

個案分析-

社交工程郵件的 APT 攻擊

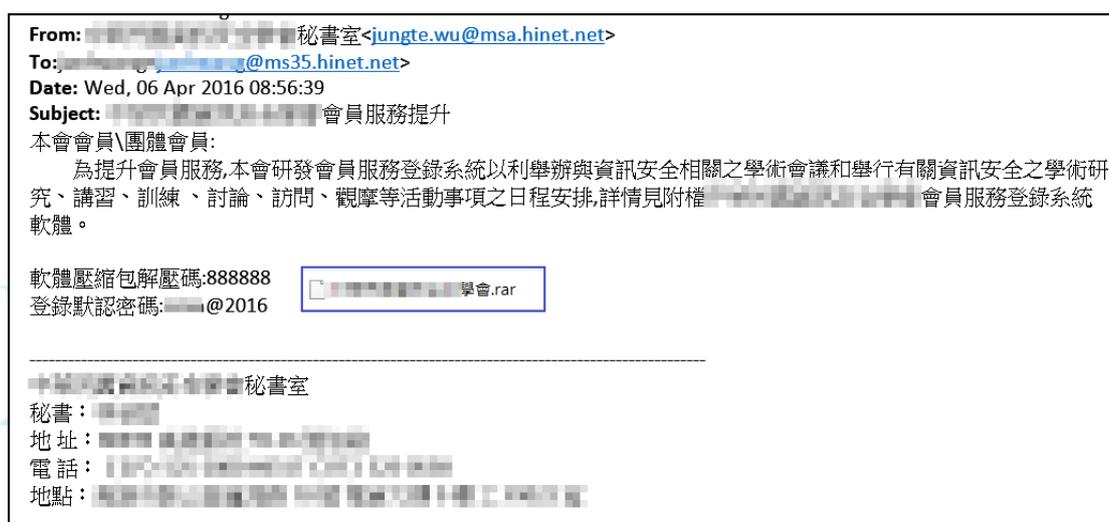
事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/5

I. 事件簡介

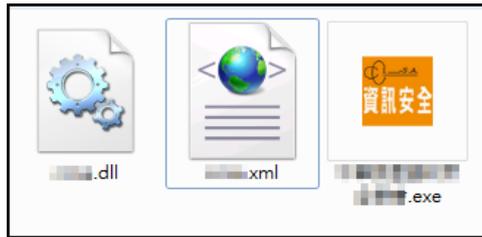
1. 近期接獲某學術單位多數人收到疑似 APT 攻擊的社交工程郵件，該單位並將此 APT 郵件交給 TACERT 進行分析測試。
2. 此信件的主旨為格式為「XXXXXX 會員服務提升」，寄件者偽造成該組織的秘書名字，並透過 HINET 郵件地址發送給單組織成員。郵件內容提供附加檔案「XXX 學會.rar」的解壓縮密碼以及網站登入的密碼進行誘騙。



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

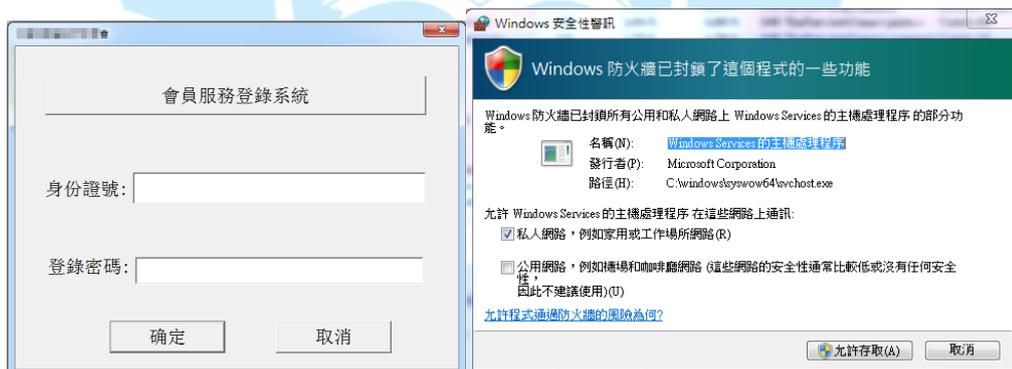
1. 該惡意程式的測試環境為 Win 7(x64)，將附件檔案 RAR 解壓縮時會要求輸入解壓縮密碼，測試只有信件提供的密碼「888888」才能解開。
2. RAR 壓縮檔解開後，會出現三個檔案，分別是 dll、xml 和 exe 執行檔，且檔案名稱都是以該單位名稱命名。



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。

Antivirus	Result	Update
Avira (no cloud)	TR/Agent.Y.857	20160504
Ikarus	Trojan.Agent	20160504
McAfee-GW-Edition	BehavesLike.Win32.Downloader.dh	20160503

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，都是透過名為 svchost.exe 的惡意程式進行(紫色部分)。

Prot...	Local Address	Remote Address	State
TCP	140.0.0.0:49234	207.226.137.88:80	ESTABLISHED
TCP	140.0.0.0:49237	207.226.137.88:80	ESTABLISHED
TCP	140.0.0.0:49359	140.0.0.0:117:1357	SYN_SENT
TCP	0.0.0.0:1357	0.0.0.0:0	LISTENING
UDP	0.0.0.0:1357	*.*	

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。

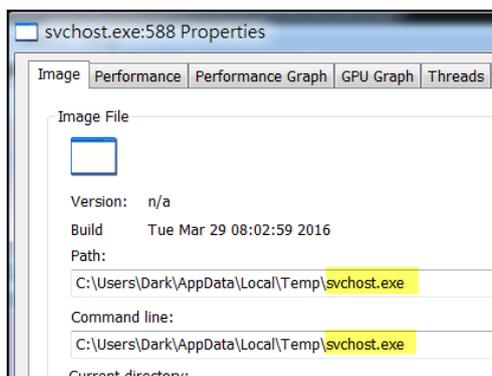
```

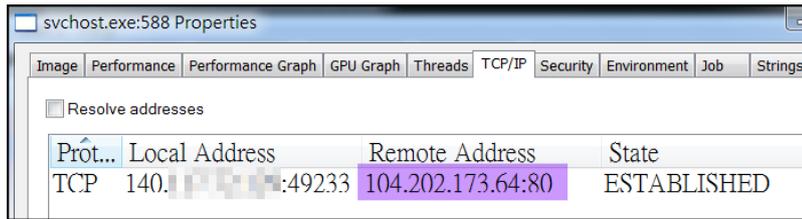
NetWitness Reconstruction for session ID: 488 ( Source 140.0.0.0:49569, Target 207.226.137.88:80 )
Time 4/07/2016 9:31:44 to 4/07/2016 9:31:44 Packet Size 3,886 bytes Payload Size 3,196 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 12

GET /EAF72A0F601C66BFD541A36E HTTP/1.1
Accept: */*
Cookie: Y+7RdQCFe/5cQ5fTg1/M+W2k6bsHZGIXOVTVZ7ZPG8Pg01QAPAwTn8rzhFBT22xWf+80NxNzg
+sPM032QtKn1V5VjGjco34XAPagZFznjVnc783Gu4c+dRuXx+11aXJtyRcNcoEENroBS4c4sf1M4u0v8N
oPzs04v9/MvSv49UzH/dCfYetV6jXsckeTEgwerqvOip/jSYIXZ4e1JEx1FFoiW16+VfX8TDA+Xt9vm7U
rCK4Fk8Ji04gvHKZ1Rvvnvni+CF4GEqMBjtZrwccJZQdeRa+061XFnsnsp4d1QePyD1cLiavB+dcauAzQ
vAdNc1JqIjCI2hkNzU7pjql6PmOXe1ruZQdPwPwHagyZevUUFKGTzZPejFKuq2+sceNLeZ191b+skkoPm
JfEa8jfeqYu+4UeQ40spZPi5dIHxG6FvyQt11gi83dBG+afc41Lx4WzjJpSmP4+EUqi/eC3HyrUcziKM5
Gp9/5dY7KNM3yD8MLIpN/EguP9k2nYzLoeipBwLFrBH1b31SJ6nhT7q3adt fmyds4qL00e5IUw+khTI
QyeTvGSXRNFILQG3i2RIjnsV+2uP9ND4YTNo2LgSiapuC4GZXaqDbONop5JVruhMnkjMMRXr8E9pM72e1
m77NTJ8Q4zPwaKGxAI6W8W1PdjpMUUnqJWJAWjC1EO+AscKyxrucg1DeafTzg5uveJFZ8xAW54QeDkI
iNN/auaKTqaecK0/8xu4wbXbZT2VUegW5Uz2x8TeOGmlcDAEwan5ttrAYAvYZ50W9zpnLpuIToxYrIG+f
Z8vThIgcH1galysCqHTDwwh11VRzTwBGFq10cT1dFnmCzulyOz0lhqj+VUNEe02LMOpvzo/Fwx50REe1X
znDtInsrssybHCSPUqNj10qohD1I tmwI73L/5dQsGaryYGBIN1JJocq8n8hixAFeammQwcQ3oL+oPu7M
Hwi1aREvHjkzrBL4jjNCq3nK8IFmOTrr8Au3FKdzRK8mXqicue6KJriH363BKKkuzZQxQQQEsKH1AEkcD
1ANRQxppqfNDia4HvwVvJr4bhAQOHBThazpzWMZD7sCyRm/RbNJR4WPRbYQxJXLwXrWCwa7cOCYKxAKxd
IvEfbXFLor62i9TMcgs2Eu1kmZ6oA3G+4shC4DV1kbEP8EU22FyTsg8WET3qE+qJnVUTkZA4u7QZ3Q1f
SmaHkdCuuXOMOAgssyDeMPB3p03QmDG35nv+hNpf38PQIMvE+uZgyd72zDGaplygLTUhbVcFEW2gC6/br74

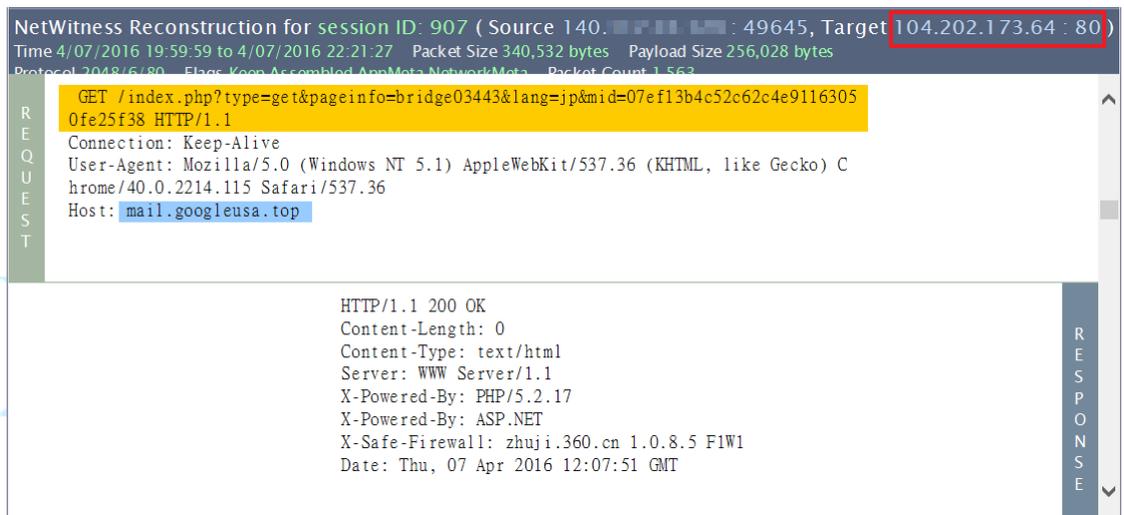
```

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。

2016/4/7 上午 09:18:32	Added	svchost.exe	TCP	140....	:49259	140....	17:1357
2016/4/7 上午 09:18:32	Removed	svchost.exe	TCP	140....	:49258	140....	16:1357
2016/4/7 上午 09:18:34	Added	svchost.exe	TCP	140....	:49260	140....	18:1357
2016/4/7 上午 09:18:34	Removed	svchost.exe	TCP	140....	:49259	140....	17:1357
2016/4/7 上午 09:18:36	Added	svchost.exe	TCP	140....	:49261	140....	19:1357
2016/4/7 上午 09:18:36	Removed	svchost.exe	TCP	140....	:49260	140....	18:1357
2016/4/7 上午 09:18:38	Added	svchost.exe	TCP	140....	:49262	140....	20:1357
2016/4/7 上午 09:18:38	Removed	svchost.exe	TCP	140....	:49261	140....	19:1357
2016/4/7 上午 09:18:40	Added	svchost.exe	TCP	140....	:49263	140....	21:1357
2016/4/7 上午 09:18:40	Removed	svchost.exe	TCP	140....	:49262	140....	20:1357
2016/4/7 上午 09:18:43	Removed	svchost.exe	TCP	140....	:49263	140....	21:1357

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

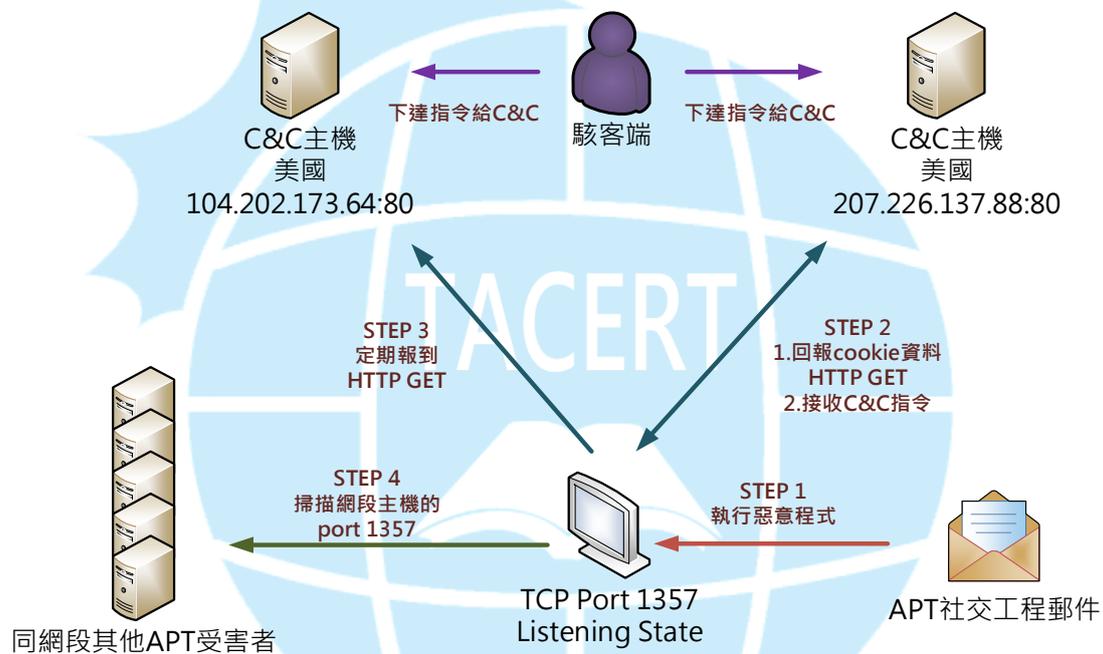
Prot...	Local Address	Remote Address	State
TCP	140. [bar] 49158	104.202.173.64:80	ESTABL...

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。

SHA256:	2c7c9fd09a0a783badfb42a491cccec159207ee7f65444088ba8e7c8e617ab5a5	
File name:	c.dll	
Detection ratio:	22 / 57	
Analysis date:	2016-04-08 05:42:12 UTC (1 month ago)	

Antivirus	Result	Update
ALYac	Trojan.GenericKD.3141527	20160408
AVware	Trojan.Win32.Generic!BT	20160408
Ad-Aware	Trojan.GenericKD.3141527	20160408
AegisLab	Bkdr.Zacom.Genlc	20160408
AhnLab-V3	Trojan/Win32.Gen	20160407

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 主機以 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。

