個案分析-

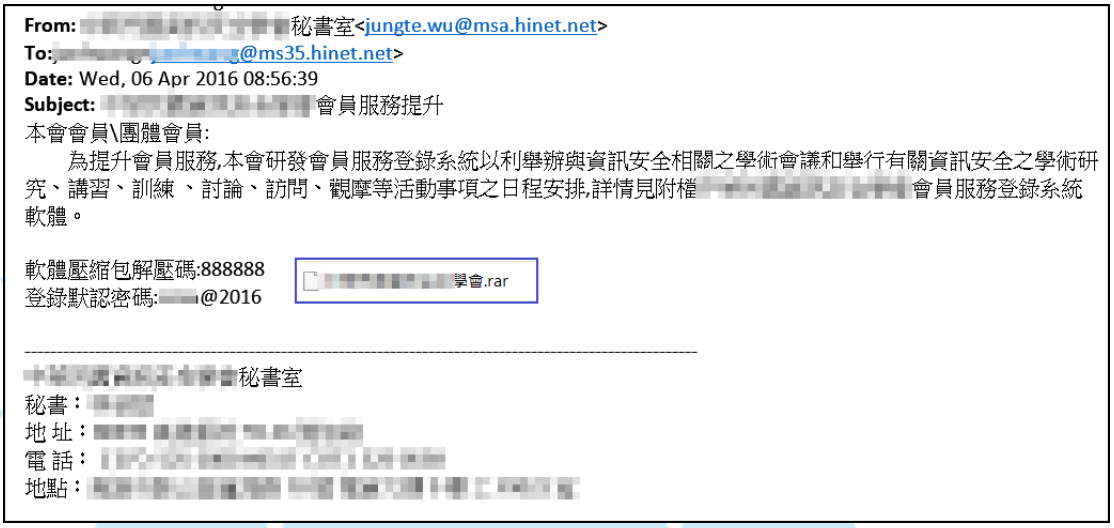
社交工程郵件的 APT 攻擊事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/5

I. 事件簡介

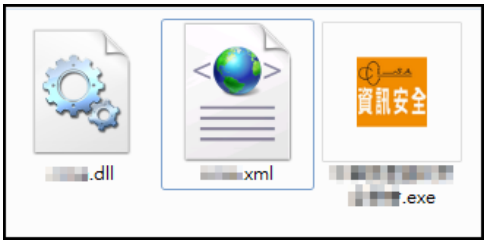
1. 近期接獲某學術單位多數人收到疑似 APT 攻擊的社交工程郵件，該單位並將此 APT 郵件交給 TACERT 進行分析測試。
2. 此信件的主旨為格式為「XXXXXX 會員服務提升」，寄件者偽造成該組織的秘書名字，並透過 HINET 郵件地址發送給單組織成員。郵件內容提供附加檔案「XXX 學會.rar」的解壓縮密碼以及網站登入的密碼進行誘騙。



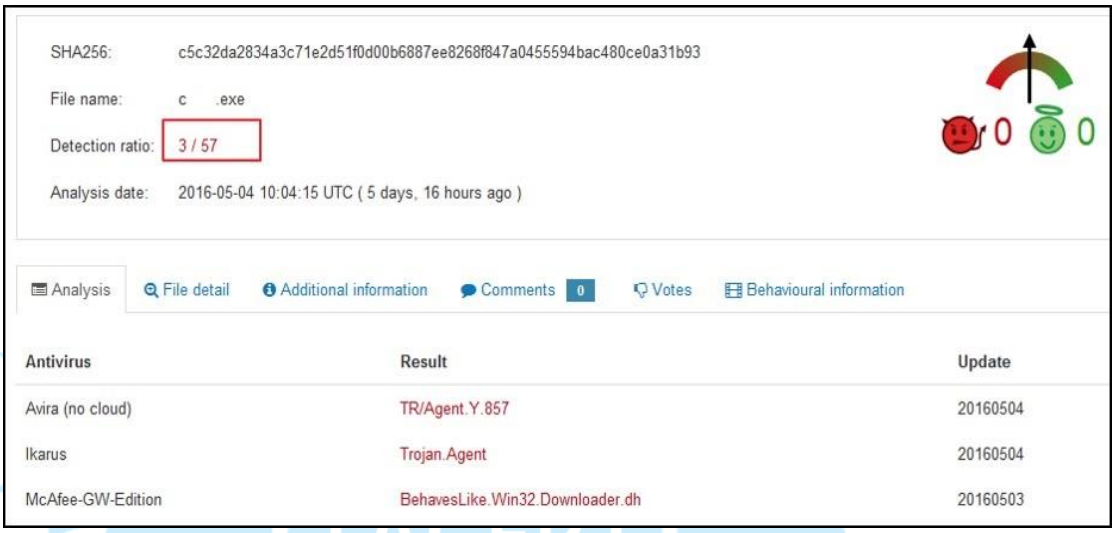
3. 此郵件為典型的社交工程 APT 攻擊郵件，信件的主旨內容以及相關資訊都是針對該單位量身設計，並偽造成單位秘書去發送，並將附加檔案進行加密，一旦感染則可能被駭客掌控重要資料。
4. 本單位透過虛擬主機進行隔離測試，並且側錄惡意程式的網路行為以及惡意程式的運作情形進行分析。

II. 事件檢測

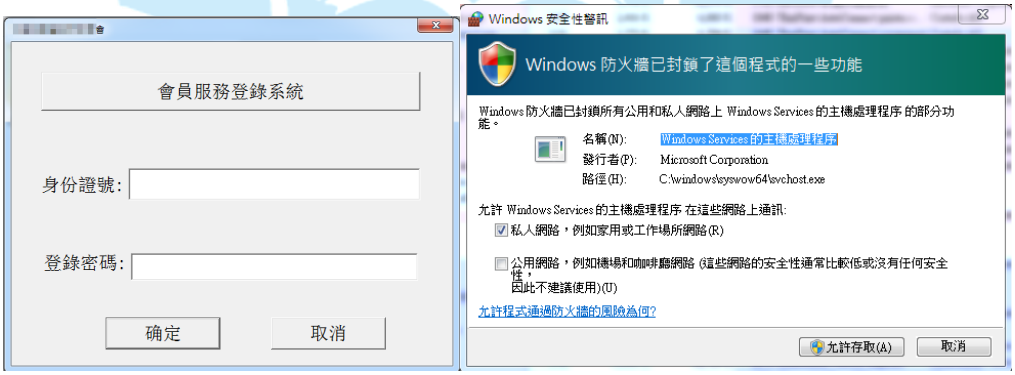
1. 該惡意程式的測試環境為 Win 7(x64)，將附件檔案 RAR 解壓縮時會要求輸入解壓縮密碼，測試只有信件提供的密碼「888888」才能解開。
2. RAR 壓縮檔解開後，會出現三個檔案，分別是 dll、xml 和 exe 執行檔，且檔案名稱都是以該單位名稱命名。



3. 首先透過 Virustotal 掃描該程式，其被偵測出的比例相當低，只有 3/57，算是客製化的惡意程式。

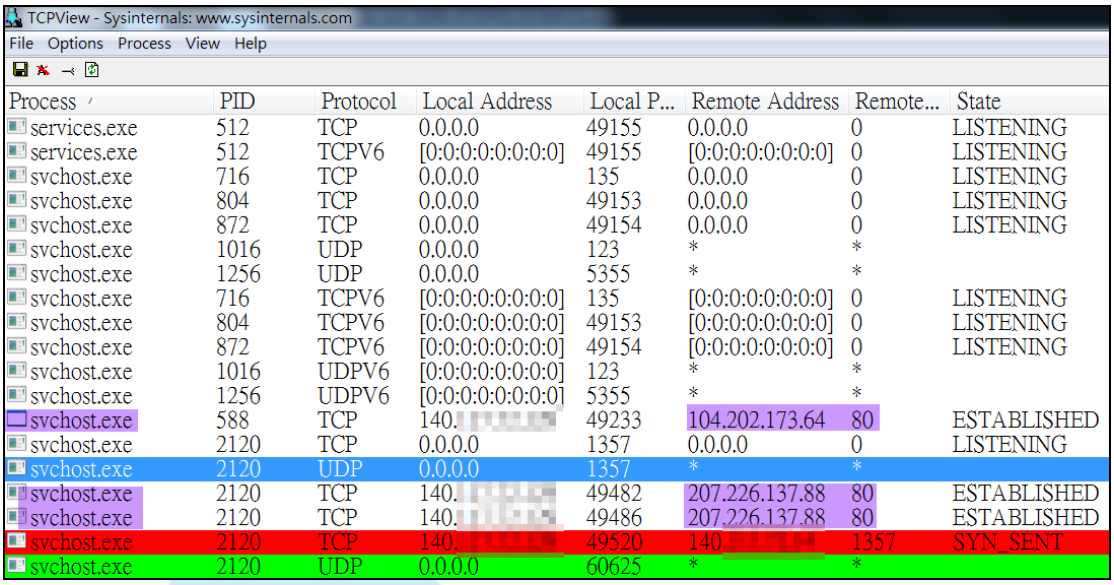


4. 實際執行該 EXE 執行檔，會出現一個登入介面為會員服務登錄系統，並要求輸入身分證號和登入密碼，然而尚未輸入任何資料以前，防火牆就已經出現外部網路存取權限要求，表示惡意程式已經開始產生網路行為。



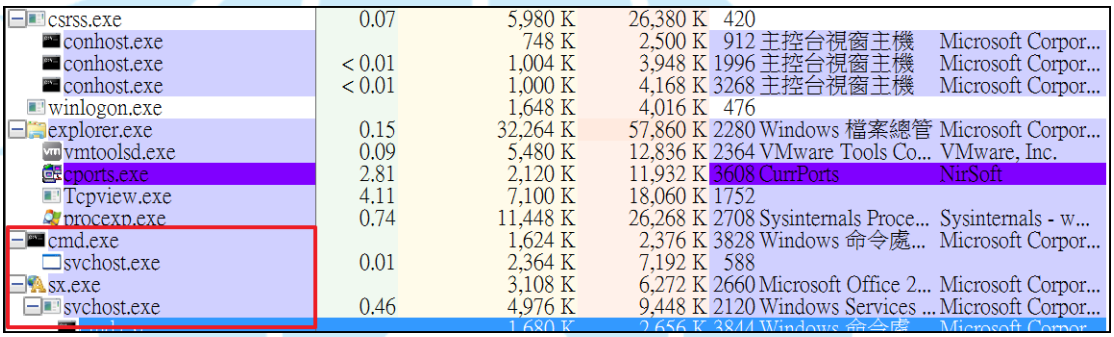
5. 實際隨意輸入身分證號以及指定的登入密碼，該程式會開啟瀏覽器並且連結至該單位的官方網站，並無出現任何額外訊息，表示該登入只是一般的開啟網頁行為。

6. 此時透過 tcpview 工具檢查網路連線狀態，發現有大量的網路行為正在產生，都是透過名稱為 svchost.exe 的惡意程式進行(紫色部分)。



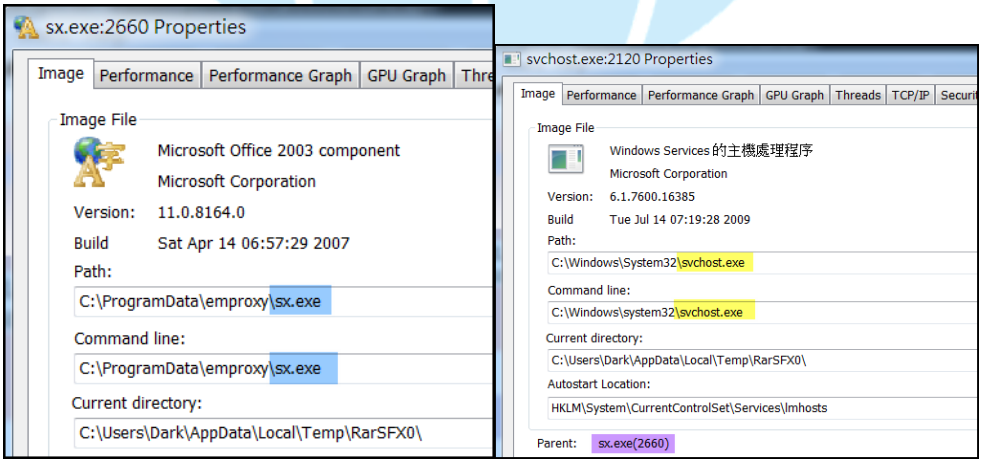
Process	PID	Protocol	Local Address	Local P...	Remote Address	Remote...	State
services.exe	512	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING
services.exe	512	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	716	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING
svchost.exe	804	TCP	0.0.0.0	49153	0.0.0.0	0	LISTENING
svchost.exe	872	TCP	0.0.0.0	49154	0.0.0.0	0	LISTENING
svchost.exe	1016	UDP	0.0.0.0	123	*	*	
svchost.exe	1256	UDP	0.0.0.0	5355	*	*	
svchost.exe	716	TCPV6	[0:0:0:0:0:0:0:0]	135	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	804	TCPV6	[0:0:0:0:0:0:0:0]	49153	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	872	TCPV6	[0:0:0:0:0:0:0:0]	49154	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	1016	UDPV6	[0:0:0:0:0:0:0:0]	123	*	*	
svchost.exe	1256	UDPV6	[0:0:0:0:0:0:0:0]	5355	*	*	
svchost.exe	588	TCP	140.	49233	104.202.173.64	80	ESTABLISHED
svchost.exe	2120	TCP	0.0.0.0	1357	0.0.0.0	0	LISTENING
svchost.exe	2120	UDP	0.0.0.0	1357	*	*	
svchost.exe	2120	TCP	140.	49482	207.226.137.88	80	ESTABLISHED
svchost.exe	2120	TCP	140.	49486	207.226.137.88	80	ESTABLISHED
svchost.exe	2120	TCP	140.	49520	140	1357	SYN_SENT
svchost.exe	2120	UDP	0.0.0.0	60625	*	*	

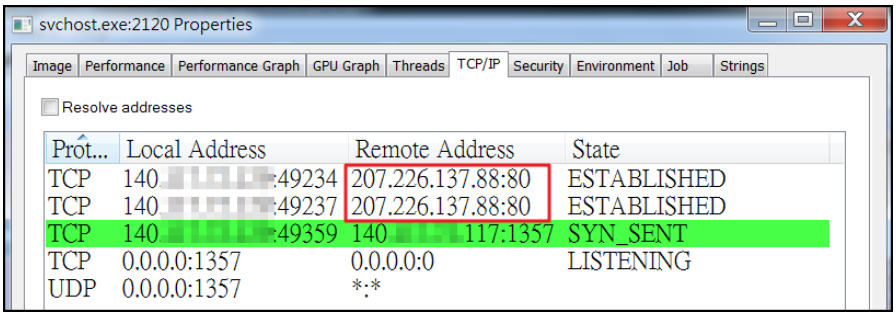
7. 此時透過 procexp 檢查背景程式執行狀況，會出現兩支異常的程式正在執行，檔案名稱都是 scvhost.exe。



csrss.exe	0.07	5,980 K	26,380 K	420	
conhost.exe		748 K	2,500 K	912 主控台視窗主機	Microsoft Corpor...
conhost.exe	< 0.01	1,004 K	3,948 K	1996 主控台視窗主機	Microsoft Corpor...
conhost.exe	< 0.01	1,000 K	4,168 K	3268 主控台視窗主機	Microsoft Corpor...
winlogon.exe		1,648 K	4,016 K	476	
explorer.exe	0.15	32,264 K	57,860 K	2280 Windows 檔案總管	Microsoft Corpor...
vmtoolsd.exe	0.09	5,480 K	12,836 K	2364 VMware Tools Co...	VMware, Inc.
cports.exe	2.81	2,120 K	11,932 K	3608 CurrPorts	NirSoft
Tcpview.exe	4.11	7,100 K	18,060 K	1752	
procexp.exe	0.74	11,448 K	26,268 K	2708 Sysinternals Proce...	Sysinternals - w...
cmd.exe		1,624 K	2,376 K	3828 Windows 命令處...	Microsoft Corpor...
svchost.exe	0.01	2,364 K	7,192 K	588	
sx.exe		3,108 K	6,272 K	2660 Microsoft Office 2...	Microsoft Corpor...
svchost.exe	0.46	4,976 K	9,448 K	2120 Windows Services ...	Microsoft Corpor...

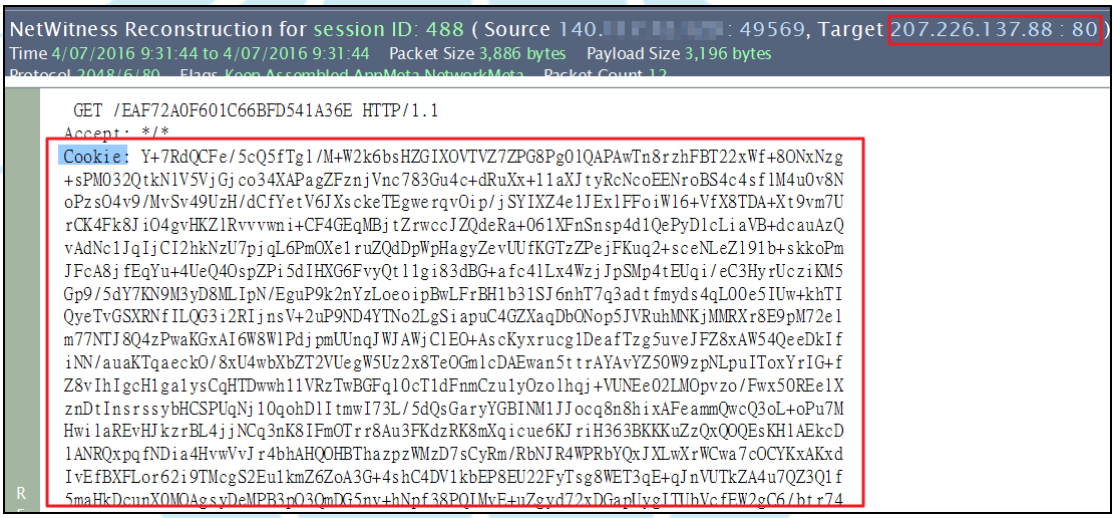
8. 檢查由 sx.exe 並無網路連線，而是由其呼叫 PID 2120 的 svchost.exe 進行網路連線，目的端為 207.226.137.88 的 port 80，並且開啟 TCP port 1357 接收 C&C 指令。



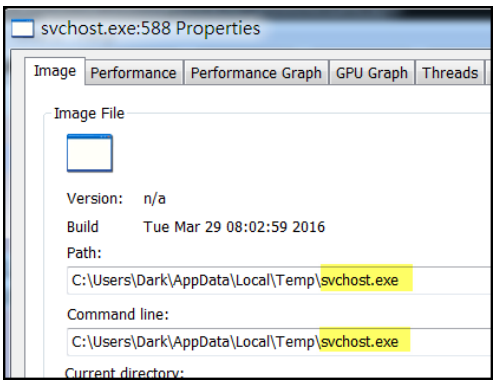


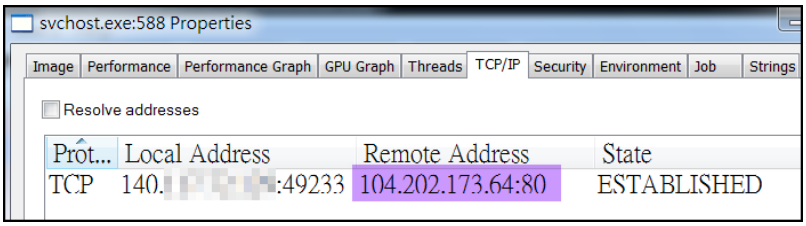
9. 檢測 IP 位址 207.226.137.88，為位於美國的 IP，且直接透過瀏覽器無法開啟，應為駭客報到用的 C&C 主機。

10. 透過檢查該連線的封包資料，都是以 HTTP GET 方式將資料送到 207.226.137.88 的 port 80 接收，而且疑似將竊取的資訊加密塞入 cookie 欄位傳送，而非常見的 HTTP POST 方式。

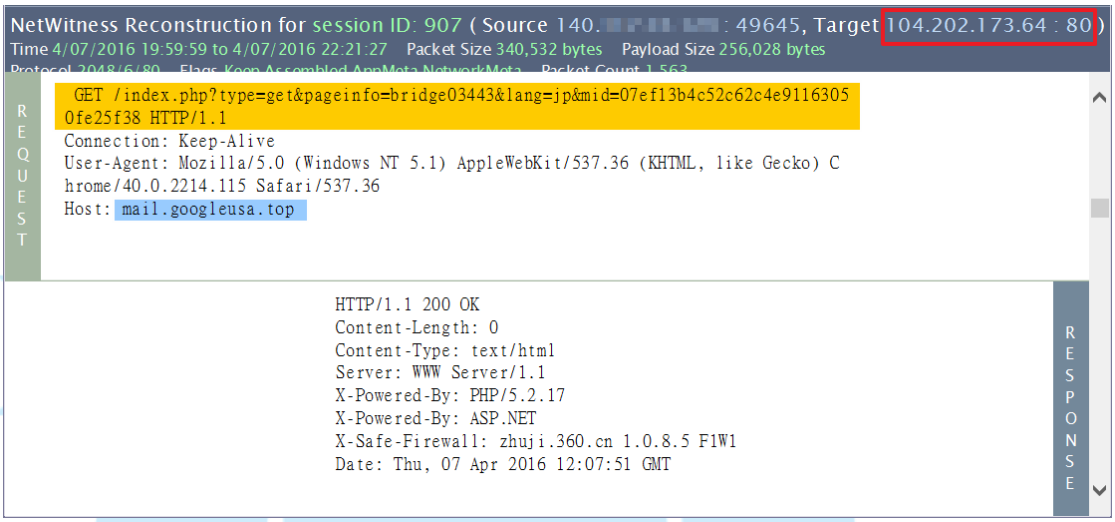


11. 檢測另一個 PID 588 的 svchost.exe，其也有固定的網路連線至美國的 104.202.173.64:80，然而該網址透過瀏覽器也是無法開啟，應同為報到用的駭客 C&C 主機。

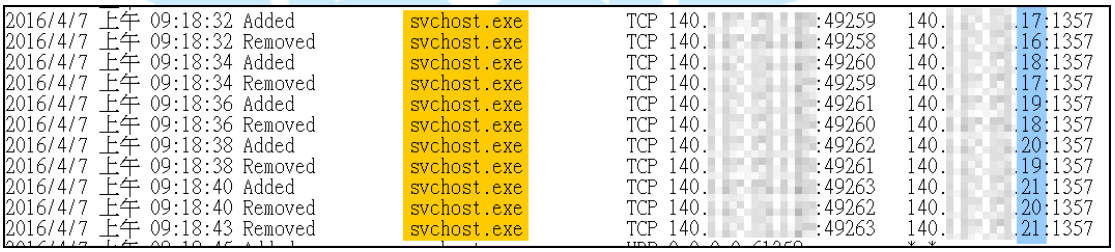


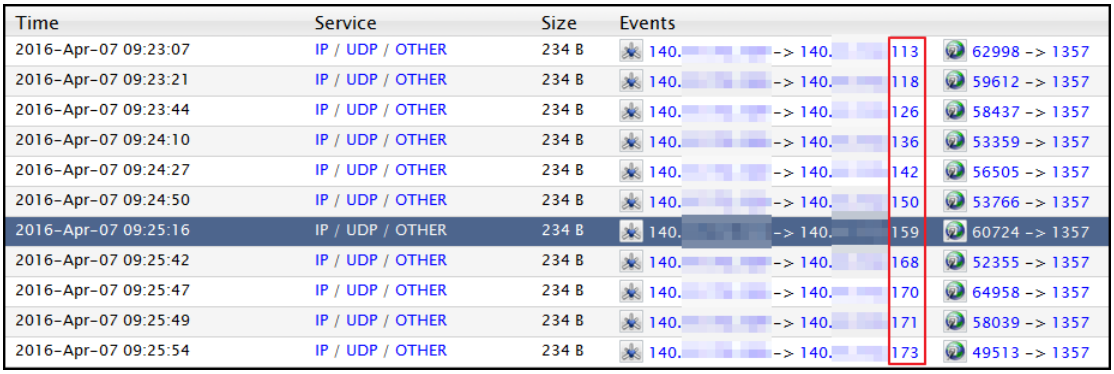


12. 檢查連線 104.202.173.64 的封包紀錄，svchost.exe 會透過 HTTP GET 方式連到美國主機 104.202.173.64 的 port 80，從回傳參數來看應該是在做回報的動作。



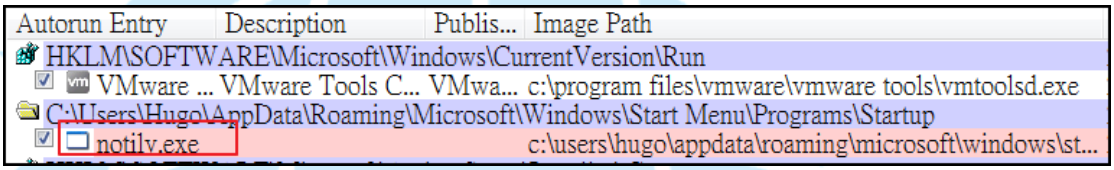
13. 惡意程式 EXE 執行後，svchost.exe 除了對外部產生連線，也會對內部網路進行主機掃描，都是針對 TCP 或 UDP port 1357。



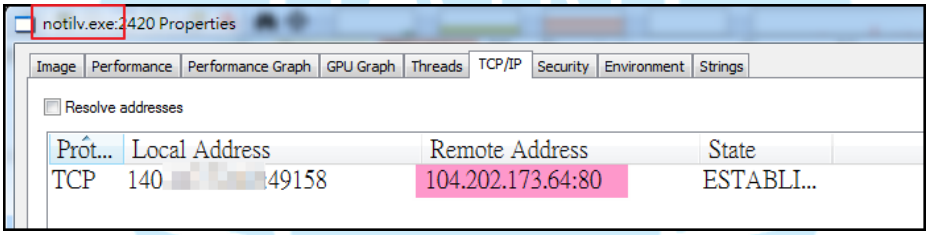


Time	Service	Size	Events
2016-Apr-07 09:23:07	IP / UDP / OTHER	234 B	140. -> 140. 113 62998 -> 1357
2016-Apr-07 09:23:21	IP / UDP / OTHER	234 B	140. -> 140. 118 59612 -> 1357
2016-Apr-07 09:23:44	IP / UDP / OTHER	234 B	140. -> 140. 126 58437 -> 1357
2016-Apr-07 09:24:10	IP / UDP / OTHER	234 B	140. -> 140. 136 53359 -> 1357
2016-Apr-07 09:24:27	IP / UDP / OTHER	234 B	140. -> 140. 142 56505 -> 1357
2016-Apr-07 09:24:50	IP / UDP / OTHER	234 B	140. -> 140. 150 53766 -> 1357
2016-Apr-07 09:25:16	IP / UDP / OTHER	234 B	140. -> 140. 159 60724 -> 1357
2016-Apr-07 09:25:42	IP / UDP / OTHER	234 B	140. -> 140. 168 52355 -> 1357
2016-Apr-07 09:25:47	IP / UDP / OTHER	234 B	140. -> 140. 170 64958 -> 1357
2016-Apr-07 09:25:49	IP / UDP / OTHER	234 B	140. -> 140. 171 58039 -> 1357
2016-Apr-07 09:25:54	IP / UDP / OTHER	234 B	140. -> 140. 173 49513 -> 1357

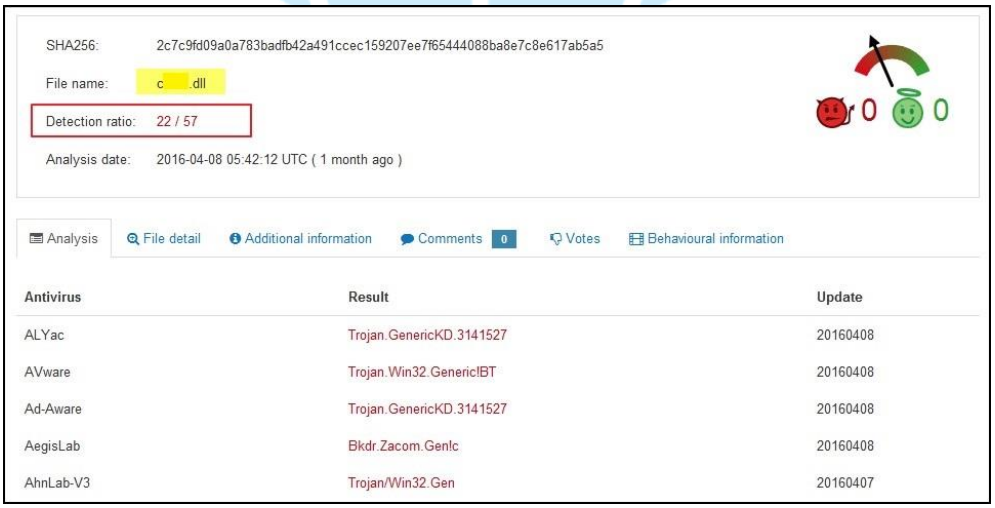
14. 主機感染經過一段時間後，系統被會強制關機，判斷是駭客從 C&C 主機下指令操作，重新開機後檢查 autoruns 開機啟動區，發現有支程式會寫入開機啟動區，名為 notilv.exe 也就是 svchost.exe，其連線 IP 同為 104.202.173.64，可以確定此 IP 為 C&C 伺服器。



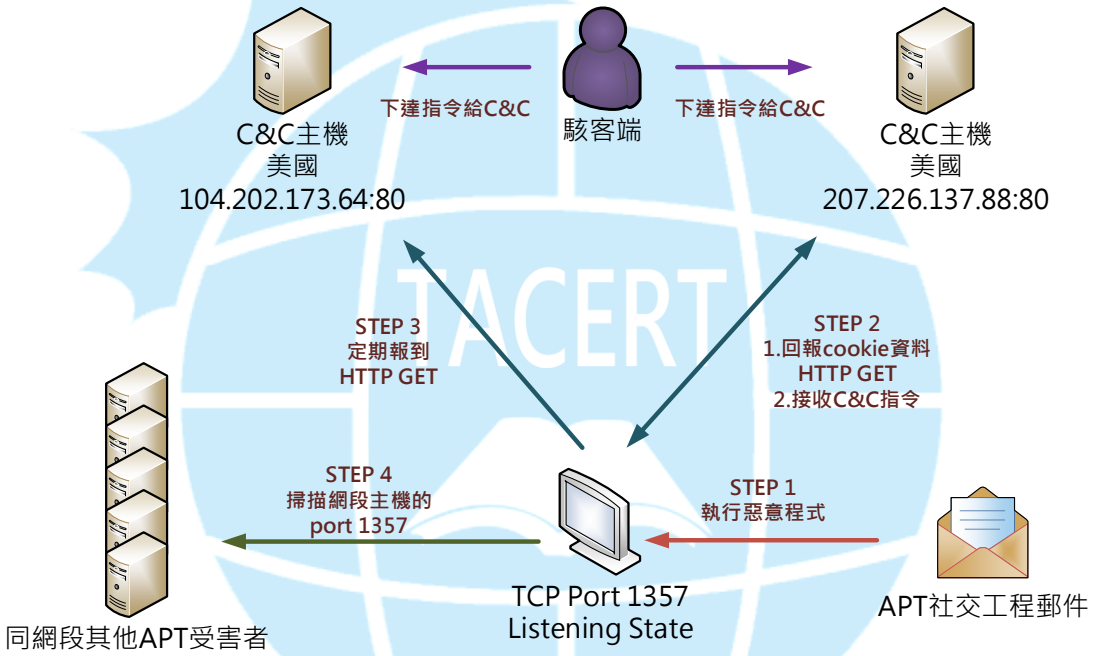
Autorun Entry	Description	Publis...	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
VMware ...	VMware Tools C...	VMwa...	c:\program files\vmware\vmware tools\vmtoolsd.exe
C:\Users\Hugo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
notilv.exe			c:\users\hugo\appdata\roaming\microsoft\windows\st...



15. 透過 virustotal 掃描 notilv.exe 也就是 svchost.exe，可以發現為偵測比率為 22/57 的木馬程式，讓駭客能夠進行遠端操控。



III. 網路架構圖



1. 收到 APT 攻擊的社交工程郵件，並且執行附件惡意程式 EXE 檔案。
2. 主機感染惡意程式後開啟 TCP port 1357 接收 C&C 指令，並且以 HTTP GET 方式回傳資料給 C&C。
3. 感染主機會定期向另一台 C&C 主機已 HTTP GET 方式回報。
4. 感染主機開始向同網段其他主機進行 port 1357 掃描相同感染主機。
5. 駭客持續透過 C&C 主機控制 APT 攻擊受害主機。

IV. 建議與總結

1. 此個案主要是透過社交工程郵件的 APT 攻擊感染，受害者很容易上當執行到

惡意程式。

2. 駭客針對該組織特性客製化惡意程式，讓使用者被操控成為殭屍電腦。
3. 受害主機會開啟 port 1357 讓駭客端透過 C&C 下達指令，執行攻擊動作、重開機或刪除電腦資料等行為。
4. 使用者一旦開啟惡意程式後，惡意程式就會在系統背景隱藏執行，並且開機自動啟用和掃描相同網段其他感染主機。
5. 此例為客製化惡意程式，防毒軟體偵測比例只有 3/57，故使用者很容易受害。
6. 使用者對於有附加檔案或網址的郵件開啟前務必仔細檢查，以免遭受病毒感染。