Days 2 :

HTB/Sherlock

Challenge : Unit42

Level : Very Easy

Link: [Hack The Box :: Hack The Box](https://app.hackthebox.com/sherlocks/Unit42)

Scenario :

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.

Tools use : Event view

Q1 : How many Event logs are there with Event ID 11?

Open file evtx on Window. I filter it by using “Filter current log” and with ID 11, we have 56 Event logs

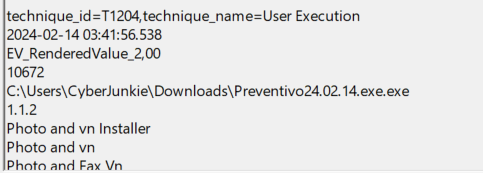


-> Answer : 56

Q2: 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?

- From hint, I search for ID 1 Event logs and you can see it here : [Sysmon Event ID 1 - Process creation (ultimatewindowssecurity.com)](https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90001)

- Filter ID 1, we can see a file run in Downloads dir

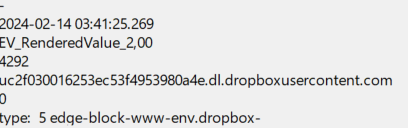


-> Answer : C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe

Q3 : Which Cloud drive was used to distribute the malware?

- From hint, I search for ID 22 Event Logs, you can read more here : [Sysmon Event ID 22 - DNSEvent (ultimatewindowssecurity.com)](https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90022)

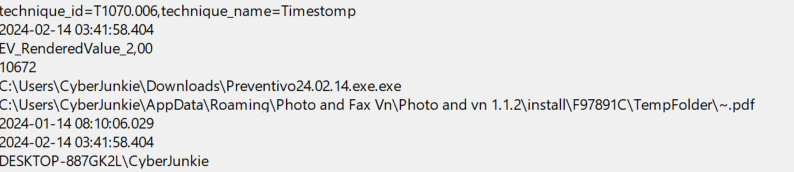
- Filter ID 22, we can see it :



-> Answer : Dropbox

Q4: 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?

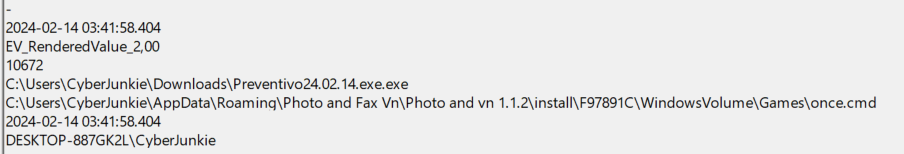
- Filter ID 2 from hint and check event logs, we can see a PDF file :



-> Answer : 2024-01-14 08:10:06

Q5 : 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.

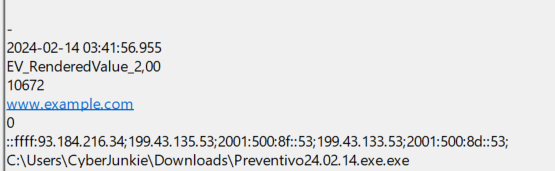
- ID 11 : [Sysmon Event ID 11 - FileCreate (ultimatewindowssecurity.com)](https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90011)



-> Answer : C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd

Q6 : 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 to?

- Filter ID 22 again and check it :

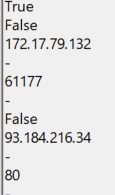


-> Answer : [www.example.com](http://www.example.com)

Q7 : Which IP address did the malicious process try to reach out to?

- [Sysmon Event ID 3 - Network connection detected (ultimatewindowssecurity.com)](https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90003#:~:text=Sysmon%20Event%20ID%203%201%20Description%20of,this%20event%202%20Field%20level%20details%203%20Examples)

- So we filter ID 3 and only 1 Event log for it :

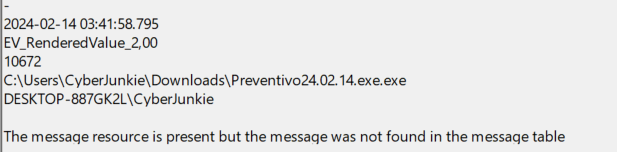


-> Answer : 93.184.216.34

Q8 : The malicious process terminated itself after infecting the PC with a backdoored variant of UltraVNC. When did the process terminate itself?

- [Sysmon Event ID 5 - Process terminated (ultimatewindowssecurity.com)](https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90005#:~:text=5%3A%20Process%20terminated%20This%20is%20an%20event%20from,the%20UtcTime%2C%20ProcessGuid%20and%20ProcessId%20of%20the%20process.)

- Filter ID 5



-> Answer : 2024-02-14 03:41:58