

Unit42,evtz(EvtzECmd、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 参考：<https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2024-01-23-IOCs-from-UltraVNC-infection.txt>

文件：Microsoft-Windows-Sysmon-Operational.evtz

使用工具：EvtzECmd、Timeline Explorer

工具参考：

- <https://ericzimmerman.github.io/#index.md>
- <https://github.com/EricZimmerman/evtz>
-

指令：

```
EvtzECmd.exe -f "C:\Users\TS0\Downloads\Microsoft-Windows-Sysmon-Operational.evtz" --csv "C:\Users\TS0\Downloads" --csvf MyOutputFile.csv
```

使用Timeline Explorer分析

Task 1

How many Event logs are there with Event ID 11?

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

MyOutputFile.csv

Drag a column header here to group by that column

Enter text to search... Find

Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel
2		2	118748	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
3		3	118749	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
5		5	118751	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
6		6	118752	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
8		8	118754	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
10		10	118756	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
15		15	118761	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
17		17	118763	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
37		37	118783	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
38		38	118784	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
72		72	118818	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
74		74	118820	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
80		80	118826	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
84		84	118830	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
86		86	118832	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
88		88	118834	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
90		90	118836	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
92		92	118838	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
94		94	118840	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win
96		96	118842	2024-02-14 03:4...	11	Info	Microsoft-Windows-Sysmon	Microsoft-Win

啟用 Windows
移至 [設定] 以啟用 Windows · Edit Filter

C:\Users\TSO\Downloads\MyOutputFile.csv

Total lines 169 | Visible lines 56 | Open files: 1 | Search options

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?

Line	Tag	Record Number	Event Record Id	Time Created	Payload Data4	Payload Data
54		54	118800	2024-02-14 03:41:57	ParentProcess: C:\Windows\System32\services.exe	ProcessID:
82		82	118828	2024-02-14 03:41:58	ParentProcess: C:\Windows\System32\msiexec.exe	ProcessID:
67		67	118813	2024-02-14 03:41:57	ParentProcess: C:\Users\CyberJunkie\Downloads\Preventivo24.02.14.exe.exe	ProcessID:
47		47	118793	2024-02-14 03:41:56	ParentProcess: C:\Windows\explorer.exe	ProcessID:
26		26	118772	2024-02-14 03:41:45	ParentProcess: C:\Program Files\Mozilla Firefox\firefox.exe	ProcessID:
59		59	118805	2024-02-14 03:41:57	ParentProcess: C:\Windows\System32\msiexec.exe	ProcessID:

啟用 Windows
移至 [設定] 以啟用 Windows · Edit Filter

C:\Users\TSO\Downloads\MyOutputFile.csv

Total lines 169 | Visible lines 6 | Open files: 1 | Search options

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
r	=	=	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

x

☒

Time Created

Is same day

2024-02-14 00:00:00

And

Payload Data4

Contains

QueryName:

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?

	Payload Data5
Y	CreationTimeUTC: 2024-01-14 08:10:06.029
	IsExecutable: False



x	<input checked="" type="checkbox"/> Payload Data4 Contains PDF And Time Created Is same day 2024-02-14 00:00:00
	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
=	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



		啟用 Windows 移至 [設定] 以啟用 Windows · Edit Fi
<input checked="" type="checkbox"/>	Payload Contains 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

nt Record Id	Time Created	Payload Data4
	=	nc
118782	2024-02-14 03:41:45	QueryName: d.dropbox.com
118747	2024-02-14 03:41:26	QueryName: uc2f030016253ec53f49539
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=

Timeline Explorer v2.0.0.1

FileToolsTabsViewHelp

MyOutputFile.csv

Enter text to search...Find

r	Event Record Id	Time Created	Payload Data4
T	=	=	📄
54	118800	2024-02-14 03:41:57	ParentProcess: C:\Windows\System32\services.exe
36	118782	2024-02-14 03:41:45	QueryName: d.dropbox.com
1	118747	2024-02-14 03:41:26	QueryName: uc2f030016253ec53f4953980a4e.dl.dropboxusercontent.com
160	118906	2024-02-14 03:41:58	QueryName: www.example.com
48	118794	2024-02-14 03:41:56	Signed: false
34	118780	2024-02-14 03:41:45	Signed: true
42	118788	2024-02-14 03:41:55	Signed: true
49	118795	2024-02-14 03:41:56	Signed: true
55	118801	2024-02-14 03:41:57	Signed: true
56	118802	2024-02-14 03:41:57	Signed: true
60	118806	2024-02-14 03:41:57	Signed: true
62	118808	2024-02-14 03:41:57	Signed: true
64	118810	2024-02-14 03:41:57	Signed: true
70	118816	2024-02-14 03:41:58	Signed: true
71	118817	2024-02-14 03:41:58	Signed: true
77	118823	2024-02-14 03:41:58	Signed: true
78	118824	2024-02-14 03:41:58	Signed: true
79	118825	2024-02-14 03:41:58	Signed: true
147	118893	2024-02-14 03:41:58	Signed: true
27	118773	2024-02-14 03:41:45	SourceImage: C:\Program Files\Mozilla Firefox\firefox.exe
164	118910	2024-02-14 03:41:58	SourceIp: 172.17.79.132

QueryResults: ::ffff:93.184.216.34;199.43.135.53;2001:500:8f::53;199.43.133.53;2001:500:8d::53;

TargetImage: C:\Program Files\Mozilla Firefox\pingsender.exe

DestinationIp: 93.184.216.34

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

☒ [Event Id = 5] ▾

ATCSDemo - DAM - Out - File ...

2024-02-14 03:41:58