Unit42,evtx(EvtxECmd、Timeline Explorer)

```
Sherlock 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.
* * *
About Unit42
In this very easy 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.
```

palo alto unit 42 UltraVNC 參考：https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2024-01-23-IOCs-from-UltraVNC-infection.txt

文件：Microsoft-Windows-Sysmon-Operational.evtx
使用工具：EvtxECmd、Timeline Explorer

工具參考：

- https://ericzimmerman.github.io/#!index.md
- https://github.com/EricZimmerman/evtx
-

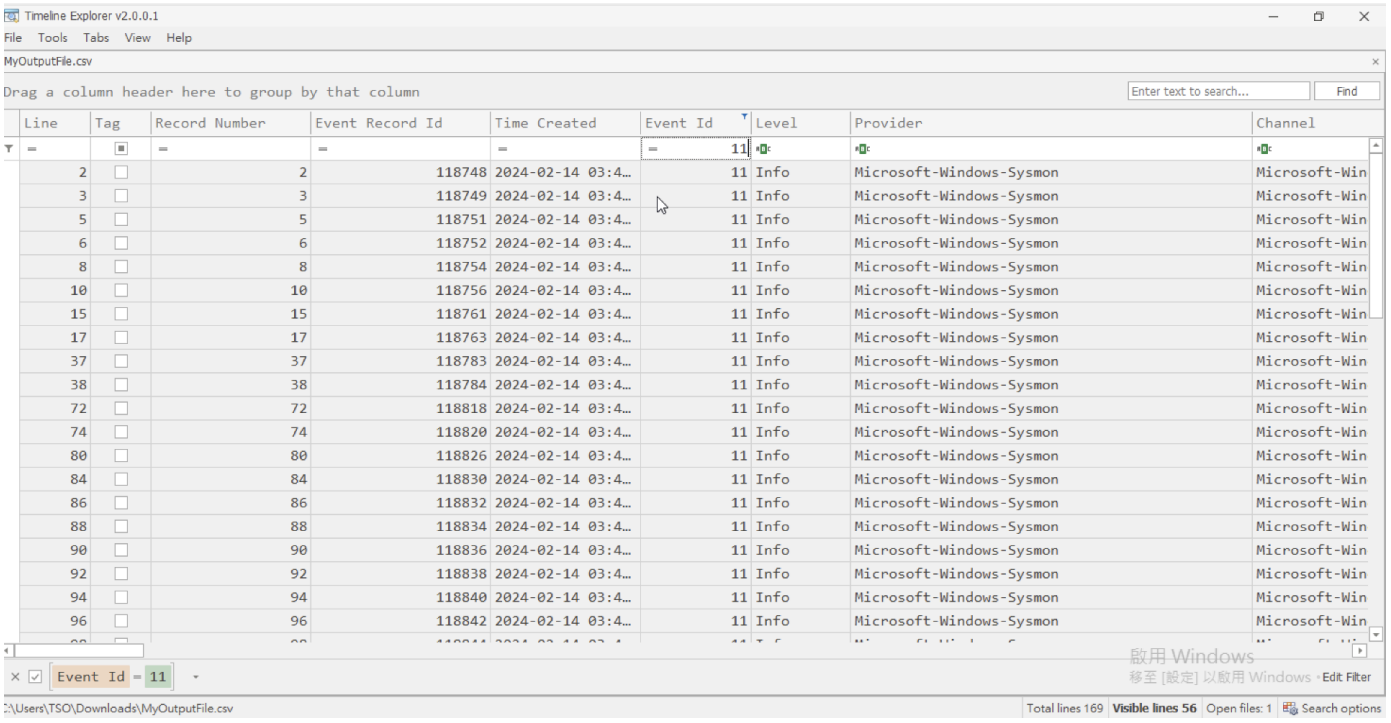
指令：

```
EvtxECmd.exe -f "C:\Users\TSO\Downloads\Microsoft-Windows-Sysmon-Operational.evtx" --csv "C:\Users\TSO\Downloads" --csvf MyOutputFile.csv
```

使用Timeline Explorer分析

Task 1

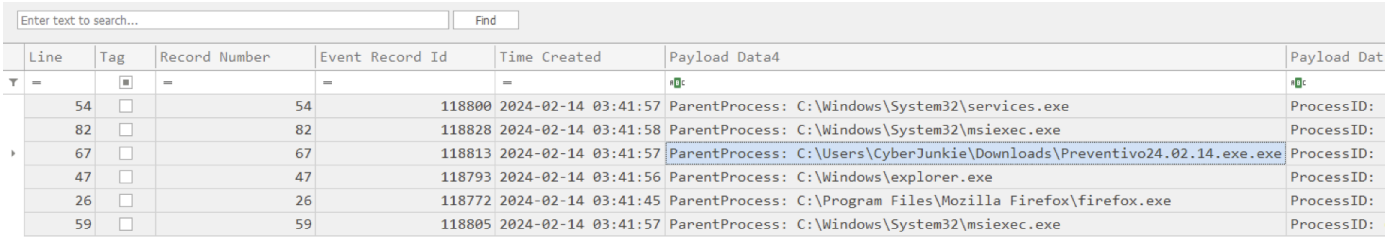
How many Event logs are there with Event ID 11?

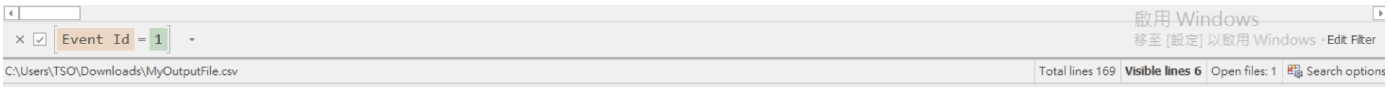


56

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`

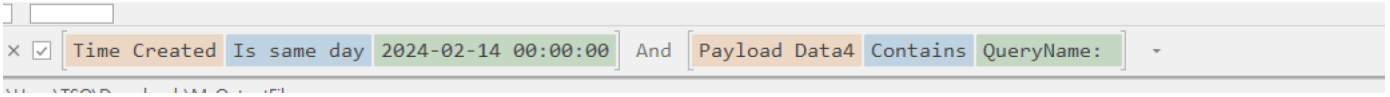
時間點：`2024-02-14 03:41:57`

Task 3

Which Cloud drive was used to distribute the malware?

使用時間篩選先2024-02-14，在逐一檢查並發現雲，後續在篩選一次

	Event Record Id	Time Created	Payload Data4
	=	=	QueryName:
6	118782	2024-02-14 03:41:45	QueryName: d.dropbox.com
1	118747	2024-02-14 03:41:26	QueryName: uc2f030016253ec53f4953980a4e.dl.dropboxusercontent.com
0	118906	2024-02-14 03:41:58	QueryName: www.example.com



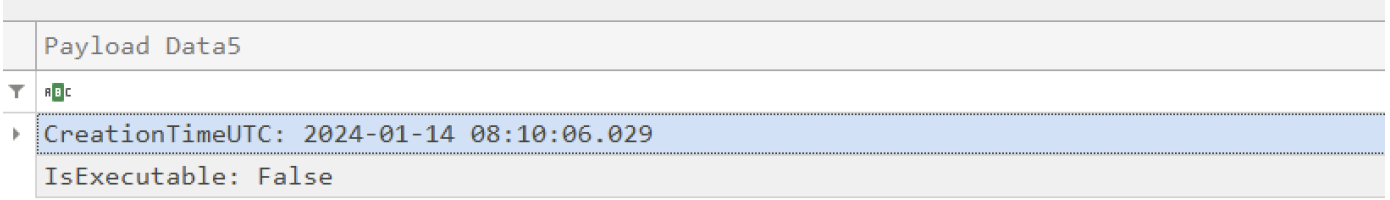
雲時間 與 執行檔時間 相差沒多久

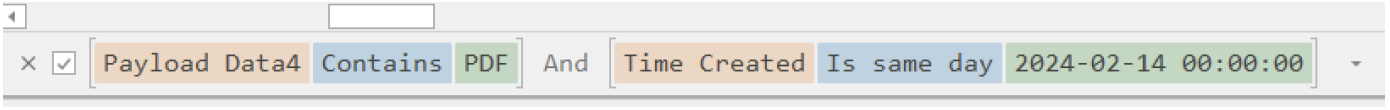
`dropbox`

題外：Event id = 22

Task 4

For many of the files it wrote to disk, the initial malicious file used a defense evasion technique called Time Stomping, where the file creation date is changed to make it appear older and blend in with other files. What was the timestamp changed to for the PDF file?



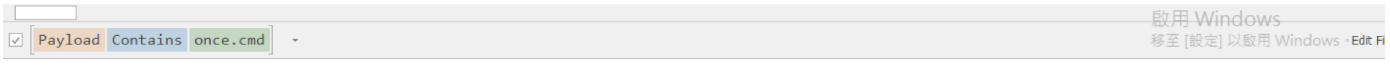


2024-01-14 08:10:06

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.

Time Created	Payload Data4
2024-02-14 03:41:58	TargetFilename: C:\Games\once.cmd
2024-02-14 03:41:58	TargetFilename: C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd
2024-02-14 03:41:58	TargetFilename: C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd
2024-02-14 03:41:58	TargetFilename: C:\Users\CyberJunkie\AppData\Roaming\Photo and Fax Vn\Photo and vn 1.1.2\install\F97891C\WindowsVolume\Games\once.cmd



```
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 to?

回到第3題，查詢id = 22

ht Record Id	Time Created	Payload Data4
	=	
118782	2024-02-14 03:41:45	QueryName: d.dropbox.com
118747	2024-02-14 03:41:26	QueryName: uc2f030016253ec53f4953
118906	2024-02-14 03:41:58	QueryName: www.example.com

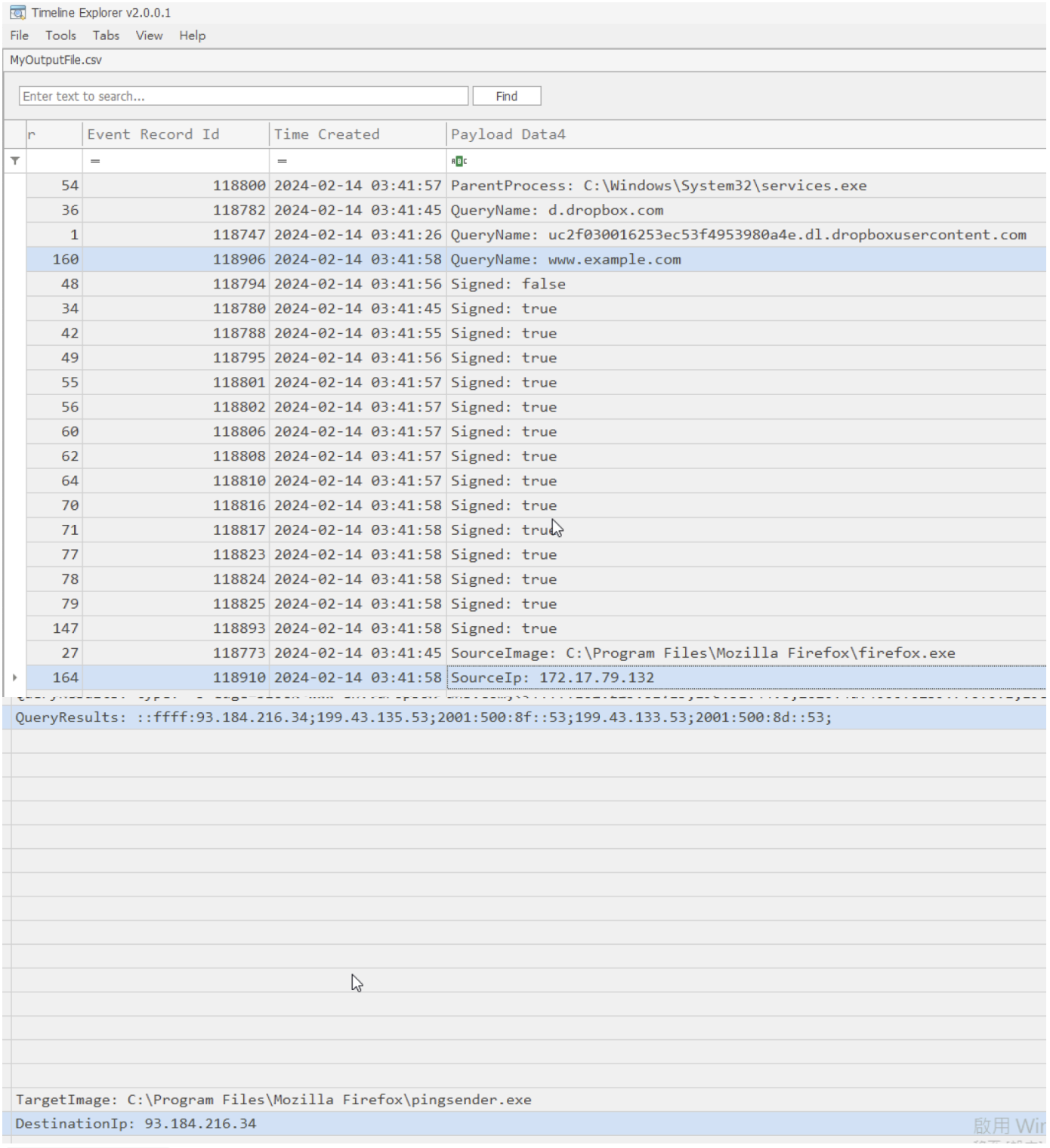
Event Id = 22

`www.example.com`

Task 7

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

看到QueryName底下有src ip，時間相同，往旁邊確認dst ip=



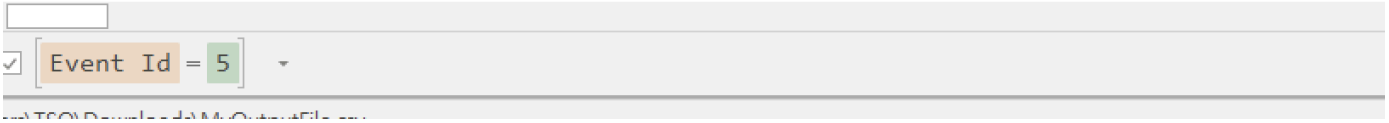
`93.184.216.34`

Task 8

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

事件 ID 5（進程終止）可用於識別特定進程何時退出

Time Created	Payload Data1
=	
2024-02-14 03:41:58	ProcessID: 10672, ProcessGUID: 817bddf3-3684-65cc-2d02-000000001900



2024-02-14 03:41:58