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。

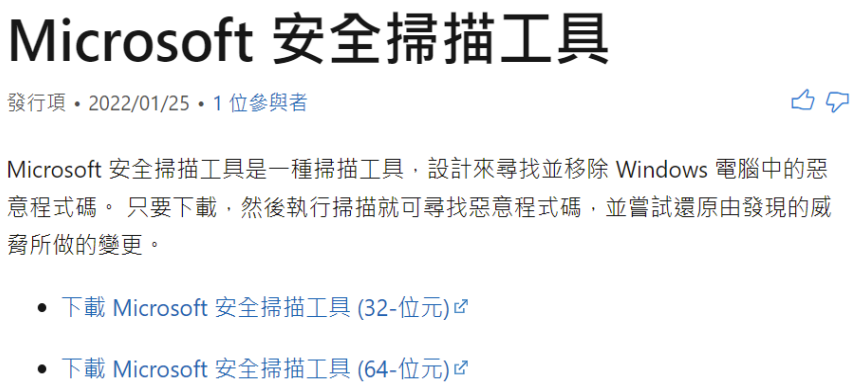

圖 1 Msert 介紹

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.O, 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。

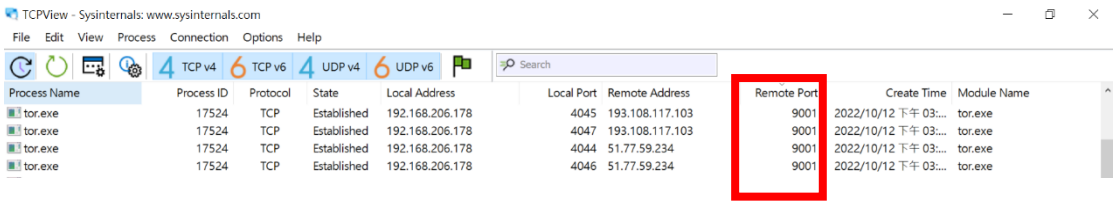

圖 3 TCPView 查看是否有可疑的程式建立連線

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)。

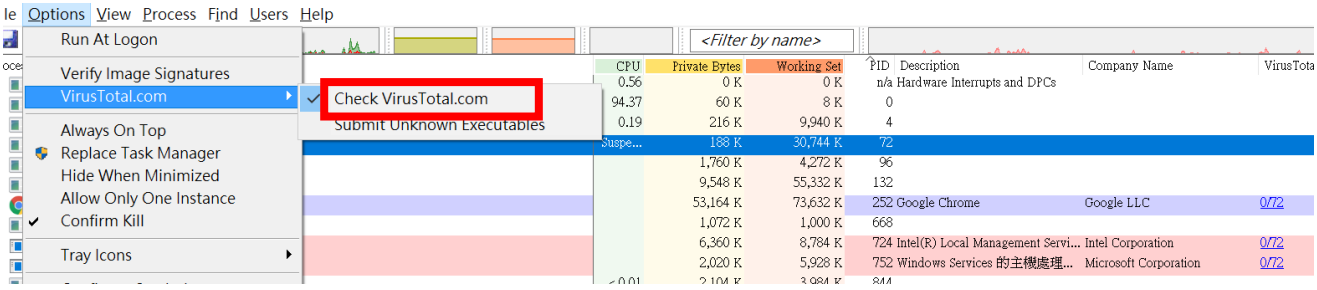

圖 4 Process Explorer 查看疑似惡意程式的方式

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)。

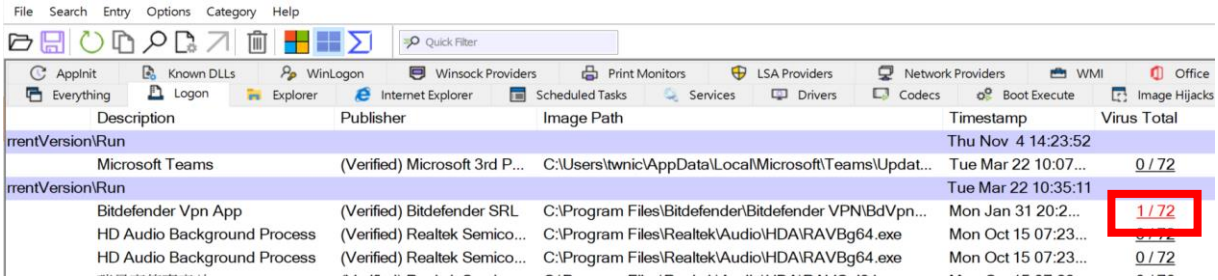

圖 5 AutoRuns 查看疑似惡意程式的方法

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」。

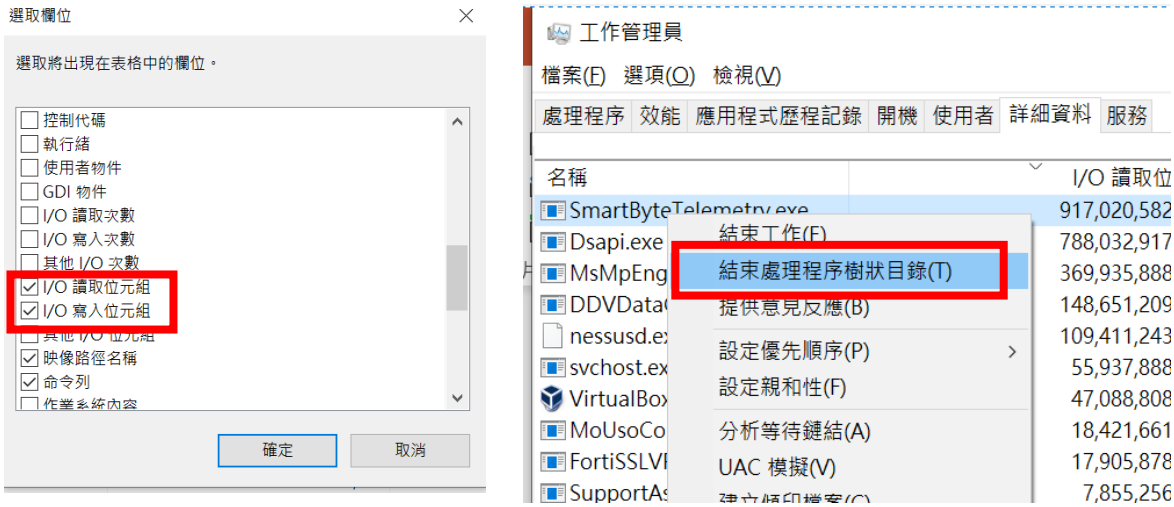

圖 6 I/O 讀寫與結束樹狀目錄

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

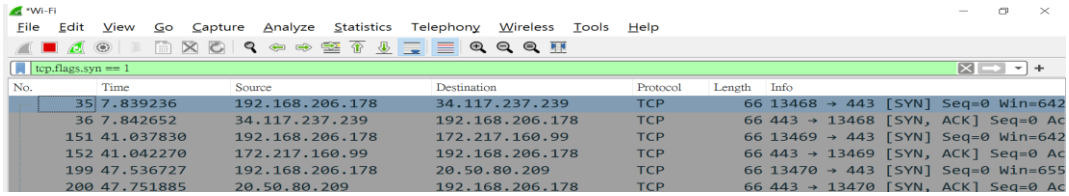

圖 7 使用 Wireshark 檢查 SYN 封包數量

(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

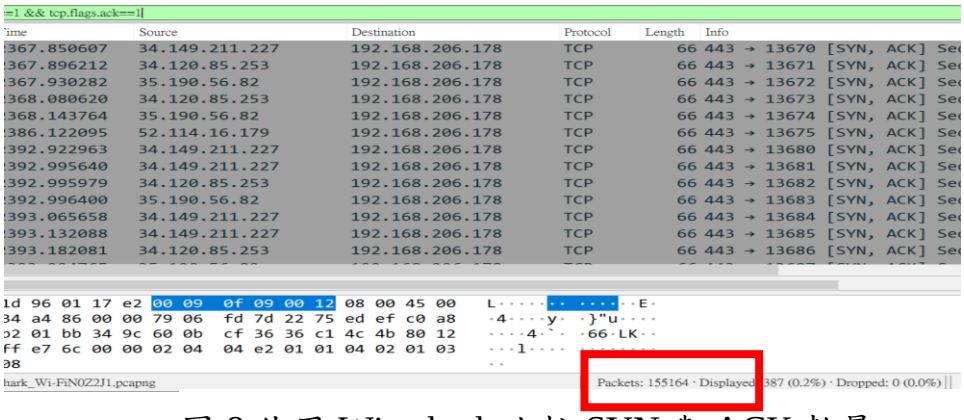

圖 8 使用 Wireshark 比較 SYN 與 ACK 數量

(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

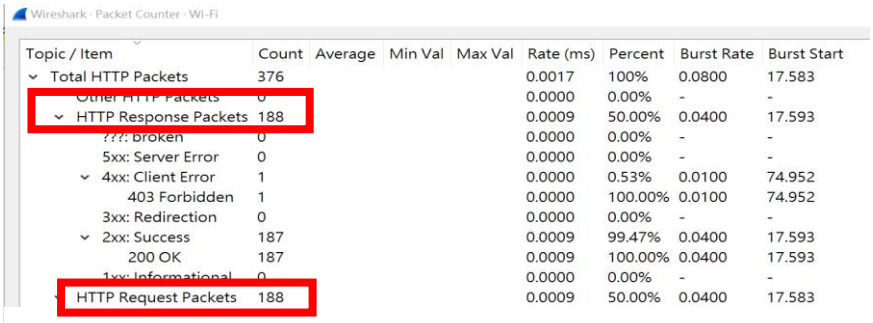

圖 9 使用 Wireshark 觀察 Request 與 Response 的數量