個案分析-

校園主機感染 WannaCry 病毒事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

106 年 6 月

I. 事件簡介

1. 在今年 5 月中旬爆發 WannaCry 病毒利用 Windows 系統的 SMB 漏洞，透過 TCP445 連接埠來傳播，進行大規模攻擊未更新 Windows 系統的電腦。
2. 本事件為 S 大學之校內一台測試主機發生疑似惡意程式連線行為，對外進行大量 445 連接埠的連線。
3. 該主機為測試用的虛擬主機，所安裝的系統為 Windows Server 2008 R2 系統，而且自今年 3 月初過後關機至今年 5 月 17 日才再次開機。
4. 本單位取得該虛擬主機的樣本後，以還原系統的方式進行研究分析。

II. 事件檢測

1. 首先我們將已感染中毒的虛擬主機在 VM 環境內還原，並執行檢測工具來觀察其程式行為與其對外網路行為。此外，也準備一台 Windows 7 系統的待感染主機，來觀察其病毒感染途徑與網路行為，檢測環境如圖 1 所示。

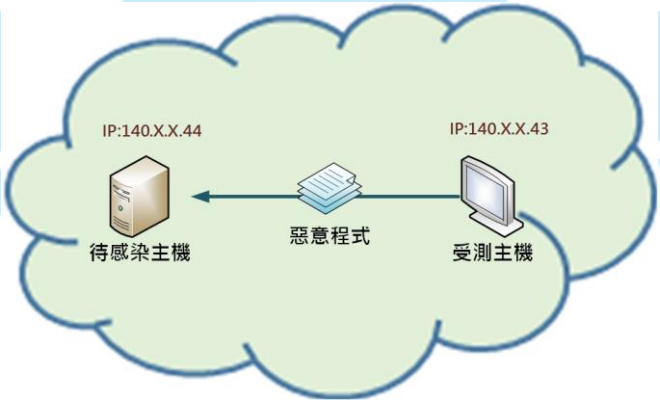


圖 1:檢測環境示意圖

2. 以 Nmap 工具檢視受測主機對外的連接埠資訊，發現 135、445、3389、49154 等連接埠為開啟狀態(如圖 2)。

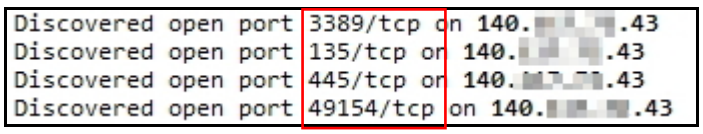


圖 2:受檢測主機對外開啟的連接埠資訊

3. 透過 Currports 工具發現有一個執行中的程式 mssecsvc.exe，正在產生大量對外連線 445 連接埠行為，嘗試對外進行連線攻擊(如圖 3)。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State	Process Path
svchost.exe	768	TCP	49153	::		::	Listening	C:\Windows\System32\svchost.exe
svchost.exe	812	TCP	49154	::		::	Listening	C:\Windows\System32\svchost.exe
System	4	TCP	47001	0.0.0.0		0.0.0.0	Listening	System
System	4	TCP	47001	::		::	Listening	System
wininit.exe	396	TCP	49152	0.0.0.0		0.0.0.0	Listening	C:\Windows\System32\wininit.exe
wininit.exe	396	TCP	49152	::		::	Listening	C:\Windows\System32\wininit.exe
svchost.exe	956	UDP	57851	0.0.0.0				C:\Windows\System32\svchost.exe
mssecsvc.exe	1104	TCP	51286	140.[redacted].43	445	92.149.107.15	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51287	140.[redacted].43	445	48.149.193.76	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51288	140.[redacted].43	445	61.76.48.20	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51290	140.[redacted].43	445	68.146.33.5	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51298	140.[redacted].43	445	214.254.212.56	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51302	140.[redacted].43	445	184.14.167.141	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51304	140.[redacted].43	445	94.89.108.205	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51305	140.[redacted].43	445	60.210.138.175	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51308	140.[redacted].43	445	104.133.190.36	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51313	140.[redacted].43	445	40.239.116.238	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51318	140.[redacted].43	445	100.254.120.227	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51325	140.[redacted].43	445	81.65.174.129	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51327	140.[redacted].43	445	1.199.242.100	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51330	140.[redacted].43	445	113.208.185.162	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51333	140.[redacted].43	445	35.65.19.101	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51334	140.[redacted].43	445	164.41.72.132	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51335	140.[redacted].43	445	5.46.229.131	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51338	140.[redacted].43	445	165.107.58.239	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51346	140.[redacted].43	445	79.132.16.105	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51360	140.[redacted].43	445	93.234.26.147	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51368	140.[redacted].43	445	189.124.110.117	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51372	140.[redacted].43	445	189.131.20.171	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51379	140.[redacted].43	445	118.136.34.197	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51386	140.[redacted].43	445	140.99.64.148	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51388	140.[redacted].43	445	109.246.168.199	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51389	140.[redacted].43	445	181.39.29.161	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51392	140.[redacted].43	445	126.105.152.180	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51394	140.[redacted].43	445	198.31.106.69	Syn-Sent	C:\WINDOWS\mssecsvc.exe

圖 3:mssecsvc.exe 對外連線 445 連接埠行為側錄

4. 透過 procexp 與 procmon 工具檢視背景程式狀態，發現程式 mssecsvc.exe 執行時會啟動另一個程式 tasksche.exe(如圖 4)。

mssecsvc.exe (4516)	Microsoft® Disk Defragmenter	C:\Windows\mssecsvc.exe
tasksche.exe (8056)		C:\WINDOWS\tasksche.exe
mssecsvc.exe (8108)	Microsoft® Disk Defragmenter	C:\Windows\mssecsvc.exe
tasksche.exe (13232)		C:\WINDOWS\tasksche.exe
mssecsvc.exe (8176)	Microsoft® Disk Defragmenter	C:\Windows\mssecsvc.exe
tasksche.exe (13276)		C:\WINDOWS\tasksche.exe

圖 4: mssecsvc.exe 執行時啟動 tasksche.exe 的紀錄截圖

5. 查看程式 mssecsvc.exe 與 tasksche.exe 的內容，發現此兩個執行檔的建立日期皆為 106 年 5 月 17 日 11:07(如圖 5)，推測可能為受測主機感染病毒的時間點。

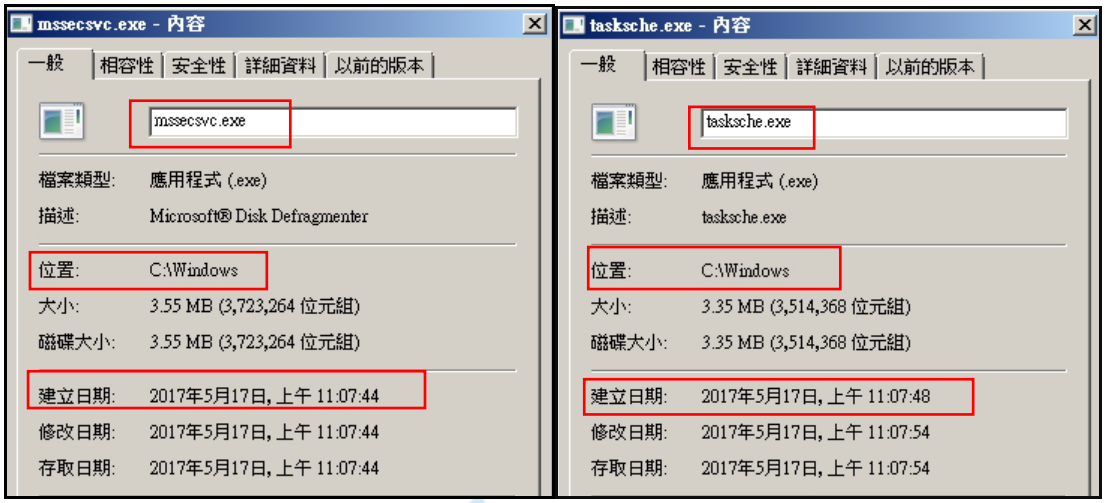


圖 5:程式 mssecsvc.exe 與 tasksche.exe 在系統內的建立時間截圖

6. 由事件檢視紀錄，發現到兩程式 mssecsvc.exe 與 tasksche.exe 在建立時只有 mmsecsvc.exe 成功執行(如圖 6)，而程式 tasksche.exe 啟用失敗，並且發生不正確的 XML 語法錯誤(如圖 7)。

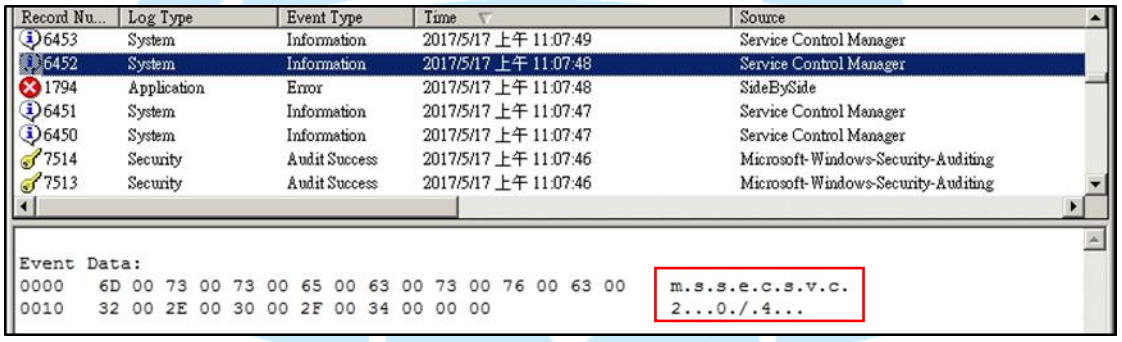


圖 6:在 11 時 7 分系統執行 mssecsvc.exe 成功的紀錄

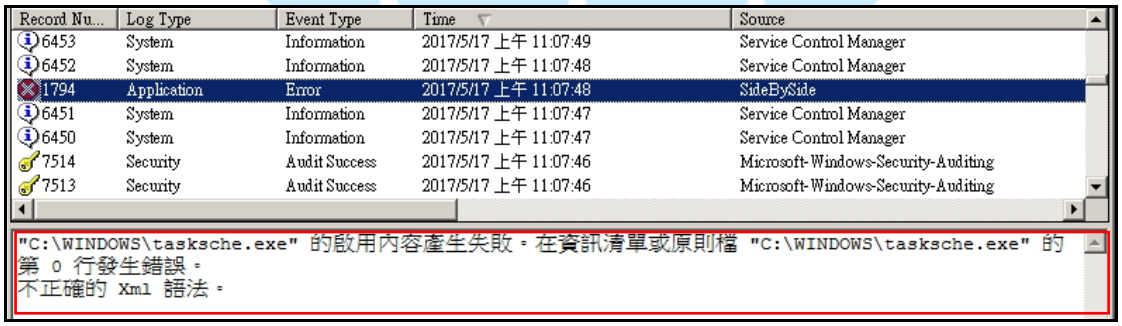


圖 7:在 11 時 7 分系統執行 tasksche.exe 啟動失敗的紀錄

7. 因為受測主機存在 mssecsvc.exe 與 tasksche.exe 兩程式，又有大量以 445 連接埠對外連線攻擊的行為，因此推斷受測主機可能感染到 WannaCry 病毒。接著搜尋主機內是否存在該病毒特徵:tasksche.exe 執行後會產生的三個檔

案(@WanaDecryptor@.exe、Taskdk.exe 與 Taskdl.exe)，結果無法搜尋到，可能與 tasksche.exe 無法被成功開啟有關。

8. 從封包內容檢視，經觀察程式 mssecsvc.exe 於執行初期，會嘗試對網域名稱伺服器(DNS)發出網域名稱解析請求，網域名稱為 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com(如圖 8)。

Time	Source	Destination	Protocol	Length	Info
40 34.304588	140.[redacted].43	140.[redacted].1	DNS	109	Standard query 0x8bee A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
41 34.304593	140.[redacted].43	140.[redacted].1	DNS	109	Standard query 0x8bee A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
42 34.316426	140.[redacted].1	140.[redacted].43	DNS	549	Standard query response 0x8bee A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea

圖 8:受測主機向網域名稱伺服器(DNS)發出請求網域名稱之紀錄

9. 檢視封包內容與對程式 mssecsvc.exe 進行逆向工程，發現 mssecsvc.exe 會檢查 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 網址是否可以連線，若無法連線會繼續進行後續程式行為，判斷該網址為一個 Kill-Switch 的網址(如圖 9、圖 10 與圖 11)。

```
sub     esp, 50h
push    esi
push    edi
mov     ecx, 0Eh
mov     esi, offset aHttpWww_iuqerf ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
lea     edi, [esp+58h+szUrl]
xor     eax, eax
rep movsd
```

```
aHttpWww_iuqerf db 'http://www.iuqerfsodp9ifjaposdfjhgo'
db 'surijfaewrwergwea.com',0
```

圖 9:mssecsvc.exe 之逆向工程內容中連結 Kill-Switch 網址的佐證資訊

其中圖 10 為 DNS 回覆給受測主機 Kill-Switch 網址的網域名稱解析內容，共對應到 5 台主機的 IP 位址，第一台主機為 104.17.37.137。

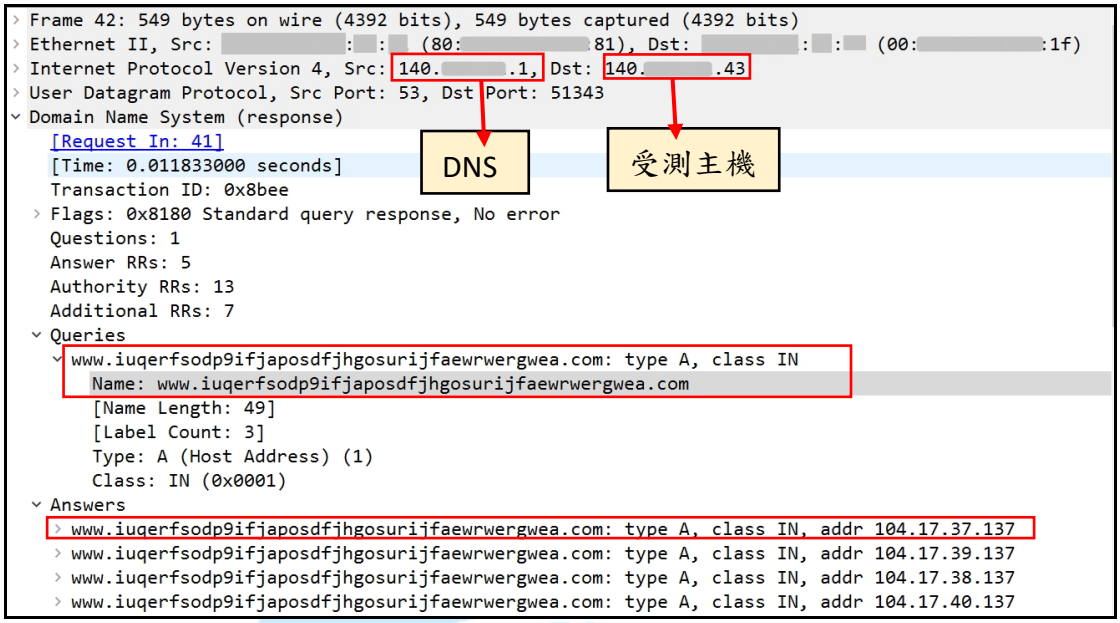


圖 10: DNS 回覆受測主機所查詢的網域名稱之紀錄

圖 11 為受測主機 140.x.x.43 連線到 Kill-Switch 網址的主機 104.17.37.137 之封包來往紀錄，由圖中可以判斷有成功連線。

No.	Time	Source	Destination	Protocol	Length	Info
43	35.553016	140. .43	104.17.37.137	TCP	66	49156 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
44	35.553021	140. .43	104.17.37.137	TCP	66	[TCP Out-Of-Order] 49156 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
45	35.579111	104.17.37.137	140. .43	TCP	66	80 → 49156 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PE
46	35.579454	140. .43	104.17.37.137	TCP	54	49156 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
47	35.579458	140. .43	104.17.37.137	TCP	54	[TCP Dup ACK 46#1] 49156 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
48	35.616897	140. .43	104.17.37.137	HTTP	154	GET / HTTP/1.1
49	35.616901	140. .43	104.17.37.137	TCP	154	[TCP Retransmission] 49156 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 L
50	35.643682	104.17.37.137	140. .43	TCP	60	80 → 49156 [ACK] Seq=1 Ack=101 Win=29696 Len=0
51	36.283530	104.17.37.137	140. .43	TCP	516	[TCP segment of a reassembled PDU]
52	36.283531	104.17.37.137	140. .43	HTTP	60	HTTP/1.1 200 OK (text/html)
53	36.283532	104.17.37.137	140. .43	TCP	60	80 → 49156 [FIN, ACK] Seq=468 Ack=101 Win=29696 Len=0
54	36.283978	140. .43	104.17.37.137	TCP	54	49156 → 80 [ACK] Seq=101 Ack=469 Win=65024 Len=0
55	36.283983	140. .43	104.17.37.137	TCP	54	[TCP Dup ACK 54#1] 49156 → 80 [ACK] Seq=101 Ack=469 Win=65024 Len=
56	36.339250	140. .43	104.17.37.137	TCP	54	49156 → 80 [FIN, ACK] Seq=101 Ack=469 Win=65024 Len=0
57	36.339254	140. .43	104.17.37.137	TCP	54	[TCP Out-Of-Order] 49156 → 80 [FIN, ACK] Seq=101 Ack=469 Win=65024
58	36.339393	140. .43	104.17.37.137	TCP	54	49156 → 80 [RST, ACK] Seq=102 Ack=469 Win=0 Len=0
59	36.339396	140. .43	104.17.37.137	TCP	54	49156 → 80 [RST, ACK] Seq=102 Ack=469 Win=0 Len=0
60	36.364724	104.17.37.137	140. .43	TCP	60	80 → 49156 [ACK] Seq=469 Ack=102 Win=29696 Len=0

圖 11:受測主機連線至 DNS 所回覆的網站 IP 位址 (104.17.37.137)之封包紀錄

10. 以 Nmap 工具檢視 Kill-Switch 網址所對應主機 104.17.37.137 對外的連接埠資訊，發現 443、80、8080、8443 等連接埠為開啟狀態(如圖 12)，表示該網址目前的 80 連接埠是可連線的。

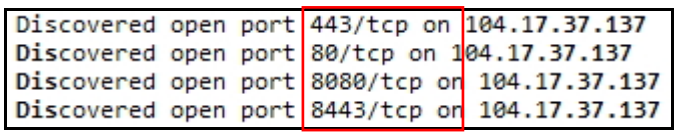


圖 12:104.17.37.137 主機對外開啟的連接埠資訊

11. 檢視受測主機連到 Kill-Switch 網址後的封包內容，發現該網頁內容無法被正常顯示(如圖 13)，可見該網址只是單純作為程式判斷是否可以連線的用途。

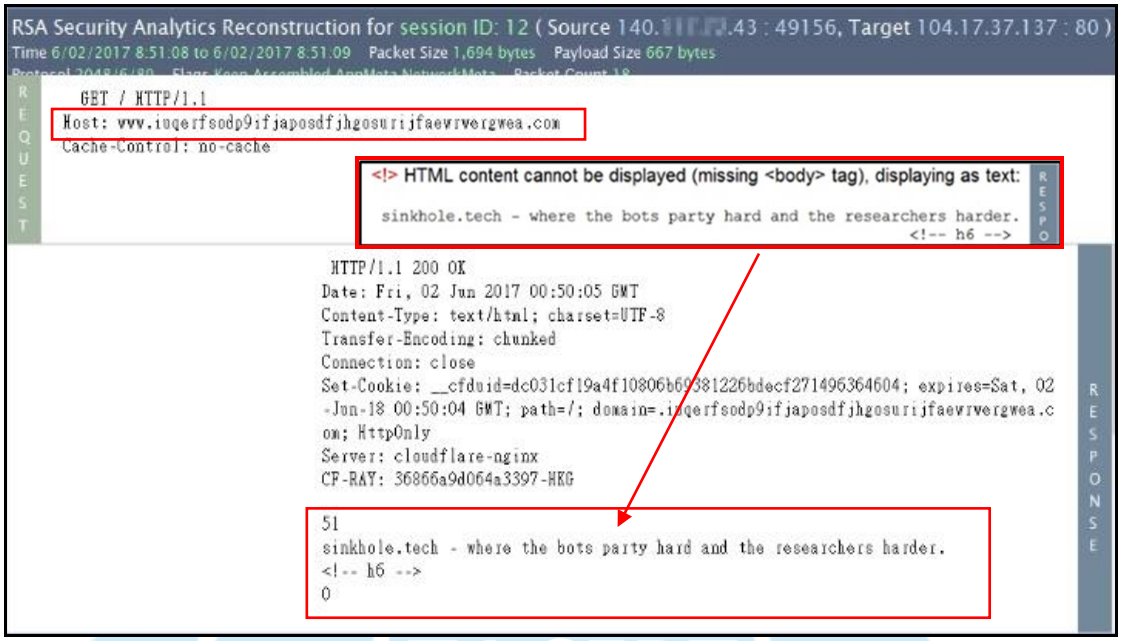


圖 13:受測主機連到 Kill-Switch 網址的封包解析內容

12. 將 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 網址送到 Virustotal 檢測是否為惡意網站，檢測比率為 2/65，為「非惡意網站」的比例相當高，表示該網站目前是安全網站（如圖 14）。

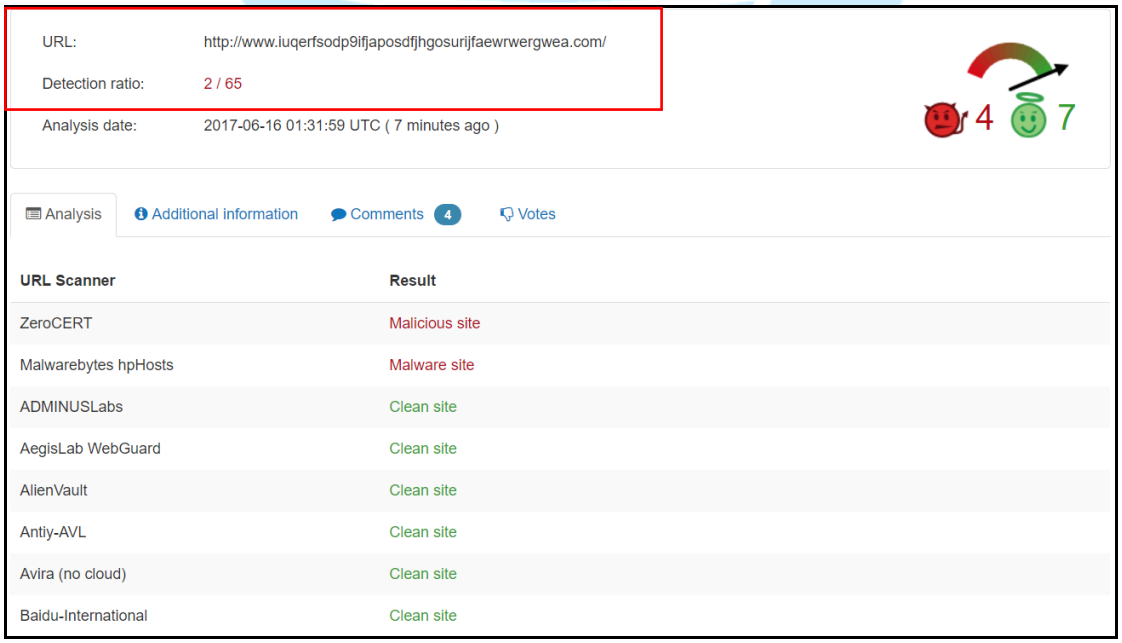


圖 14:www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 網址於 Virustotal 網站的檢測結果

13. 從該主機在開機 7 小時的短暫測試期間內，至少對外進行 69 萬 7,488 次 445 連接埠攻擊(如圖 15)，若以國別來分有 232 個國家受影響(如圖 16)，可見其散播速度之快與影響範圍之大。

圖 15:受測主機對外連線 445port 的連線數量統計

圖 16:受測主機對外連線 445port 的受影響國家數量統計

14. 將程式樣本 mssecsvc.exe 送到 Virustotal 檢測，檢測為惡意的比例為 57/61 相當明顯(如圖 17)，但仍然有 4 家防毒公司的軟體尚未檢測出其為惡意程式。(如圖 18)。

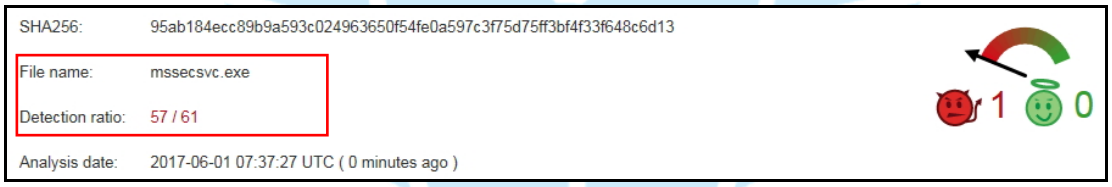


圖 17: mssecsvc.exe 於 Virustotal 網站的檢測結果

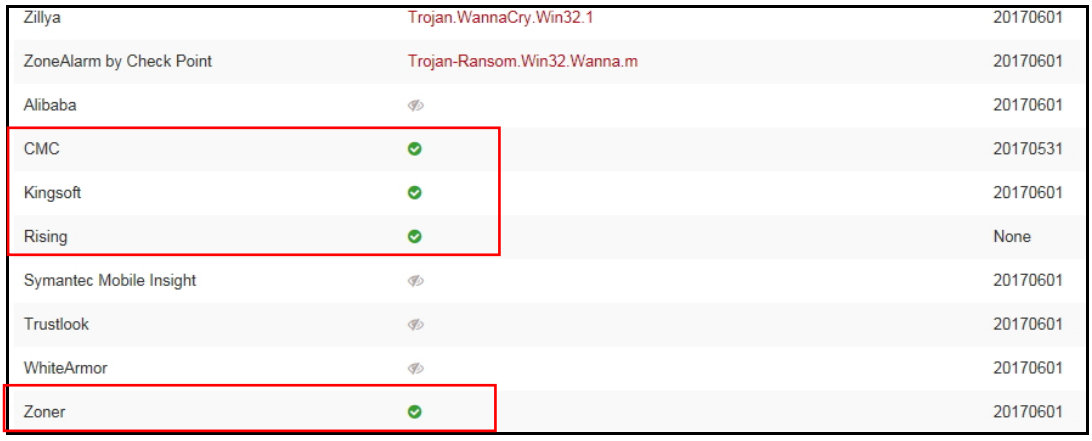


圖 18: 無法檢測出惡意程式 mssecsvc.exe 的防毒公司名單

15. 另一支程式 tasksche.exe 透過 Virustotal 檢測，檢出比例為 55/61 相當高（如圖 19），但有 6 家防毒公司的軟體尚未檢測出其為惡意程式(如圖 20)。

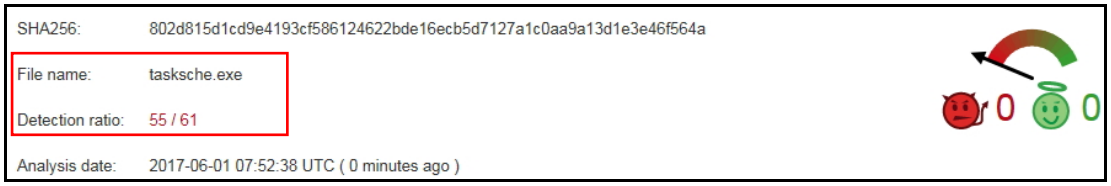


圖 19: tasksche.exe 於 Virustotal 網站的檢測結果

Zoner	Trojan.Wanna	20170601
Alibaba		20170601
CMC	✓	20170531
Invincea	✓	20170519
Kingsoft	✓	20170601
Rising	✓	None
SUPERAntiSpyware	✓	20170601
Symantec Mobile Insight		20170601
Trustlook		20170601
VBA32	✓	20170531
WhiteArmor		20170601

圖 20: 無法檢測出惡意程式 tasksche.exe 的防毒公司名單

16. 觀察待感染主機發現，當受測主機對外進行 445 port 連線時，會用匿名連線方式與待感染主機建立連線(如圖 21)，之後兩個程式 mssecsvc.exe 與 tasksche.exe 開始安裝與執行(如圖 22 與圖 23)，經與受測主機的事件檢視紀錄比對，發現受測主機與待感染主機兩者行為相同。

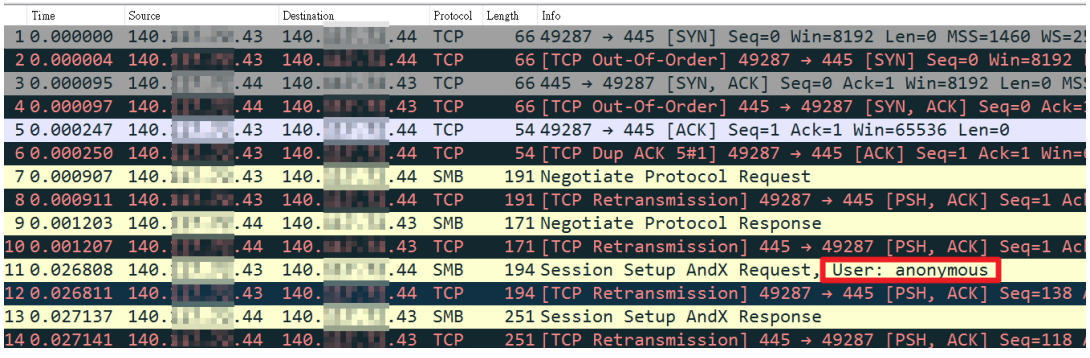


圖 21:受測主機以匿名連線方式連入待感染主機的封包側錄

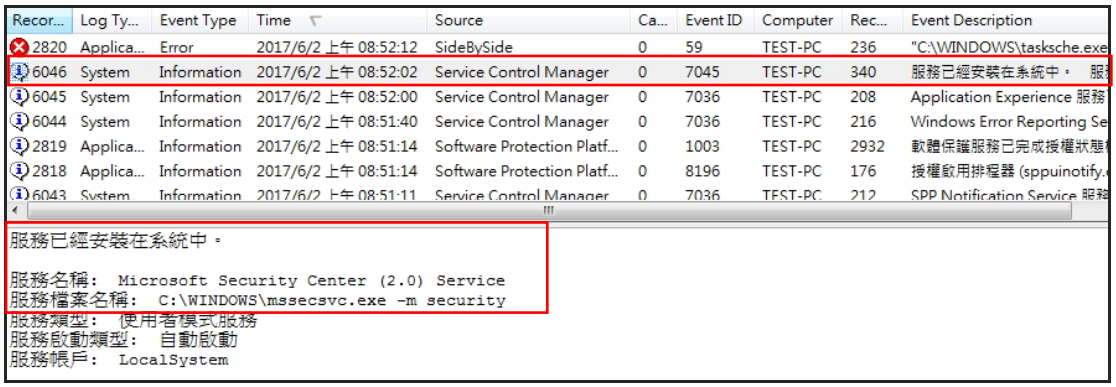
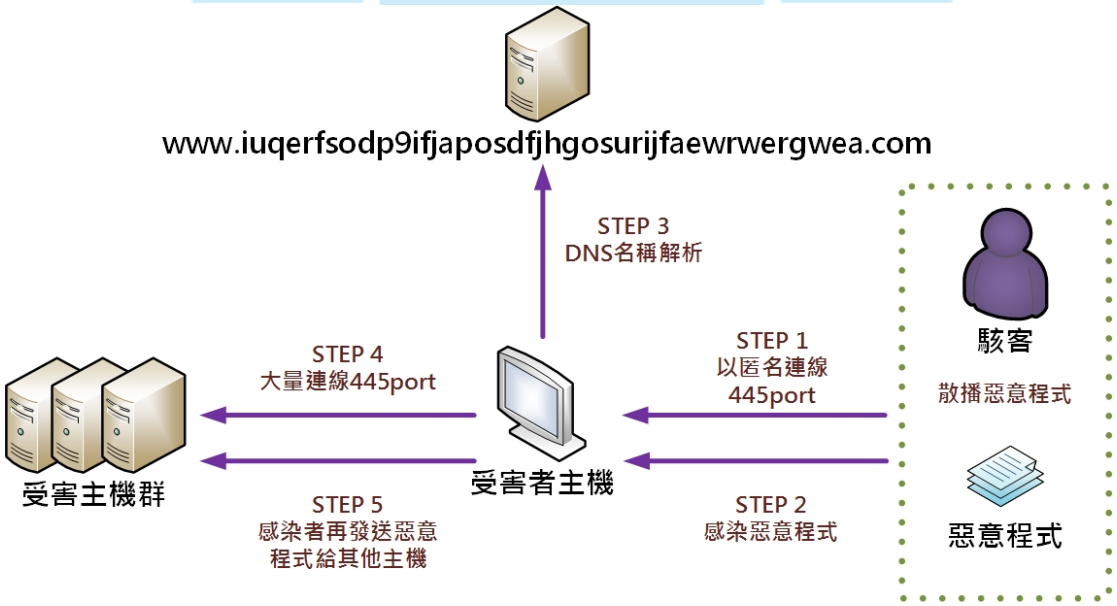


圖 22:mssecsvc.exe 安裝於待感染主機的事件紀錄

圖 23:taskche.exe 在待感染主機內啟用失敗的事件紀錄

III. 網路架構圖



1. 駭客散播惡意程式，以匿名方式 445port 連線受害者主機。
2. 植入惡意程式 mssecsvc.exe 於受害主機，該程式會呼叫與執行另一個惡意程式 tasksche.exe。

3. mssecsvc.exe 進行 DNS 名稱解析。
4. 受害者主機對外進行大量 445 port 攻擊。
5. 受害者主機植入惡意程式到受感染主機。

IV.建議與總結

此個案為電腦未執行系統更新來修補 SMB 漏洞，而被駭客透過開啟的 445 port 植入惡意程式。為有效預防感染 WannaCry 病毒，建議使用者進行下列的防禦措施:

1. 關閉 Windows 系統的 445 通訊埠。
2. 立即使用隨身碟、外接硬碟或者雲端空間，備份重要資料。
3. 使用 Windows Update 自動更新或手動更新微軟 KB4012215 的漏洞修補程式(漏洞編號 MS17-010)。
4. 確認防毒軟體已更新至最新版本病毒碼與偵測程式碼，並定期執行電腦掃毒作業。

V. 相關報導

1. http://www.ithome.com.tw/news/114144

2. http://www.ithome.com.tw/news/114148