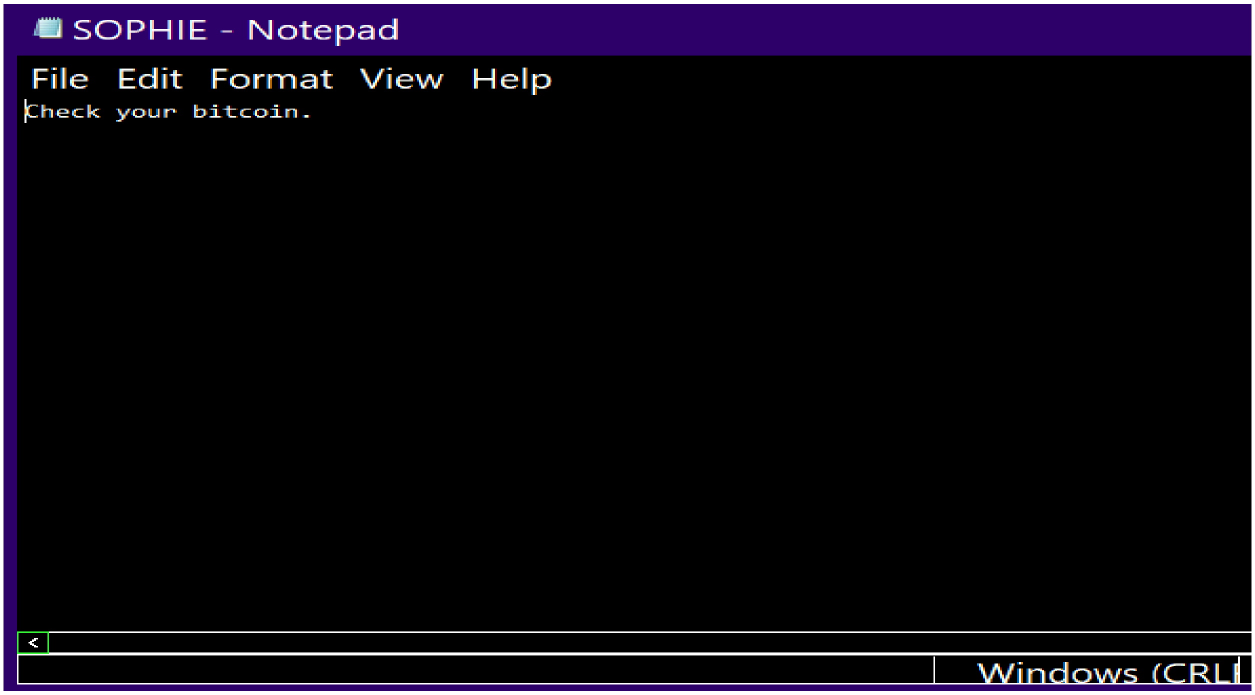
Technical Project: Endpoint Security Monitoring

Tools used: Powershell, Event Viewer, Sysmon, TryHackMe Virtual Machine

Task Overview

I've been called in to investigate a suspicious incident involving a computer infection. The user, Sophie, downloaded and ran an installer for what she believed was antivirus software. Shortly afterward, she noticed that her files were inaccessible, her wallpaper had changed to a ransom demand, and a message instructed her to pay to recover her files. Panicked, Sophie left the room to seek help. However, by the time she returned, her computer appeared to be back to normal, except for a mysterious message instructing her to check her Bitcoin wallet.

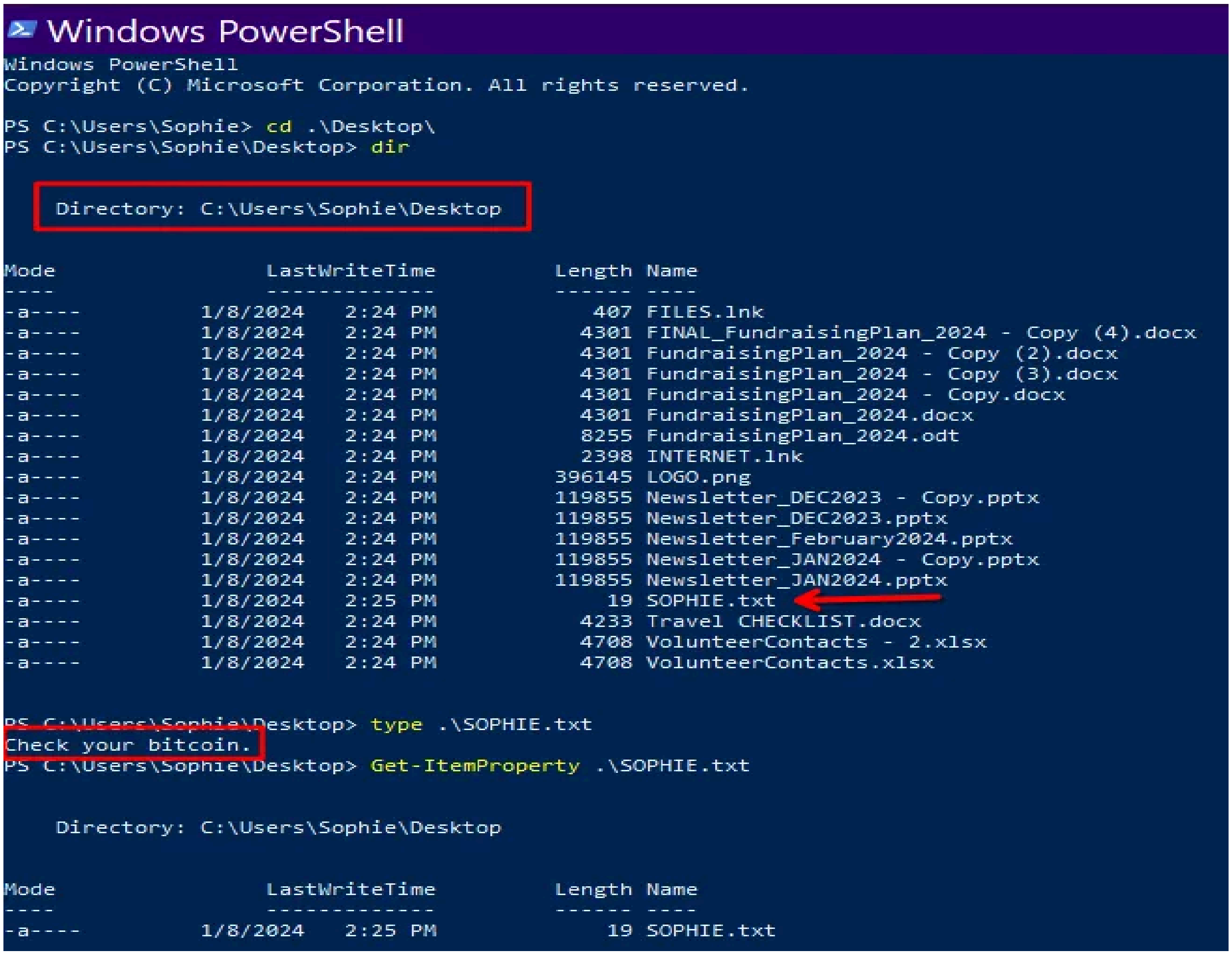
My task is to thoroughly examine the system to determine what happened, assess whether the computer is safe, and piece together the sequence of events that transpired.



Check your bitcoin.

Step 1: Investigating the Desktop Message

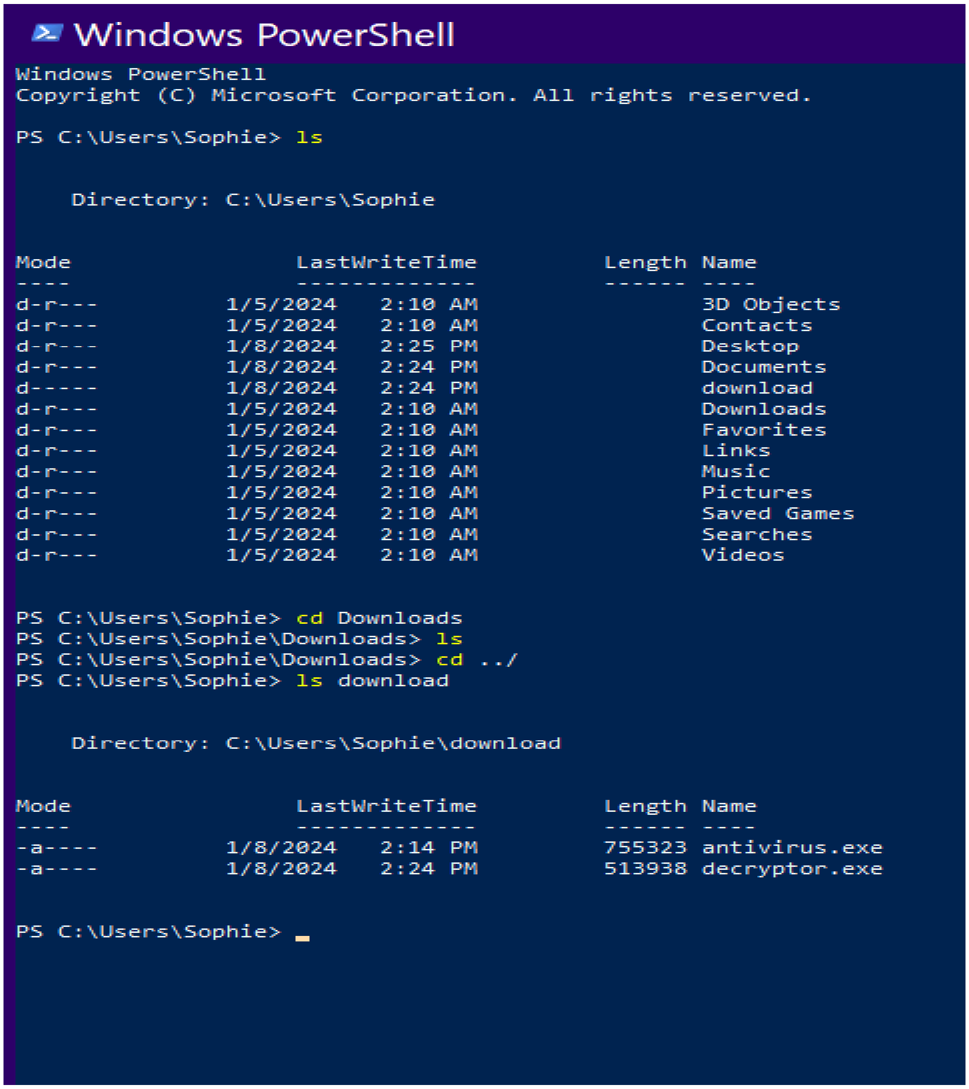
- **Objective:** Find and analyze the message file left on the desktop.
    - Located the text file at:
        - **Full Path:** `C:\Users\Sophie\Desktop\SOPHIE.txt`
    - Verified the program that created the file:
        - **Program:** `notepad.exe`
    - Identified the process creation time from Sysmon logs (Event ID 1):
        - **Execution Time:** `2024-01-08 14:25:30 UTC`



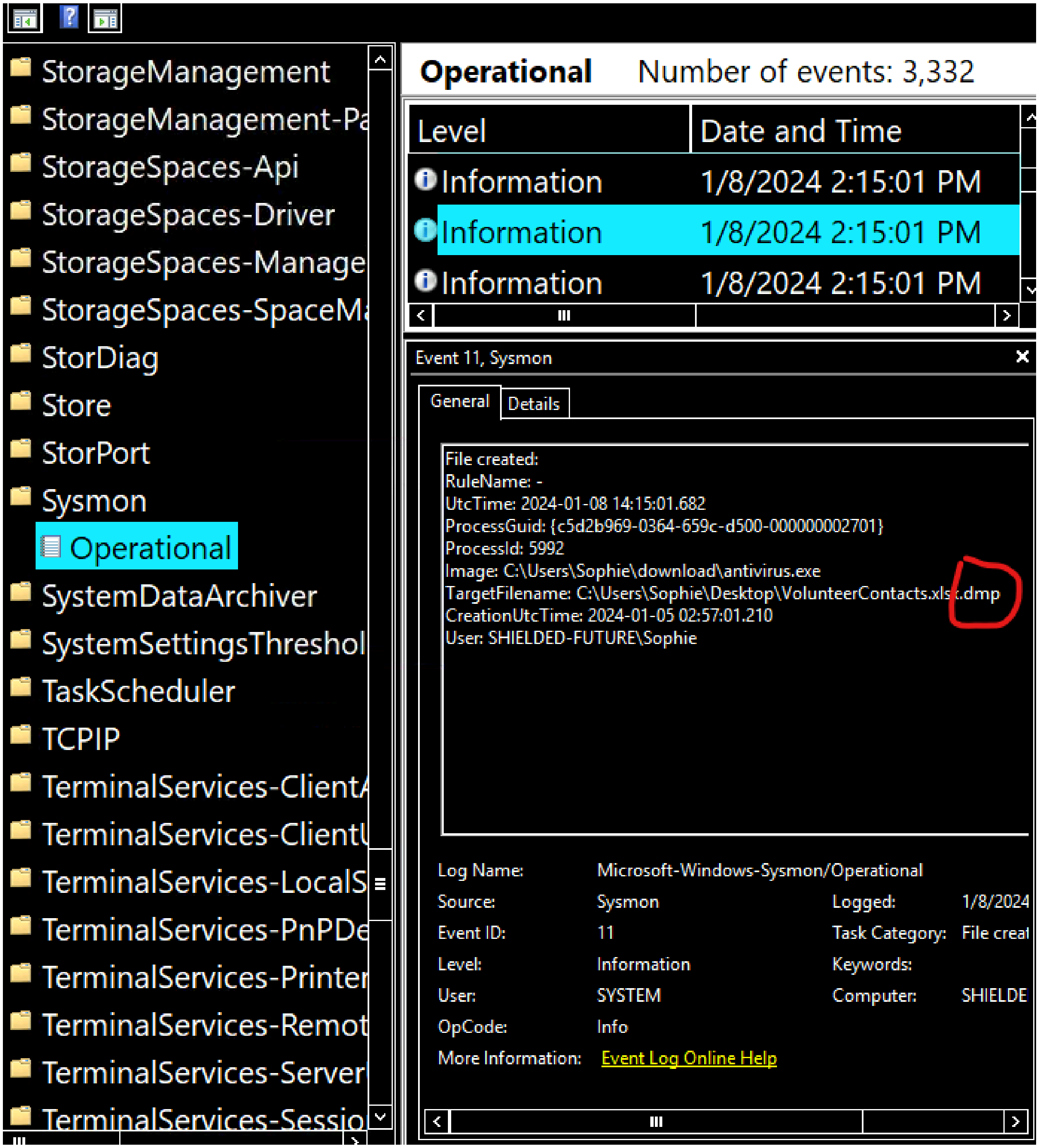
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Sophie> cd .\Desktop\
PS C:\Users\Sophie\Desktop> dir


    Directory: C:\Users\Sophie\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          1/8/2024   2:24 PM            407 FILES.lnk
-a----          1/8/2024   2:24 PM           4301 FINAL_FundraisingPlan_2024 - Copy (4).docx
-a----          1/8/2024   2:24 PM           4301 FundraisingPlan_2024 - Copy (2).docx
-a----          1/8/2024   2:24 PM           4301 FundraisingPlan_2024 - Copy (3).docx
-a----          1/8/2024   2:24 PM           4301 FundraisingPlan_2024 - Copy.docx
-a----          1/8/2024   2:24 PM           4301 FundraisingPlan_2024.docx
-a----          1/8/2024   2:24 PM           8255 FundraisingPlan_2024.odt
-a----          1/8/2024   2:24 PM           2398 INTERNET.lnk
-a----          1/8/2024   2:24 PM         396145 LOGO.png
-a----          1/8/2024   2:24 PM         119855 Newsletter_DEC2023 - Copy.pptx
-a----          1/8/2024   2:24 PM         119855 Newsletter_DEC2023.pptx
-a----          1/8/2024   2:24 PM         119855 Newsletter_February2024.pptx
-a----          1/8/2024   2:24 PM         119855 Newsletter_JAN2024 - Copy.pptx
-a----          1/8/2024   2:24 PM         119855 Newsletter_JAN2024.pptx
-a----          1/8/2024   2:25 PM             19 SOPHIE.txt
-a----          1/8/2024   2:24 PM           4233 Travel CHECKLIST.docx
-a----          1/8/2024   2:24 PM           4708 VolunteerContacts - 2.xlsx
-a----          1/8/2024   2:24 PM           4708 VolunteerContacts.xlsx


PS C:\Users\Sophie\Desktop> type .\SOPHIE.txt
Check your bitcoin.
PS C:\Users\Sophie\Desktop> Get-ItemProperty .\SOPHIE.txt


    Directory: C:\Users\Sophie\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          1/8/2024   2:25 PM             19 SOPHIE.txt
```

Step 2: Examining the Malware Installer

- **Objective:** Analyze the malware that Sophie downloaded.
  - Identified the installer:
    - **Filename:** `antivirus.exe`
  - Found its download location:
    - **Path:** `C:\Users\Sophie\download`
  - Discovered in Event Viewer that the installer encrypted files and added an extension:
    - **File Extension:** `.dmp`
  - Tracked the external IP the installer reached out to:
    - **IP Address:** `10.10.8.111`



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Sophie> ls


    Directory: C:\Users\Sophie


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          1/5/2024   2:10 AM                3D Objects
d-r---          1/5/2024   2:10 AM                Contacts
d-r---          1/8/2024   2:25 PM                Desktop
d-r---          1/8/2024   2:24 PM                Documents
d-----          1/8/2024   2:24 PM                download
d-r---          1/5/2024   2:10 AM                Downloads
d-r---          1/5/2024   2:10 AM                Favorites
d-r---          1/5/2024   2:10 AM                Links
d-r---          1/5/2024   2:10 AM                Music
d-r---          1/5/2024   2:10 AM                Pictures
d-r---          1/5/2024   2:10 AM                Saved Games
d-r---          1/5/2024   2:10 AM                Searches
d-r---          1/5/2024   2:10 AM                Videos


PS C:\Users\Sophie> cd Downloads
PS C:\Users\Sophie\Downloads> ls
PS C:\Users\Sophie\Downloads> cd ../
PS C:\Users\Sophie> ls download


    Directory: C:\Users\Sophie\download


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          1/8/2024   2:14 PM         755323 antivirus.exe
-a----          1/8/2024   2:24 PM         513938 decryptor.exe


PS C:\Users\Sophie> _
```



Operational Number of events: 3,332

Level	Date and Time
Information	1/8/2024 2:15:01 PM
Information	1/8/2024 2:15:01 PM
Information	1/8/2024 2:15:01 PM

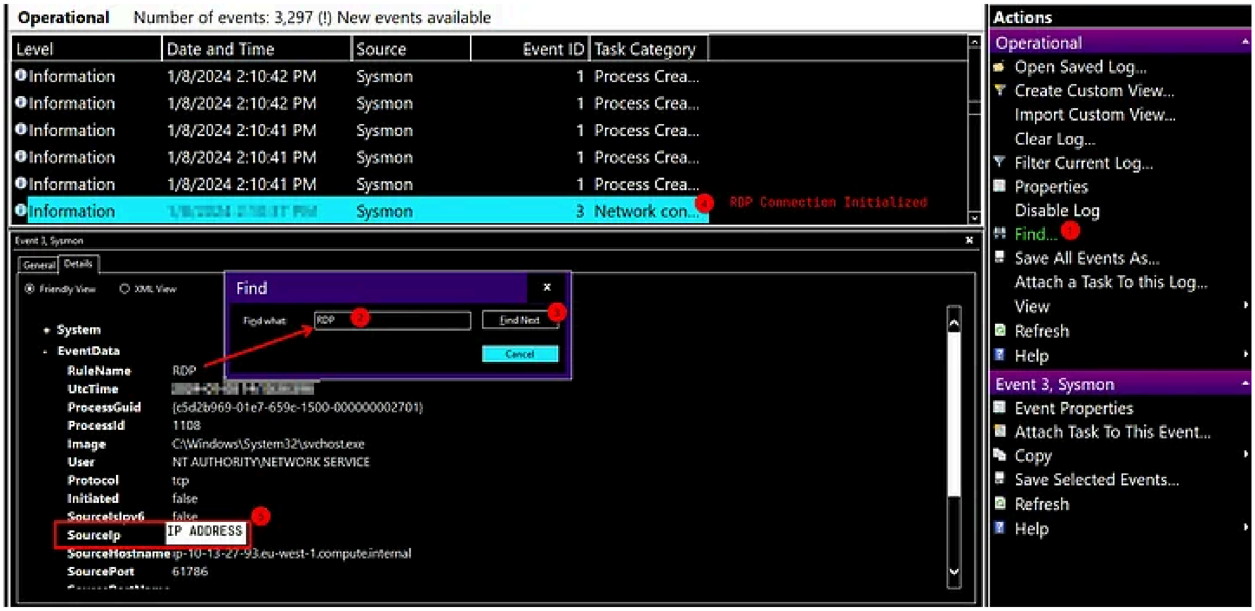
Event 11, Sysmon

```
File created:
RuleName: -
UtcTime: 2024-01-08 14:15:01.682
ProcessGuid: {c5d2b969-0364-659c-d500-000000002701}
ProcessId: 5992
Image: C:\Users\Sophie\download\antivirus.exe
TargetFilename: C:\Users\Sophie\Desktop\VolunteerContacts.xlsx.dmp
CreationUtcTime: 2024-01-05 02:57:01.210
User: SHIELDED-FUTURE\Sophie
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	1/8/2024
Event ID:	11	Task Category:	File creat
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	SHIELDE
OpCode:	Info		
More Information:	Event Log Online Help		

Step 3: Investigating Remote Access

- **Objective:** Trace activity related to the threat actor's remote login.
    - Found the source IP of the RDP login:
    - *Note: Filtering for Event ID=3 and "RDP" helped narrow results. Navigating to the download directory in PowerShell helped deduce the time of the malware download which helped find the RDP login time**:
        - **Source IP:** `10.11.27.46`
    - Identified the time the second person downloaded and ran a file:
        - **Execution Time:** `2024-01-08 14:24:18 UTC`



Operational Number of events: 3,297 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	1/8/2024 2:10:42 PM	Sysmon	1	Process Crea...
Information	1/8/2024 2:10:42 PM	Sysmon	1	Process Crea...
Information	1/8/2024 2:10:41 PM	Sysmon	1	Process Crea...
Information	1/8/2024 2:10:41 PM	Sysmon	1	Process Crea...
Information	1/8/2024 2:10:41 PM	Sysmon	1	Process Crea...
Information	[redacted]	Sysmon	3	Network con...

RDP Connection Initialized

Event 3, Sysmon

General | Details

◉ Friendly View ○ XML View

Find

Find what: RDP

Find Next

Cancel

```
+ System
- EventData
    RuleName          RDP
    UtcTime           [redacted]
    ProcessGuid       {c5d2b969-01e7-659c-1500-000000002701}
    ProcessId         1108
    Image             C:\Windows\System32\svchost.exe
    User              NT AUTHORITY\NETWORK SERVICE
    Protocol          tcp
    Initiated         false
    SourceIsIpv6      false
    SourceIp          IP ADDRESS
    SourceHostname    ip-10-13-27-93.eu-west-1.compute.internal
    SourcePort        61786
```

Step 4: Arranging Events in Sequence

- **Objective:** Chronologically order the events based on the timeline:
    1. Sophie downloaded the malware and ran it.
    2. The malware encrypted files and displayed a ransomware note.
    3. Sophie ran out to seek help.
    4. An intruder logged into Sophie's machine via RDP.
    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. Investigated the incident upon arrival.

Summary

I conducted a forensic analysis of Sophie's computer to investigate a potential malware infection. By analyzing Sysmon logs, desktop files, and the activity timeline, I discovered that Sophie had been tricked into running ransomware. Interestingly, a threat actor remotely accessed her computer, reversed the ransomware’s effects, and left a message about Bitcoin, which raised questions about their motives. This investigation allowed me to apply key cybersecurity concepts such as process analysis, remote access tracing, and event correlation.