# 個案分析-S 單位 與 E 單位 之 APT 社交 工程郵件事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/08



TANET 中某單位行政部門同仁收到含有惡意程式附檔的電子郵件,實為常見的 APT 社交工程攻擊,該附件檔命名為"通訊錄.rar",解開後有一個正常 word 檔案、一個 lnk 執行檔案及一個 ini 隱藏檔,該 lnk 執行檔會去執行惡意的隱藏 檔,一旦執行後 ini 隱藏檔就會自我移除,並且於背景產生一隻後門程式 PeerDistSvc.exe 將電腦資料傳送給上層的感染主機,並且該程式會常駐在開機時 後自動執行。一旦遭受感染的主機可能個資帳密都會外洩,務必將惡意程式移除 後更改帳號及密碼。

## 事件說明

一、 檢測工具及環境準備:

- 1. 測試主機為 VMware: Win7(x64), 無安裝任何修補程式。
- 2. 安裝的 Office 2007 版本, 無安裝任何修補程式。
- 3. 使用實體 IP,並用 Wireshark 側錄該感染主機之 Pcap 封包。
- 4. 使用 Currport 每 2 秒去紀錄網路連線埠號的使用狀況。
- 5. 使用 procmon 紀錄該程式的變化。

#### 二、 事件過程(一)-S 單位:

- 1. 06/20 S 單位內部某同仁收到疑似含後門程式之惡意信件。
- 2. 06/20 S 單位將該惡意信件封存為 msg 檔以保留信件 Header,請本單位 TACERT 協助測試分析。
- 3. 此惡意原始信件資訊為:
  - (1).收件者另含隱藏密件副本,從信件標頭只知會 CC 給 S 單位某人。

	2013/6/20 (週四) 上午 10:38 cyin101 <cyin101@yahoo.com.tw> 通訊錄</cyin101@yahoo.com.tw>		
收件者 cyin1	01	- 1	
附件	通訊錄.rar	- 1	
檢附通訊	錄乙份請大家確認是否正確.		
謝謝			
Received: from t by gate with ES Thu, 20	mail0edu.tw (EHLO fmail0edu.tw) ([140]) edu.tw (MOS 4.1.10-GA FastPath queued) MTP id BDI28573; Jun 2013 10:40:26 +0800 (CST)		
Received: from ( ESMTP id oFVIT) Received: from ( Received: from ) Received: from ( Received: from )	m35-vm9.bulletmail.sg3.yahoo.com (nm35-vm9.bulletmail.sg3.yahoo.co 3hprcivEzlc for <otto@edu.tw>; Thu, 20 Jun 2013 10:40:24 +08 106.10.166.126] by nm35.bulletmail.sg3.yahoo.com with NNFMP; 20 Jun 106.10.167.183] by tm15.bulletmail.sg3.yahoo.com with NNFMP; 20 Jun 127.00.1] by smtp156.mail.sg3.yahoo.com with NNFMP; 20 Jun 2013 02: vi101@vahoo.com tw&gt;</otto@edu.tw>	om [106.1 300 (CST) 2013 02: 2013 02:4 40:24 -00	0.150.238]) by fmail0 edu: :40:24 -0000 40:24 -0000 :00

w with

4. 該附件『通訊錄.rar』解壓縮後有三個檔案:

- (1).6月17日.doc:為正常檔案,內含許多人的姓名、電話、Email。
- (2).0617photo.lnk:為一個連結執行檔。
- (3).desktop.ini:為隱藏的組態檔,是惡意後門程式,文件編輯顯示內容為 亂碼。

W	6月17日.doc 作者: 行政院勞工委員會	大小: 42.0 KB
	0617photo 頬型: 捷徑	大小: <b>768 個位元組</b>
	desktop.ini <sub>類型:</sub> 組態設定	大小: <b>46.0 KB</b>

圖 1、『通訊錄.rar』解壓縮之後檔案

- 三、 檢測過程-S 單位:
  - 1. 將檔案『6月17日.doc』上傳至 Virustotal 檢測正常。
  - 2. 將檔案『0617photo.lnk』上傳至 Virustotal 檢測正常,其 hash value 比對其 實是為 cmd.exe,為合法檔案做的偽裝,主要執行隱藏的 desktop.ini。
  - 將隱藏檔案 desktop.ini 上傳至 Virustotal 檢測,病毒檢出比例 6/47。信件 檔案『6月17日.doc』為正常檔案,開啟後有許多人的個資,如名字、電 話及 Email。
  - 4. 執行信件檔案『0617photo.lnk』, 此檔會執行同目錄下的隱藏檔

P						
U	de	ve k	to	n	1n'	1
	uu	~OD	ιυ	νυ.	ш.	L

L ] Š			_
		0617photo	
	[二]+三/4月11]	陈田田子	
	日保親型:	應用程巧	
	目標位置:	System32	
	目標(T):	C:\Windows\System32\cmd.exe /c desktop.ini	

圖 2、0617photo 其實是去執行惡意檔 desktop.ini

- 5. 之後『desktop.ini』就會自我刪除,並產生一個叫做『PeerDistSvc.exe』(或 其他名稱)的執行檔開始在背景執行,並開啟 TCP Port 對外連線至上層的 中繼站 140.X.X.15:443,感染主機個資可能被竊取。
- 中繼站 140.X.X.15 經調查發現是 TANET 底下學校的郵件伺服器, 位於台 中 Y 國中。
- 『PeerDistSvc.exe』的 Hash 值比對發現其實就是自我刪除的『desktop.ini』, 藏在在隱藏目錄 C:\Users\username\AppData\Local\PeerDistSvc.exe。

Process Monitor - C:\Users\ming\Documen	ts\0617photo-2-1.PML		_ 0 X
File Edit Event Filter Tools Options	Help		
📔 🖨 📔 🕺 💸 📴 🖾 🛛 🗢 📥 🌚 🗌	E   🗛 📕   🔣 🗟 🔍 🗖 🗷		
Time of Day Process Name	PID Operation	Path	Result
└─ \ + 01:31:13 III PeerDistSvc.exe	2600 🔬 TCP Connect	WIN-9GLFJBE2SQD:49200 -> mail2. edu.tw:https	SUCCESS
└─ \+ 01:31:13 IIIPeerDistSvc.exe	2600 📥 TCP Send	WIN-9GLFJBE2SQD:49200 -> mail2. 🗾 edu.tw:https	SUCCESS
⊢ + 01:31:14  PeerDistSvc.exe	2600 📥 TCP Receive	WIN-9GLFJBE2SQD:49200 -> mail2. edu.tw:https	SUCCESS
⊬ + 01:31:14  PeerDistSvc.exe	2600 📥 TCP Disconnect	WIN-9GLFJBE2SQD:49200 -> mail2. edu.tw:https	SUCCESS
•			Þ
Showing 4 of 2,642,900 events (0.00015%)	Backed by C:\Users\ming\Documents\0617p	hoto-2-4.PML	

Page	1 of 380 🛛 🔿 💌		<b>  88 (</b>	> 🖶 🖪 😭 🔊			
	Time	Service	Size	Events		Displaying 1 - 20 of 7586	^
View	2013-Jun-21 10:31:21	IP / TCP / HTTP	1.68 KB	★ 140> 140	49	243 -> 443 (https)	Ξ
View	2013-Jun-21 10:31:22	IP / TCP / HTTP	1.67 KB	<b>★ 140.</b> -> 140	49	244 –> 443 (https)	
View	2013-Jun-21 10:31:53	IP / TCP / HTTP	1.68 KB	<b>★ 140.</b> -> 140	49	245 -> 443 (https)	_
View	2013-Jun-21 10:31:56	IP / TCP / HTTP	1.92 KB	<b>★ 140.</b> -> 140	49	246 -> 443 (https)	
View	2013-Jun-21 10:32:24	IP / TCP / HTTP	1.79 KB	* 140> 140	49	247 –> 443 (https)	_
View	2013-Jun-21 10:32:31	IP / TCP / HTTP	2.08 KB	<b>★</b> 140> 140		250 -> 443 (https)	-
							Þ

圖 3、惡意程式向中繼站主機建立連線

Ne Tir	B → → → → → → → → → → → → → → → → → → →	jet 14	40. 15 : 443 )	
R E Q U E S T	GET /security.jsp?ch=izvmwil11D30025E4G HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729) Host: 140	R E S P O N S E		A
R E Q U E S T		R E S P O N S E	HTTP/1.1 200 0K Content-Length: 12 Content-Type: application/octet-stream Connection: Close 1V &,挽口5	

圖 4、測試主機向上層中繼站傳送加密資料,中繼站成功接收則回覆 OK

- 8. 透過 Tcpview 發現一開始會以特定 PID 的『PeerDistSvc.exe』對外的連線, 之後就會變成 PID:0 的 Unknown 程式去連線,使人不易察覺為異常程式。
- 9. 原則上惡意程式在 C:\Users\username\AppData\ 會產生執行檔 『igfxtray.exe』在註冊機碼寫入開機自動於背景執行連線。



圖 5、igfxtray 的位置與自動執行

- 『igfxtray.exe』與『PeerDistSvc.exe』行為一樣,連線至中繼站
   140.X.X.15:443 傳送資料,只是『PeerDistSvc.exe』重開機不會自動執行。
- 11. 『0617photo.lnk』的同目錄下會產生一個『cmd.exe』去執行系統檔

rundll32.exe,再執行隱藏目錄 C:\Users\username\AppData\Local\Temp\ 的 惡意程式『new.dll』,並建立連線至「220.130.160.113」傳送較大的資料 檔案。

Ра	ge 1 of 1 🛛 🖸 🔍 💌								
	Time	Service	Size	Events	Displaying 1 - 7 of 7				
View	2013-Jun-21 10:53:14	IP / TCP / OTHER	230.54 KB	№ 140.	👰 49300 -> 443 (https)				
View	2013-Jun-21 11:39:00	IP / TCP / OTHER	347.52 KB	▲ 140> 220.130.160.113	👰 49464 -> 443 (https)				
View	2013-Jun-21 12:17:07	IP / TCP / OTHER	7.49 KB	😹 140.          → 220.130.160.113	😡 49563 -> 443 (https)				
View	2013-Jun-21 12:23:19	IP / TCP / OTHER	432 B	🗼 140.         -> 220.130.160.113	😡 49566 -> 443 (https)				
View	2013-Jun-21 12:38:20	IP / TCP / OTHER	432 B	🗼 140.         -> 220.130.160.113	😡 49596 -> 443 (https)				
View	2013-Jun-21 12:53:21	IP / TCP / OTHER	432 B	★ 140.	😡 49626 -> 443 (https)				
View	2013-Jun-21 13:08:22	IP / TCP / OTHER	432 B	★ 140.	😡 49657 -> 443 (https)				
٠					4				
R R C Q U E S T	Vitness Reconstructio 5/21/2013 10:53:14 to 6/2 5/21/2013 10:53:14 to 6/2 5/21/2013 10:53:14 to 6/2 5/21/2013 10:53:14 to 6/2 10:00 10:53:14 to 6/2 11:00 10:53:14 to 6/2	● I III IIII IIII IIIIIIIIIIIIIIIIIIII	: 8190 ( Second Se	Source 140 : 49300, Ta Play Audio di Size 170,540 bytes Reconstruct any audio content contained in the currently loaded session.	arget 220.130.160.113 : 443 ) S E				
n □ Ix;硉 0 ?P敖e0i □ □2□!□"□□(r7催 '氾( 瑔QT□0廢 \$J,黯s □ □) { 4J鈸KV□ □ □]措顳' . □5跙 瀘 □' 鎤V□< 4 榝;#%-Yf 麅b三7桓 IrA推筠 <u跴監□5 ;□9(k□="" x□(□="" □錙)□="" 所□="">w居設□ V`5#j□=□:(□ 0]匜s=9R琏:□ /x□ 琡0 □ □ □□"h曆□9書 □?_□8t礂M=WrBb□!□/□ 0~ 電。9b卮H□ &amp;V辦 □ □:8□ □" 楑&amp;Mt総A穭□ 騙□ □□ 探常 +□=鋎\$勞喻辭2□ 3□ 懦d □%a □&lt;虧r奕M□ 0滍]鈰盹 D紛燉□□&amp;6&gt; 醡]□□ f:zI膜e傳#菢6妣碠y□ 鎌 "礝 :6</u跴監□5>									
D					· · · ·				

圖 6、受害主機向中繼站傳送加密資料,疑似使個資外洩

12. 程序監測工具紀錄出異常程式運作情形。

rocess	Command	Company	Description
🗉 📖 cmd.exe (2872)	"C:\Windows\system32\cmd.exe"	Microsoft	Windows 個分.
rundll32.exe (1924)	rundll32.exe c:\users\ming\appdata\local\temp\new.dll	Microsoft	Windows 冊案.
🗉 🥏 Procmon.exe (2432)	"C:\Users\ming\Desktop\SysinternalsSuite\Procmon.exe"	Sysinternal	Process Monit
autoruns.exe (2124)	"C:\Users\ming\Desktop\SysinternalsSuite\autoruns.exe"	Sysinternal	Autostart proc
igfxtray.exe (2156)	"C:\Users\ming\AppData\igfxtray.exe"	1	
Explore.exe (904)	"C:\Program Files (x86)\Internet Explorer\iexplore.exe"	Microsoft	Internet Explo
@iexplore.exe (2440)	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SC	Microsoft	Internet Explo
🗉 📼 cmd.exe (1376)	"C:\Windows\System32\cmd.exe"	Microsoft	Windows 信你.
rundll32.exe (596)	rundll32 c:\users\ming\appdata\local\temp\new.dll	Microsoft	Windows 州業
rundll32.exe (2292)	rundll32 c:\users\ming\appdata\local\temp\new.	Microsoft	Windows 卅鄴.
mrundll32.exe (308)	rundll32.exe c:\users\ming\appdata\local\temp\new.exe	Microsoft	Windows 卅粼.
🛄 PeerDistSvc.exe (2600)	C:\Users\ming\AppData\Local\PeerDistSvc.exe "C:\Users\		
		-	
	< III		,
cription:			
npany:			
h: C:\Users\ming\AppData\Local\PeerDistSvc.e			
mmand: C: Users (ming (AppData (Local (PeerDistSvc.))	xxe "C: (Users (ming (Desktop (malicious ))更計級) (desktop, ini "		

#### 圖 7、紅色標記為惡意程式

四、 簡易網路架構:



- 五、 惡意程式排除方式-S 單位:
  - 1. 先將網路線拔除或關閉網路卡,以中斷連外網路。
  - 2. 用工作管理員或 procexp 將惡意程序 PeerDistSvc.exe 和 igfxtray.exe 刪 除。
  - 3. 將 C:\Users\username\AppData\Local\PeerDistSvc.exe 惡意程式移除。
  - 4. 將 C:\Users\username\AppData\ igfxtray.exe 惡意程式移除。
  - 5. 用 autoruns 或開始執行 msconfig 將『igfxtray.exe』自動開機啟動取消移除。
  - 6. 用掃毒軟體掃瞄系統。
- 六、 事件過程(二)-E單位:
  - 1. 06/25 上午 E 單位內陳姓同仁收到疑似夾帶惡意程式的郵件。
  - 06/25 下午E單位將此信件之附檔轉寄於本單位TACERT進行測試分析, 但因只有檔案並無原始信件,故不易查出寄信者資訊。
  - 3. 此惡意信件資訊為:

Forwarded message	
From: cyin101 < <u>cyin101@yahoo.com</u> .	tw>
To:	<u>tw</u> >
Date: Tue, 25 Jun 2013 08:42:23	
Subject: 102 年	期中報告
如有不明事宜・請洽詢聯絡人:劉紫	登鐘副主任(0936-231661)。
耑此 恭祝	
安康順心	

- 4. 該信附件『102 年 "T 單位" 期中報告.rar』(35KB),解壓縮後為『102 年 度"T單位"期中報告 V1.docx.scr』(60KB)。
- 5. 該 scr 執行檔沒有偽裝很成功,檔案圖示也不是 word,明顯為惡意程式。
- 檢測過程-E 單位: 七、
  - 1. 將信件檔案『102 年度"T單位"期中報告 V1.docx.scr』執行後,該檔案 並不會消失,但也不會有 word 打開。
  - 2. 產生一隻叫做『ProtectedStorage.exe』程式於背景執行,並開啟 TCP Port 對外連線至上層的中繼站 140.X.X.15:443, 然而該中繼站當時已經被管理 者處理過,所以連線並無建立成功。
  - 3. 『ProtectedStorage.exe』在隱藏目錄 C:\Users\username\AppData\Local\。
  - 4. 註冊機碼中並無惡意程式自動開機啟動。

ProtectedStorage.exe:2528 Properties	
Environment Job Strings Image Performance Performance Graph GPU Graph Threads TCP/IP Security Trave Te	
Version: n/s BulkTime: Fri Jun 07 11:34:25 2013 Path: C:Users/ming/AppOtati/usel/ProtectedStorage.exe Command line: C:Users/ming/AppOtati/usel/ProtectedStorage.exe Current directory: C:Users/ming/AppOtati/usel/ProtectedStorage.exe Current directory: C:Users/ming/AppOtati/usel/ProtectedStorage.exe Current directory: C:Users/ming/AppOtati/usel/ProtectedStorage.exe Current directory: C:Users/ming/AppOtati/usel/Informational/OpeOfatio	Reference       Page Higds       Applet       News Provides       Soldwid Safety         Image Part       Image Higds       Applet       News Provides       Soldwid Safety         Image Part       Image Part       Image Part       Soldwid Safety       Description         Image Part       Image Part       Image Part       Soldwid Safety       Description         Image Part       Image Part       Image Part       2013/7/29       Ff +         Image Part       Image Part       Civrogram files/w. 2013/1/1.1 + fr +       Description       Publisher       Image Part       2013/7/29       Ff +         Image Part       Image Part       Image Part       Image Part       2013/7/29       Ff +       2013/7/29       Ff +       2013/7/29       Ff +       2013/7/21       Ff +       2013/7/21
OK Cancel	Ready. Windows Entries Hidden.

圖 8、『ProtectedStorage.exe』的內容 啚

9	`	註册	機	碼	無	寫	入	.開	機	自	動	啟	動
---	---	----	---	---	---	---	---	----	---	---	---	---	---

Time	Service	Size Events	Displaying 1 - 20 of 5576
	Service	Size Events	
View 2013-Jun-26 09	:02:37 IP / TCP / OTHER	374 B 💥 140> 140. 1	5 😡 49547 -> 443 (https)
View 2013-Jun-26 09	IP / TCP / OTHER	374 B 🗼 140> 1401	5 👰 49549 -> 443 (https) ≡
View 2013-Jun-26 09	:03:41 IP / TCP / OTHER	374 B 🗼 140> 140	5 😡 49550 -> 443 (https)
View 2013-Jun-26 09	:04:13 IP / TCP / OTHER	374 B 🗼 140> 140	5 👰 49551 -> 443 (https)
View 2013-Jun-26 09	:04:45 IP / TCP / OTHER	374 B 🗼 140> 140	5 👰 49552 -> 443 (https)
View 2013-Jun-26 09	:05:18 IP / TCP / OTHER	374 B 🗼 140> 140	5 😡 49553 -> 443 (https)
View 2013-Jun-26 09	:05:50 IP / TCP / OTHER	374 B 🗼 140> 140	5 👰 49554 -> 443 (https)
View 2013-Jun-26 09	:06:22 IP / TCP / OTHER	374 B 🗼 140> 140> 140.	5 👰 49555 -> 443 (https) 🗸
<			) b

圖 10、 威染主機單純發送 SYN request,但中繼站已無回應。

#### 惡意程式排除方式-E 單位: 八、

- 1. 先將網路線拔除或關閉網路卡,以中斷連外網路。
- 2. 用工作管理員或 procexp 將惡意程序 ProtectedStorage.exe 刪除。
- 3. 將 C:\Users\username\AppData\Local\ProtectedStorage.exe 惡意程式移除。
- 4. 用 autoruns 檢查是否有惡意程式開機自動啟動,並刪除之。
- 5. 用掃毒軟體掃瞄系統。

雨事件上層為共同中繼站: 九、

- 1. 該中繼站是台中 Y 國中的套裝郵件伺服器。
- 2. 該伺服器被駭客入侵並開啟 Port 443 作為中繼接收流量使用。
- 該伺服器被入侵不久後,主機管理員已發現流量異常,故已經自行將惡意 程式移除,因此我們後來授權進去主機時已查不到任何痕跡。
- 4. 主機管理員也更改帳號密碼並加強 ACL 的 IP 登入限制。
- 5. 故測試E單位接收信件的惡意程式時候已經無法與中繼站建立連線。

### 建議措施

- 1. 以上事件的都是針對學術單位的 APT 郵件攻擊,且連至相同 IP 的中繼站。
- 2. 若有用 Outlook 收信,至選項安全信中心關閉預設的附件瀏覽功能。
- E 單位事件的惡意程式太明顯容易被識破,而 S 單位事件的惡意程式隱 藏較好比較不易察覺。
- 4. 一旦執行惡意程式都可能會讓個資外洩,盡速修改密碼。
- 5. 可疑郵件檔案請先用 Virustotal 線上掃毒,或用上傳至 Google docs 開啟 以避免受害。
- 6. 帳密定期更改並避免使用過於簡易的密碼。