Sherlock: Unit42

■ Very Easy

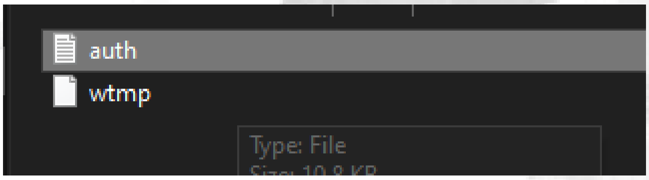
Challenge Description :

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.

Just Answer 8 Tasks

Getting Down to the Task:

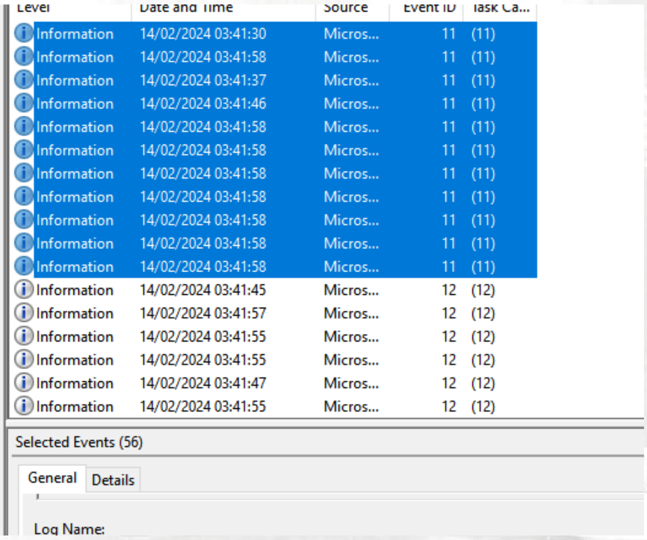
- First download the ZIP file and extract the contents of the ZIP, after that start opening the log files based on the challenges description. We are only given a Windows event log to analyze.



auth
wtmp

Type: File
Size: 10.8 KB

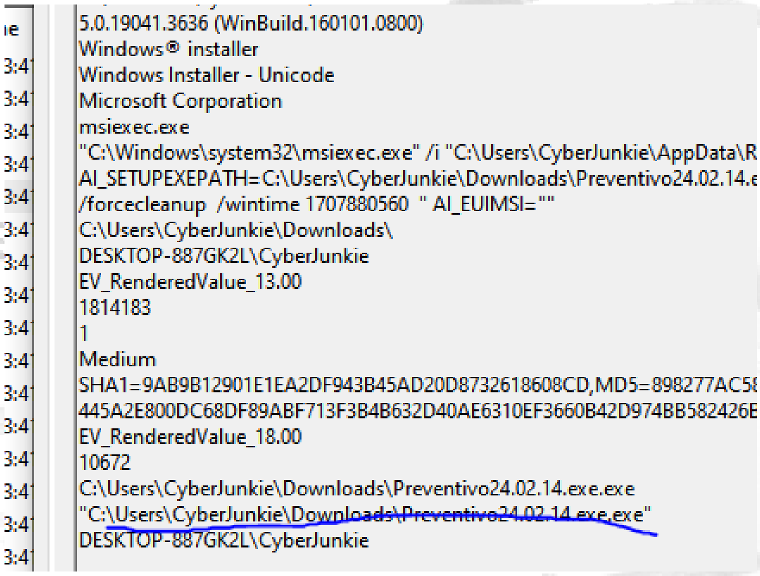
- Opening it up with a Windows machine we can use the Event Viewer to filter it and go though each event.
- To answer Task 1 we can easily just select all the Events with the ID of 11 to get the answer.



Level	Date and Time	Source	Event ID	Task Ca...
Information	14/02/2024 03:41:30	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:37	Micros...	11	(11)
Information	14/02/2024 03:41:46	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:58	Micros...	11	(11)
Information	14/02/2024 03:41:45	Micros...	12	(12)
Information	14/02/2024 03:41:57	Micros...	12	(12)
Information	14/02/2024 03:41:55	Micros...	12	(12)
Information	14/02/2024 03:41:55	Micros...	12	(12)
Information	14/02/2024 03:41:47	Micros...	12	(12)
Information	14/02/2024 03:41:55	Micros...	12	(12)

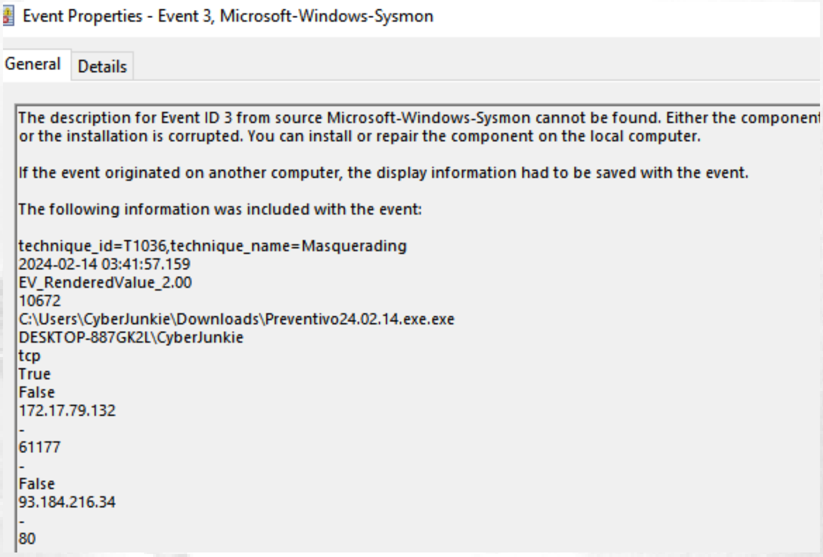
Selected Events (56)

Log Name:



```
5.0.19041.3636 (WinBuild.160101.0800)
Windows® installer
Windows Installer - Unicode
Microsoft Corporation
msiexec.exe
"C:\Windows\system32\msiexec.exe" /i "C:\Users\CyberJunkie\AppData\R
AI_SETUPEXEPATH=C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.e
/forcecleanup  /wintime 1707880560  " AI_EUIMSI=""
C:\Users\CyberJunkie\Downloads\
DESKTOP-887GK2L\CyberJunkie
EV_RenderedValue_13.00
1814183
1
Medium
SHA1=9AB9B12901E1EA2DF943B45AD20D8732618608CD,MD5=898277AC5
445A2E800DC68DF89ABF713F3B4B632D40AE6310EF3660B42D974BB582426E
EV_RenderedValue_18.00
10672
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
"C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe"
DESKTOP-887GK2L\CyberJunkie
```

- Going through the events we see a persistent .exe file that keeps appearing. This is the answer to Task 2
- Further down the events we see the answer to Task 7 and Task 3

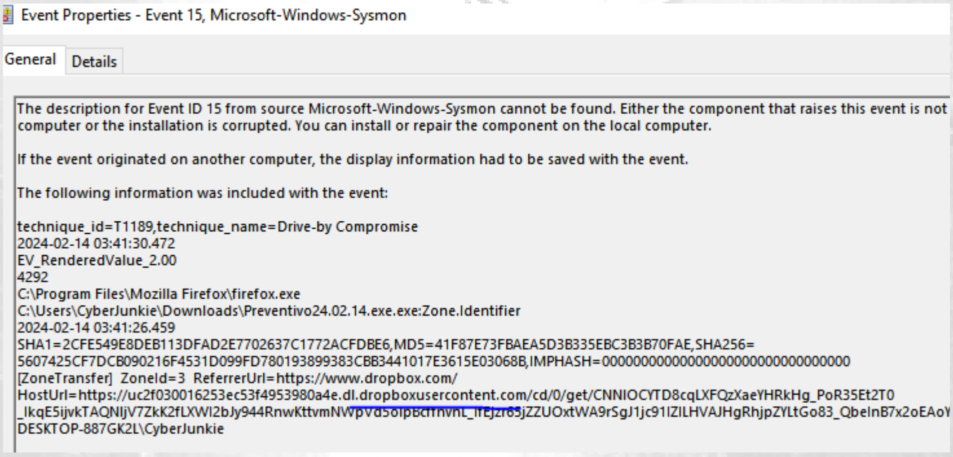


The description for Event ID 3 from source Microsoft-Windows-Sysmon cannot be found. Either the component
or the installation is corrupted. You can install or repair the component on the local computer.

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

The following information was included with the event:

```
technique_id=T1036,technique_name=Masquerading
2024-02-14 03:41:57.159
EV_RenderedValue_2.00
10672
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe
DESKTOP-887GK2L\CyberJunkie
tcp
True
False
172.17.79.132
-
61177
-
False
93.184.216.34
-
80
```



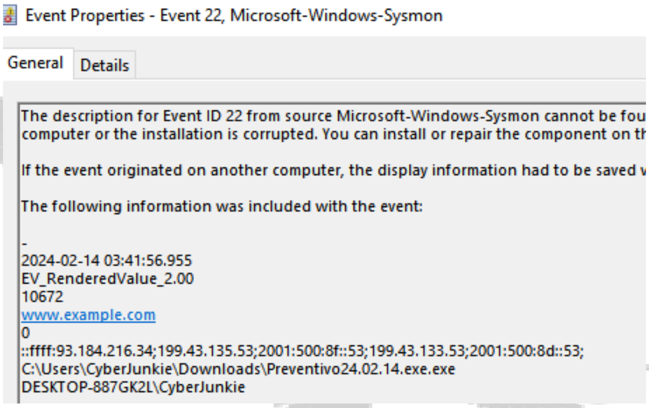
The description for Event ID 15 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not
computer or the installation is corrupted. You can install or repair the component on the local computer.

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

The following information was included with the event:

```
technique_id=T1189,technique_name=Drive-by Compromise
2024-02-14 03:41:30.472
EV_RenderedValue_2.00
4292
C:\Program Files\Mozilla Firefox\firefox.exe
C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe:Zone.Identifier
2024-02-14 03:41:26.459
SHA1=2CFE549E8DEB113DFAD2E7702637C1772ACFDBE6,MD5=41F87E73FBAEA5D3B335EBC3B3B70FAE,SHA256=
5607425CF7DCB090216F4531D099FD780193899383CBB3441017E3615E03068B,IMPHASH=00000000000000000000000000000000
[ZoneTransfer]  ZoneId=3  ReferrerUrl=https://www.dropbox.com/
HostUrl=https://uc2f030016253ec53f4953980a4e.dl.dropboxusercontent.com/cd/0/get/CNNIOCYTD8cqLXFQzXaeYHRkHg_PoR35Et2T0
_IkqE5ijvkTAQNIjV7ZkK2fLXWI2bJy944RnwKttvmNWpVd5oIpBcffnvnL_lfEjzr65jZZUOxtWA9rSgJ1jc91IZILHVAJHgRhjpZYLtGo83_QbeInB7x2oEAoY
DESKTOP-887GK2L\CyberJunkie
```

- Getting to the rest of the Tasks done we continue going through the Event logs. We hit the answer to Task 6


Event Properties - Event 22, Microsoft-Windows-Sysmon

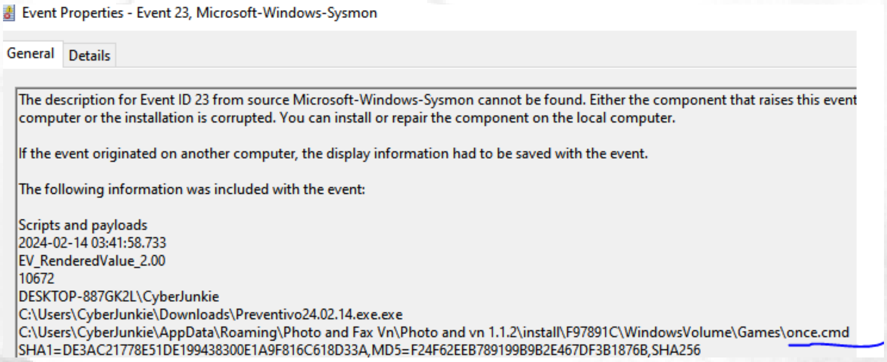
```
The description for Event ID 22 from source Microsoft-Windows-Sysmon cannot be fou
computer or the installation is corrupted. You can install or repair the component on th

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

The following information was included with the event:

-
2024-02-14 03:41:56.955
EV_RenderedValue_2.00
10672
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
```

- I finished the Events, but a quick double check shows I missed a good few like Task 8 ,Task 5 and Task 4

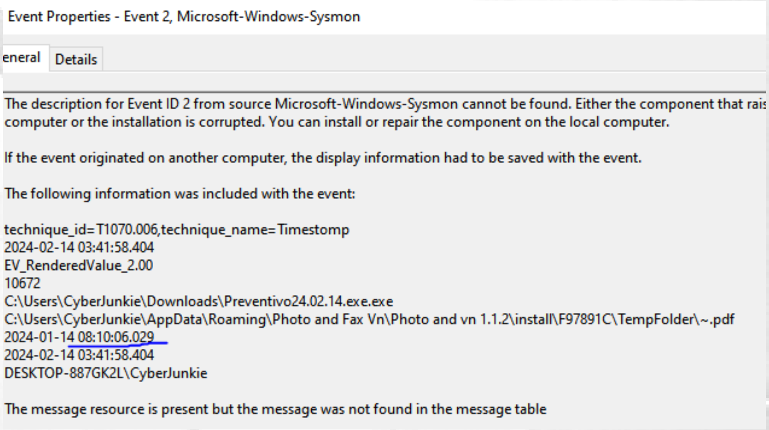

Event Properties - Event 23, Microsoft-Windows-Sysmon

```
The description for Event ID 23 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event
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.

The following information was included with the event:

Scripts and payloads
2024-02-14 03:41:58.733
EV_RenderedValue_2.00
10672
DESKTOP-887GK2L\CyberJunkie
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
SHA1=DE3AC21778E51DE199438300E1A9F816C618D33A,MD5=F24F62EEB789199B9B2E467DF3B1876B,SHA256
```


Event Properties - Event 2, Microsoft-Windows-Sysmon

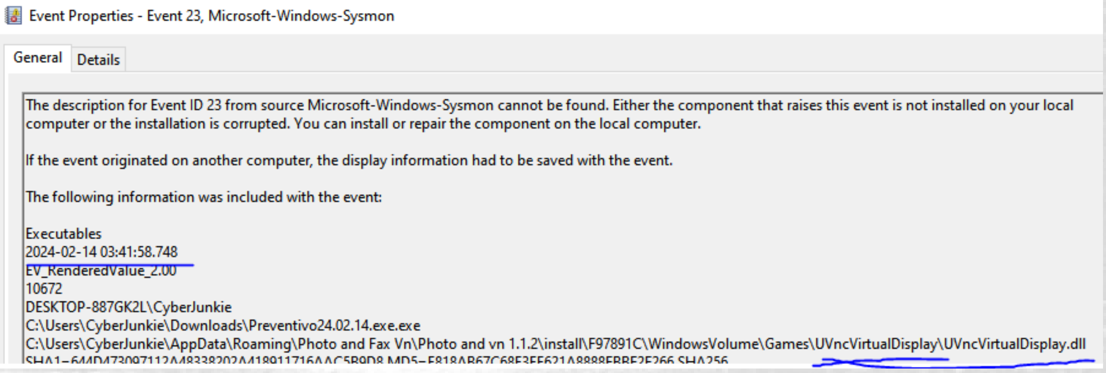
```
The description for Event ID 2 from source Microsoft-Windows-Sysmon cannot be found. Either the component that rais
computer or the installation is corrupted. You can install or repair the component on the local computer.

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

The following information was included with the event:

technique_id=T1070.006,technique_name=Timestomp
2024-02-14 03:41:58.404
EV_RenderedValue_2.00
10672
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\TempFolder\~.pdf
2024-01-14 08:10:06.029
2024-02-14 03:41:58.404
DESKTOP-887GK2L\CyberJunkie

The message resource is present but the message was not found in the message table
```


Event Properties - Event 23, Microsoft-Windows-Sysmon

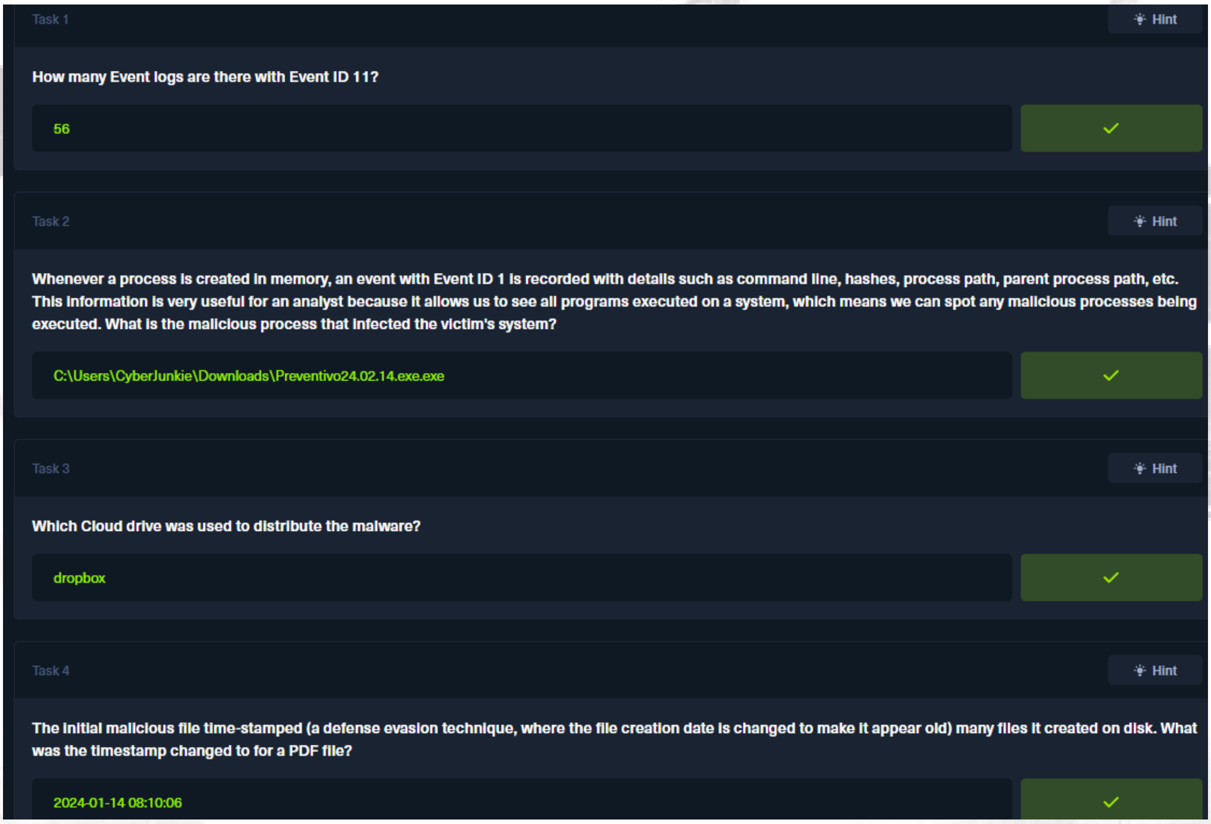
```
The description for Event ID 23 from source Microsoft-Windows-Sysmon cannot be found. Either the component that raises this event is not installed on your local
computer or the installation is corrupted. You can install or repair the component on the local computer.

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

The following information was included with the event:

Executables
2024-02-14 03:41:58.748
EV_RenderedValue_2.00
10672
DESKTOP-887GK2L\CyberJunkie
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\UVncVirtualDisplay\UVncVirtualDisplay.dll
SHA1=644D473097112A48338202A418911716AAC5B9D8,MD5=E818AB67C68F3FF621A8888EBBE2E266,SHA256
```

- This should be all the answers to the Tasks.



Task 1

How many Event logs are there with Event ID 11?

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?

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

Task 3

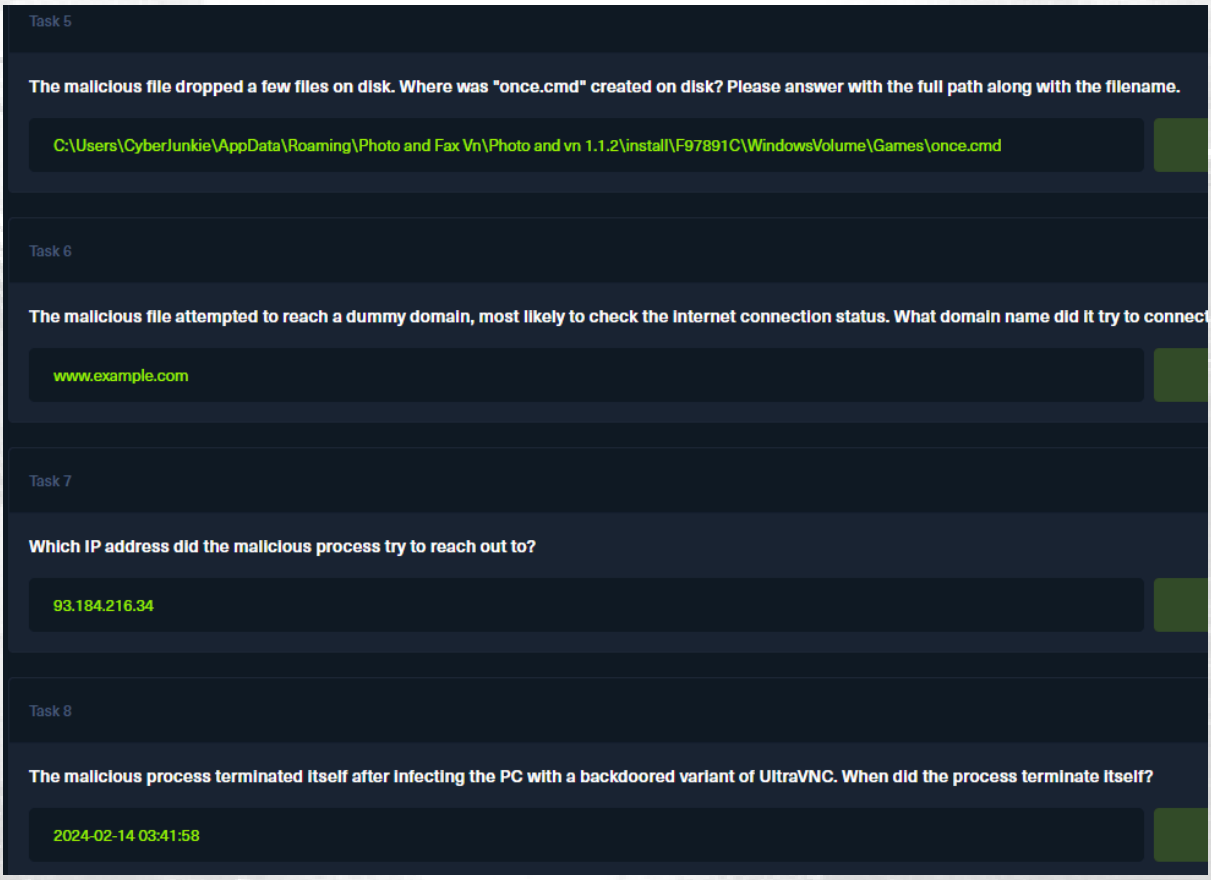
Which Cloud drive was used to distribute the malware?

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?

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.

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

www.example.com

Task 7

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

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?

2024-02-14 03:41:58

Sherlock Brutus - Birdo