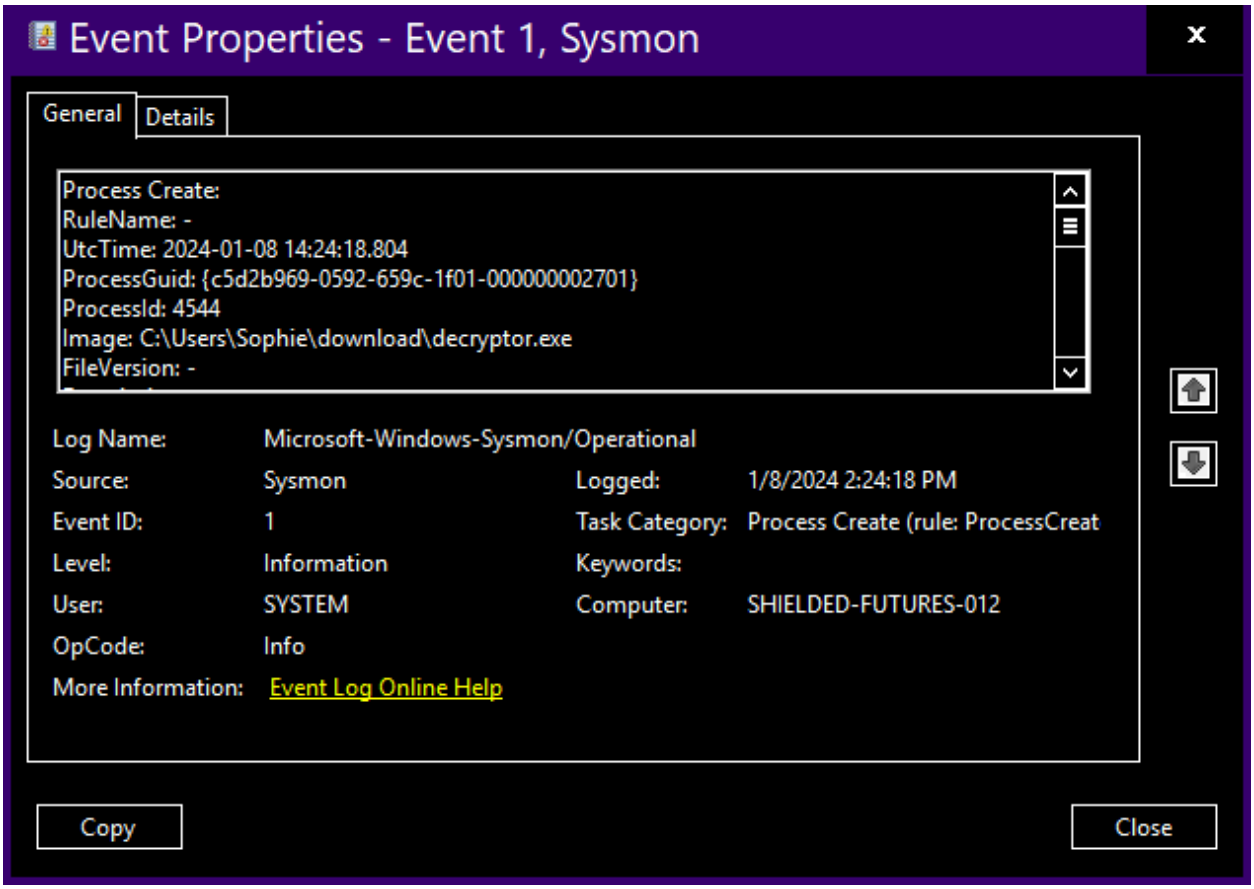


Ans: 10.11.27.46

Q: This other person downloaded a file and ran it. When was this file run? Timezone UTC (Format YYYY-MM-DD hh:mm:ss)

The person seems to download a file named “decryptor” as seen in the “download” folder. Using event viewer and filter out event ID **1 and 11**, I was able to look for when the process was created.





Ans: 2024-01-08 14:24:18

Task 5: Doesn't Make Sense

For this task, it's about arranging the events in order. Apparently, the intruder left some bitcoin for the organization after realizing it's a charity.

After seeing the ransomware note, Sophie ran out and reached out to you for help.

3

Sophie downloaded the malware and ran it.

1

After all the files are restored, the intruder left the desktop telling Sophie to check her Bitcoin.

6

The intruder realized he infected a charity organization. He then downloaded a decryptor and decrypted all the files.

5

The downloaded malware encrypted the files on the computer and showed a ransomware note.

2

While Sophie was away, an intruder logged into Sophie's machine via RDP and started looking around.

4

Sophie and I arrive on the scene to investigate. At this point, the intruder was gone.

7