**Retracted**

A file with band-aid on it

AI-generated content may be incorrect.

**TASK1: Introduction**

A Mother's Plea

"Thanks for coming. I know you are busy with your new job, but I did not know who else to turn to."

"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 fine?"

**Connecting to the Machine**

Start the virtual machine in split-screen view by clicking on the green "Start Machine" button on the upper right section of this task. If the VM is not visible, use the blue "Show Split View" button at the top-right of the page. Alternatively, you can connect to the VM using the credentials below via "Remote Desktop".

A screenshot of a computer

AI-generated content may be incorrect.

"Oh, the password doesn't work? Wait, I have it written somewhere. Uhmm... Try this:"

A screenshot of a computer

AI-generated content may be incorrect.

**TASK 2: The Message**

"So, as soon as you finish logging in to the computer, you'll see a file on the desktop addressed to me."

"I have no idea why that message is there and what it means. Maybe you do?"

**Q1. What is the full path of the text file containing the "message"?**

Locate SOPHIE.txt on the desktop and review its properties.

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

A screenshot of a computer

AI-generated content may be incorrect.

**Q2. What program was used to create the text file?**

Open Event Viewer.

Go to Application and Service Logs, then select Microsoft > Windows > Sysmon > Operational.

To access the ‘Process Create’ category, apply a filter using Event ID 1.

Many events may appear. Search for SOPHIE.txt within the results.

A screenshot of a computer

AI-generated content may be incorrect.

*A screenshot of a computer program

AI-generated content may be incorrect.*

Below the image, the program used to create the file is displayed.

*notepad.exe*

**Q3. What is the time of execution of the process that created the text file? Timezone UTC (Format YYYY-MM-DD hh:mm:ss)**

The execution time is listed under UtcTime in the Event Properties.

A screenshot of a computer program

AI-generated content may be incorrect.

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

**TASK 3: Something Wrong**

"I swear something went wrong with my computer when I ran the installer. Suddenly, my files could not be opened, and the wallpaper changed, telling me to pay."

"Wait, are you telling me that the file I downloaded is a virus? But I downloaded it from Google!"

**Q1. What is the filename of this "installer"? (Including the file extension)**

Let’s review the downloads section within the INTERNET browser.

A screenshot of a computer

AI-generated content may be incorrect.

*antivirus.exe*

**Q2. What is the download location of this installer?**

**A screenshot of a computer error

AI-generated content may be incorrect.**

*C:\Users\Sophie\download*

**Q3. The installer encrypts files and then adds a file extension to the end of the file name. What is this file extension?**

Return to Event Viewer and search for Event ID 11 related to file creation. Locate the antivirus.exe file.

A screenshot of a computer

AI-generated content may be incorrect.

*.dmp*

**Q4. The installer reached out to an IP. What is this IP?**

Filter Event ID 3 logs for network connections and locate antivirus.exe.

A screenshot of a computer program

AI-generated content may be incorrect.

*10.10.8.111*

**TASK 4: Back to Normal**

"So what happened to the virus? It does seem to be gone since all my files are back."

**Q1: The threat actor logged in via RDP right after the “installer” was downloaded. What is the source IP?**

We can use the event ID 3 filter and check for any RDP connections.

A screenshot of a computer program

AI-generated content may be incorrect.

*10.11.27.46*

**Q2: This other person downloaded a file and ran it. When was this file run? Timezone UTC (Format YYYY-MM-DD hh:mm:ss)**

To check for process creation, use Event ID 1 in the search. Let’s search for the decryptor.exe file that was previously identified in the Downloads folder.

A screenshot of a computer

AI-generated content may be incorrect.

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

**TASK 5. Doesn’t Make Sense**

"So you're telling me that someone accessed my computer and changed my files but later undid the changes?"

"That doesn't make any sense. Why infect my machine and clean it afterwards?"

"Can you help me make sense of this?"

Arrange the following events in sequential order from 1 to 7, based on the timeline in which they occurred.

**Q1. After seeing the ransomware note, Sophie ran out and reached out to you for help.**

*3*

**Q2. QqTop of Form**

**Bottom of Form**

**Sophie downloaded the malware and ran it.**

*1*

**Q3. Top of Form**

**Bottom of Form**

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

*6Top of Form*

**Q4.**

**Bottom of Form**

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

*5Top of Form*

**Q6.**

**Bottom of Form**

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

*2*Top of Form

**Q7.**

**Bottom of Form**

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

*4*Top of Form

**Q8.**

**Bottom of Form**

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

*7*

**TASK6: Conclusion**

"Adelle from Finance just called me. She says that someone just donated a huge amount of bitcoin to our charity's account!"

"Could this be our intruder? His malware accidentally infected our systems, found the mistake, and retracted all the changes?"

"Maybe he had a change of heart?"