

附件 5.資安應處事中處理工具說明

1.利用 Msert(微軟掃毒軟體)找出惡意檔案

下載連結 <https://docs.microsoft.com/zh-tw/windows/security/threat-protection/intelligence/safety-scanner-download> 根據 32 位元或是 64 位元選擇下載，工具使用期限為 10 天，超過 10 天需重新下載。

Microsoft 安全掃描工具

發行項 • 2022/01/25 • 1 位參與者



Microsoft 安全掃描工具是一種掃描工具，設計來尋找並移除 Windows 電腦中的惡意程式碼。只要下載，然後執行掃描就可尋找惡意程式碼，並嘗試還原由發現的威脅所做的變更。

- [下載 Microsoft 安全掃描工具 \(32-位元\)](#)
- [下載 Microsoft 安全掃描工具 \(64-位元\)](#)

圖 1 Msert 介紹

下載後在同資料夾開啟 cmd 輸入：`MSERT.exe /N /F` 參數意義如下：`N`:僅偵測不刪除；`F`:完整掃描，掃描完畢後在 `C:\Windows\debug\msert.log` 查看是否有異常，掃描完畢後在 `C:\Windows\debug\msert.log` 查看是否異常，若 code 代碼非 0 則為異常。

Results Summary:

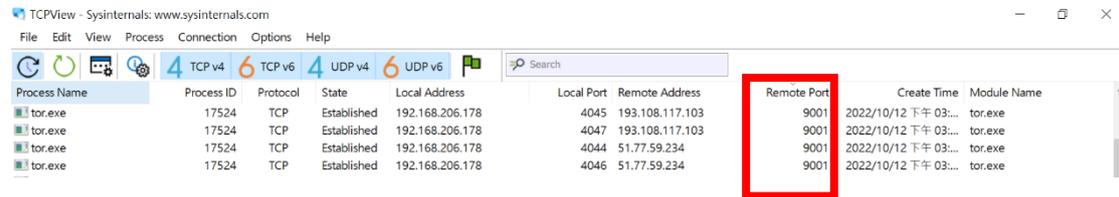
Found Trojan:Win32/Meterpreter.0, not removed.
Microsoft Safety Scanner Finished On Sun Oct 18 17:11:30 2020

Return code: 7 (0x7)

圖 2 Msert log

2.使用 TCPView 查看是否有可疑的程式建立連線

觀察建立的連線發起的程式是否有印象，或是 Port Number >9000 有可能為暗網之洋蔥路由。



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
tor.exe	17524	TCP	Established	192.168.206.178	4045	193.108.117.103	9001	2022/10/12 下午 03:...	tor.exe
tor.exe	17524	TCP	Established	192.168.206.178	4047	193.108.117.103	9001	2022/10/12 下午 03:...	tor.exe
tor.exe	17524	TCP	Established	192.168.206.178	4044	51.77.59.234	9001	2022/10/12 下午 03:...	tor.exe
tor.exe	17524	TCP	Established	192.168.206.178	4046	51.77.59.234	9001	2022/10/12 下午 03:...	tor.exe

圖 3 TCPView 查看是否有可疑的程式建立連線

3.使用 Process Explorer 查看是否有可疑的程式正在執行

使用 AutoRuns 查看惡意程式是否跟著開機一起被執行，開啟後點選「Logon」頁籤，Options > Scan Options > 勾選 Verify code signatures、Check VirusTotal(千萬不要勾 Submit Images)。

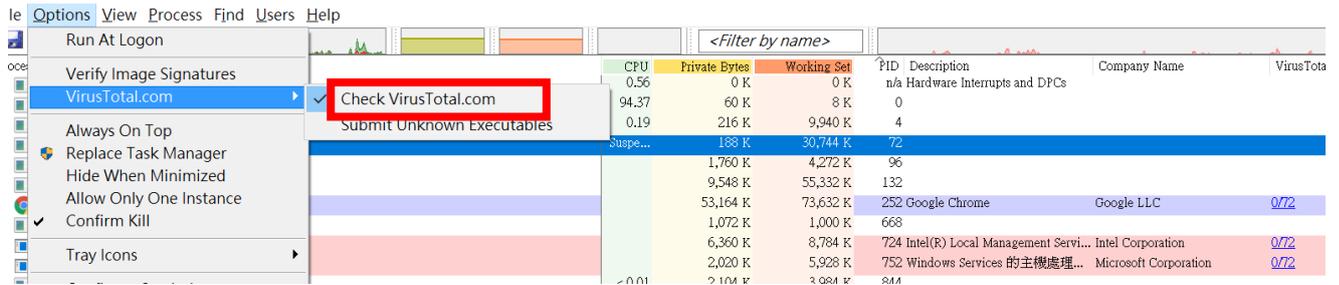
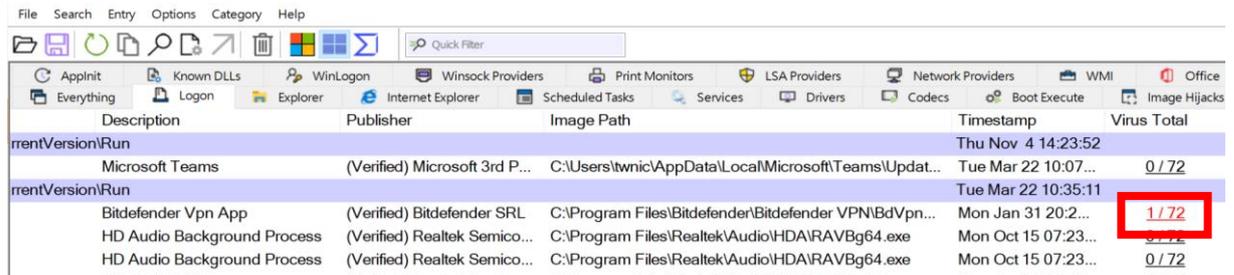


圖 4 Process Explorer 查看疑似惡意程式的方式

4.AutoRuns 識別惡意程式

使用 Process Explorer 查看執行中的程式是否包含惡意程式，
Options >VirusTotal.com>Check VirusTotal.com(不要 Submit unknown Executables)。



Description	Publisher	Image Path	Timestamp	Virus Total
Microsoft Teams	(Verified) Microsoft 3rd P...	C:\Users\twnic\AppData\Local\Microsoft\Teams\Updat...	Tue Mar 22 10:07...	0/72
Bitdefender Vpn App	(Verified) Bitdefender SRL	C:\Program Files\Bitdefender\Bitdefender VPN\BdVpn...	Mon Jan 31 20:2...	1/72
HD Audio Background Process	(Verified) Realtek Semico...	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	Mon Oct 15 07:23...	0/72
HD Audio Background Process	(Verified) Realtek Semico...	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	Mon Oct 15 07:23...	0/72

圖 5 AutoRuns 查看疑似惡意程式的方法

5.勒索軟體大量讀寫判斷

勒索軟體加密步驟是：讀取資料>加密資料>寫回硬碟，因此勒索軟體會對硬碟有大量的讀取與寫入。透過開啟系統管理員>詳細資料>右鍵選取欄位>I/O 讀寫位元，若發現 I/O 讀寫位元相當大讀取也差不多，若發現此症狀盡速點選「結束處理程序樹狀目錄」。

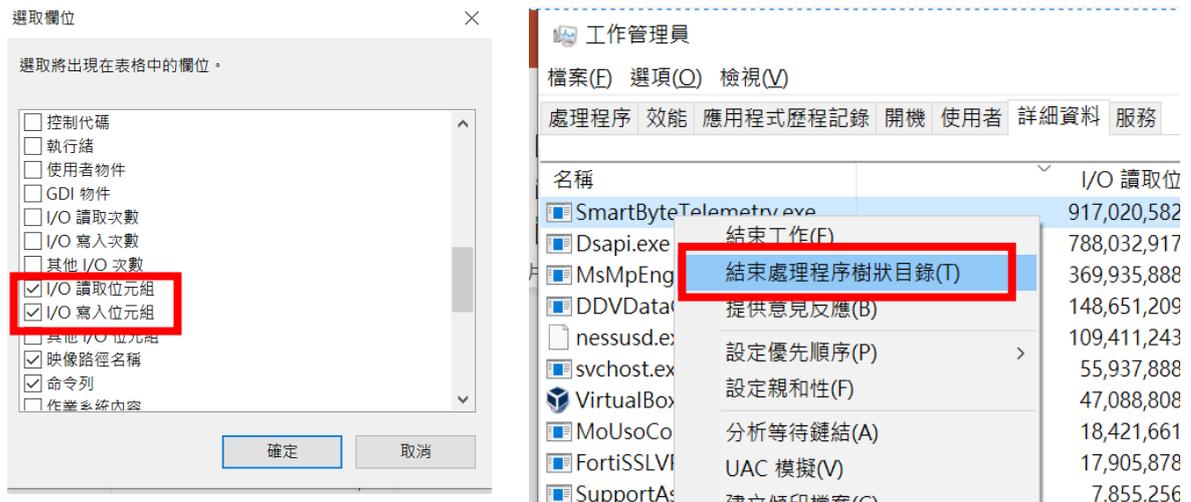
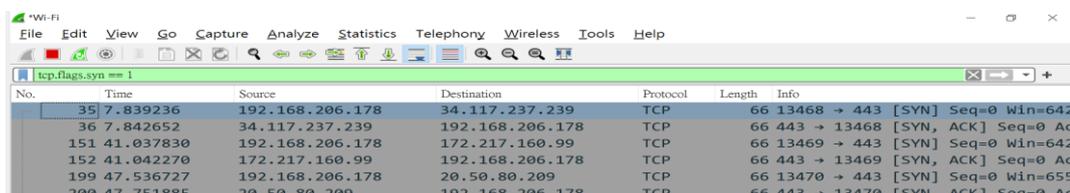


圖 6 I/O 讀寫與結束樹狀目錄

6.使用 Wireshark 找出 DDoS 的症狀

- (1) 檢視連線紀錄封包，是否有收到大量 SYN 封包 `tcp.flags.syn == 1`

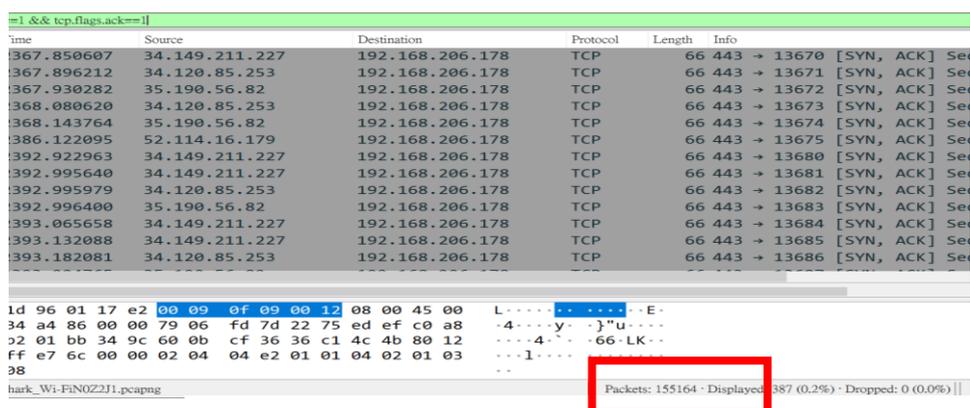


The screenshot shows a Wireshark interface with a packet list table. The filter is `tcp.flags.syn == 1`. The table contains several rows of captured packets, all of which are SYN packets.

No.	Time	Source	Destination	Protocol	Length	Info
35	7.839236	192.168.206.178	34.117.237.239	TCP	66	13468 → 443 [SYN] Seq=0 win=642
36	7.842652	34.117.237.239	192.168.206.178	TCP	66	443 → 13468 [SYN, ACK] Seq=0 Ac
151	41.037830	192.168.206.178	172.217.160.99	TCP	66	13469 → 443 [SYN] Seq=0 win=642
152	41.042270	172.217.160.99	192.168.206.178	TCP	66	443 → 13469 [SYN, ACK] Seq=0 Ac
199	47.536727	192.168.206.178	20.50.80.209	TCP	66	13470 → 443 [SYN] Seq=0 win=655
200	47.751885	20.50.80.209	192.168.206.178	TCP	66	443 → 13470 [SYN, ACK] Seq=0 Ac

圖 7 使用 Wireshark 檢查 SYN 封包數量

- (2) 比較 SYN 與 SYN/ACK 是否有大量的差距，不完整的三向交握透過指令 `tcp.flags.syn==1 && tcp.flags.ack==0` 找出 SYN 數量；`tcp.flags.syn==1 && tcp.flags.ack==0` 找出 SYN/ACK 數量。觀察右下角數量差距

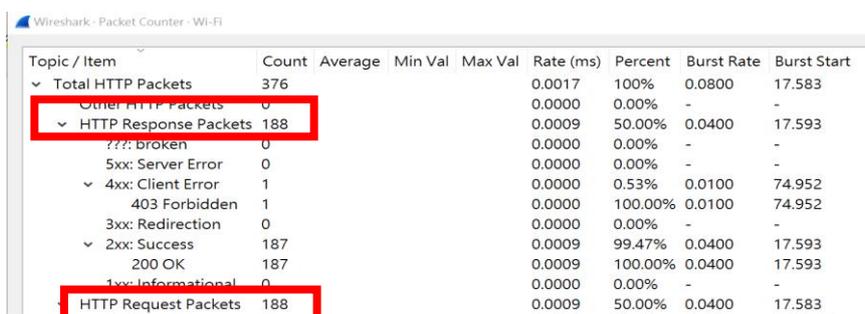


The screenshot shows a Wireshark interface with a packet list table. The filter is `tcp.flags.syn==1 && tcp.flags.ack==0`. The table contains several rows of captured packets, all of which are SYN packets. The status bar at the bottom right shows "Packets: 155164 · Displayed: 387 (0.2%) · Dropped: 0 (0.0%)".

Time	Source	Destination	Protocol	Length	Info
367.850607	34.149.211.227	192.168.206.178	TCP	66	443 → 13670 [SYN, ACK] Seq=0
367.896212	34.120.85.253	192.168.206.178	TCP	66	443 → 13671 [SYN, ACK] Seq=0
367.930282	35.190.56.82	192.168.206.178	TCP	66	443 → 13672 [SYN, ACK] Seq=0
368.080620	34.120.85.253	192.168.206.178	TCP	66	443 → 13673 [SYN, ACK] Seq=0
368.143764	35.190.56.82	192.168.206.178	TCP	66	443 → 13674 [SYN, ACK] Seq=0
386.122095	52.114.16.179	192.168.206.178	TCP	66	443 → 13675 [SYN, ACK] Seq=0
392.922963	34.149.211.227	192.168.206.178	TCP	66	443 → 13680 [SYN, ACK] Seq=0
392.995640	34.149.211.227	192.168.206.178	TCP	66	443 → 13681 [SYN, ACK] Seq=0
392.995979	34.120.85.253	192.168.206.178	TCP	66	443 → 13682 [SYN, ACK] Seq=0
392.996400	35.190.56.82	192.168.206.178	TCP	66	443 → 13683 [SYN, ACK] Seq=0
393.065658	34.149.211.227	192.168.206.178	TCP	66	443 → 13684 [SYN, ACK] Seq=0
393.132088	34.149.211.227	192.168.206.178	TCP	66	443 → 13685 [SYN, ACK] Seq=0
393.182081	34.120.85.253	192.168.206.178	TCP	66	443 → 13686 [SYN, ACK] Seq=0

圖 8 使用 Wireshark 比較 SYN 與 ACK 數量

- (3) 觀察 HTTP Request 與 Response 的數量，一般情況兩者應差距不大。點選上方「Statistics」→「HTTP」→「Packet Counter」可開啟統計頁面



The screenshot shows the Wireshark Packet Counter window. The table displays statistics for HTTP packets. The "HTTP Response Packets" and "HTTP Request Packets" are highlighted with red boxes.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	376				0.0017	100%	0.0800	17.583
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	188				0.0009	50.00%	0.0400	17.593
HTTP Request Packets	188				0.0009	50.00%	0.0400	17.583

圖 9 使用 Wireshark 觀察 Request 與 Response 的數量