# 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

# 前言

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。

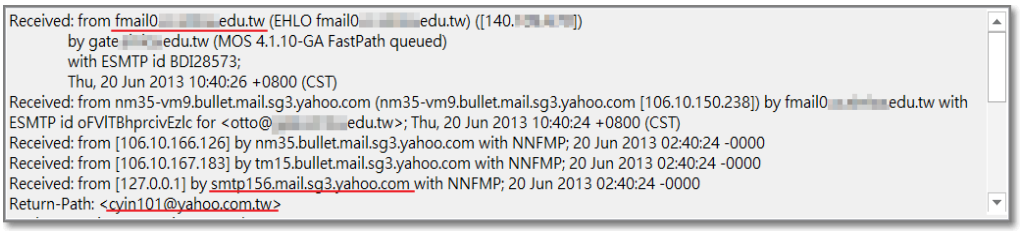
# 事件說明

## 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。


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。

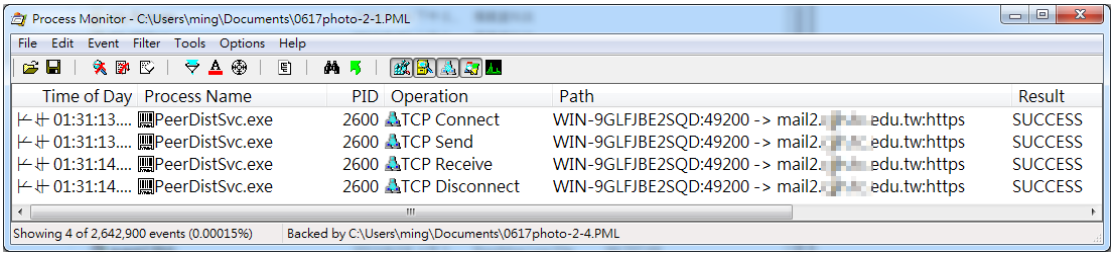

圖 1、『通訊錄.rar』解壓縮之後檔案

## 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。
3. 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『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。
6. 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。
7. 『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。



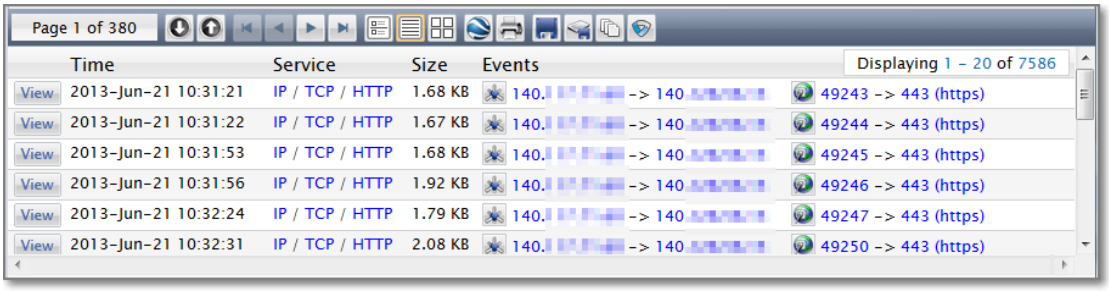



圖 3、惡意程式向中繼站主機建立連線

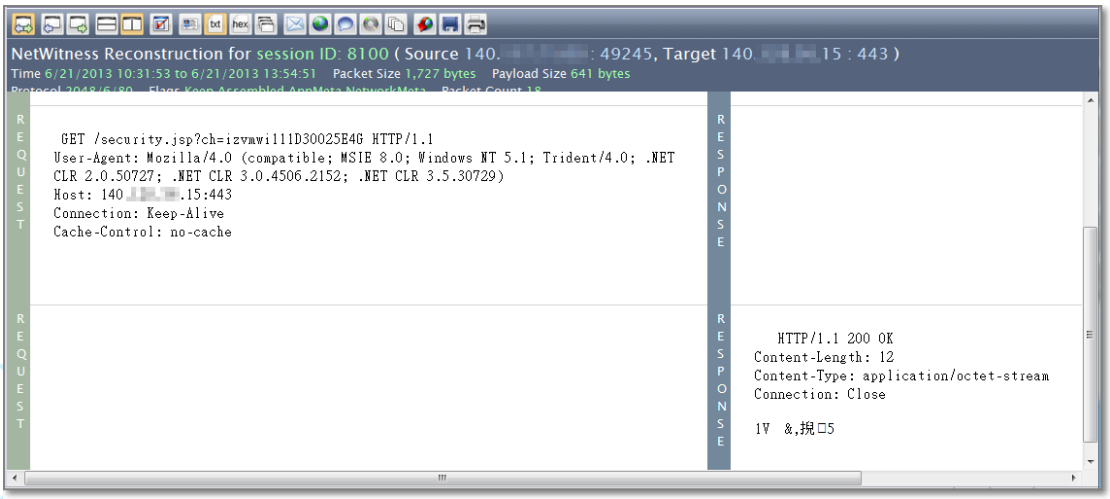



圖 4、測試主機向上層中繼站傳送加密資料，中繼站成功接收則回覆 OK

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。

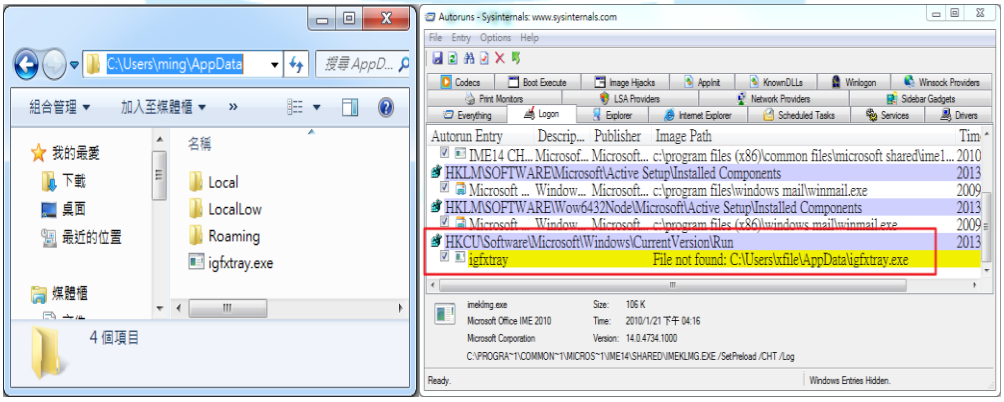



圖 5、igfxtray 的位置與自動執行

10. 『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。

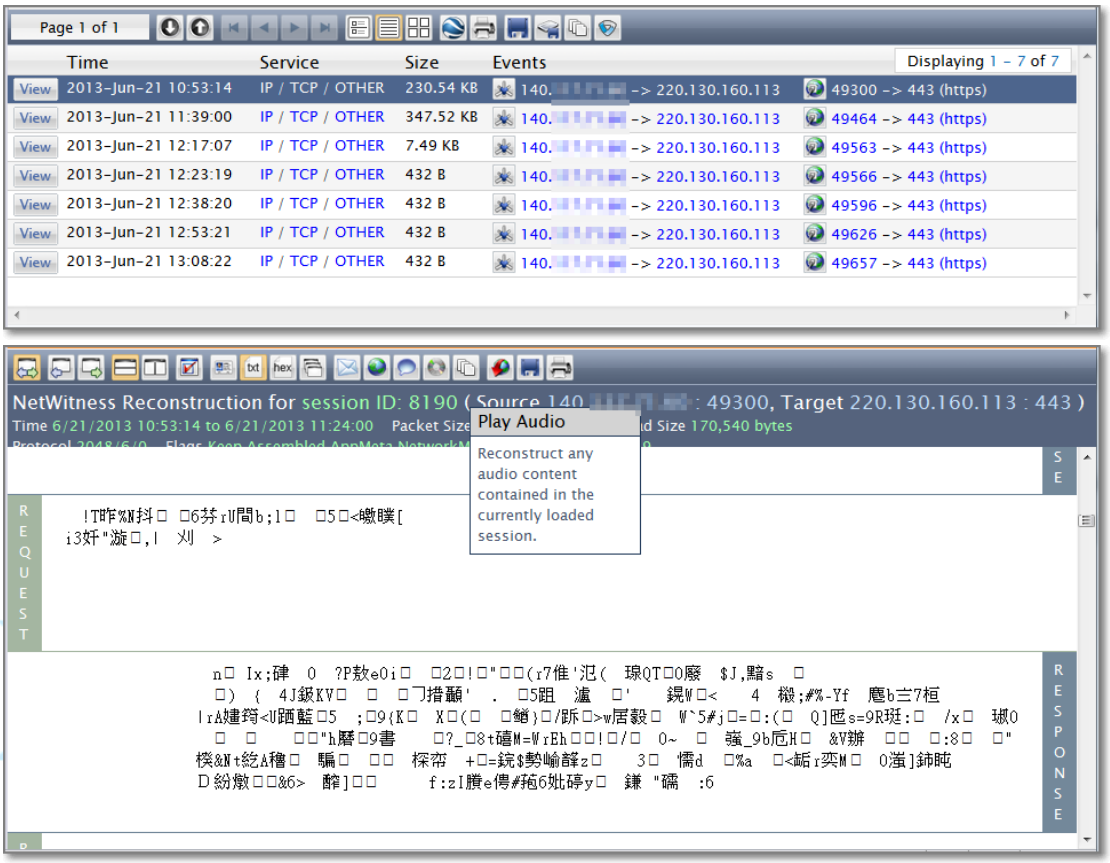



圖 6、受害主機向中繼站傳送加密資料，疑似使個資外洩

12. 程序監測工具紀錄出異常程式運作情形。

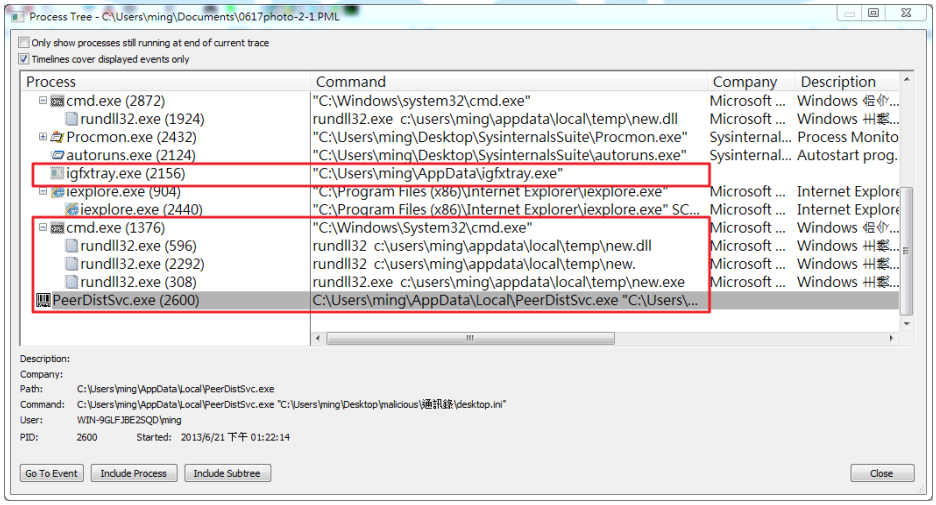
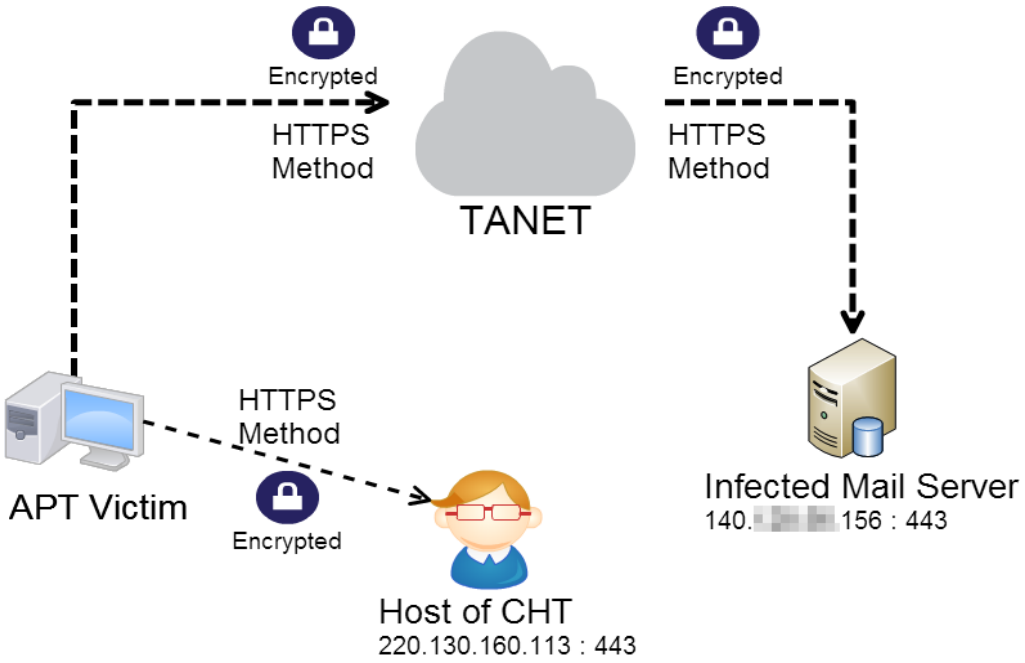



圖 7、紅色標記為惡意程式

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。
2. 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 <cyin101@yahoo.com.tw>
To: [redacted] <[redacted]tw>
Date: Tue, 25 Jun 2013 08:42:23
Subject: 102 年[redacted]期中報告

如有不明事宜，請洽詢聯絡人：劉燈鐘副主任（0936-231661）。
肅此 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。

## 七、 檢測過程-E 單位：

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。

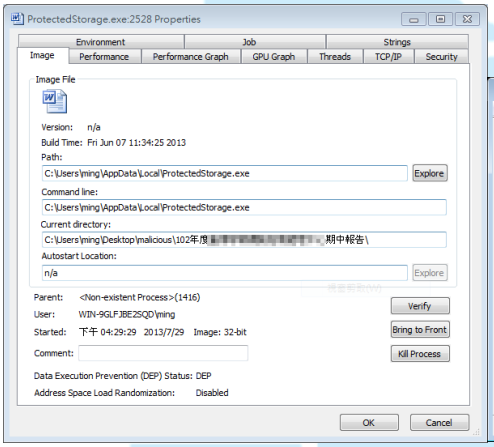



圖 8、『ProtectedStorage.exe』的內容

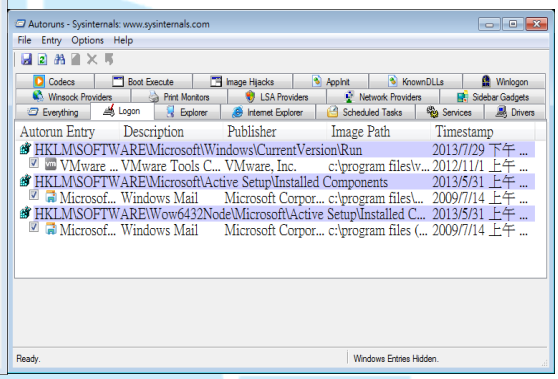



圖 9、註冊機碼無寫入開機自動啟動

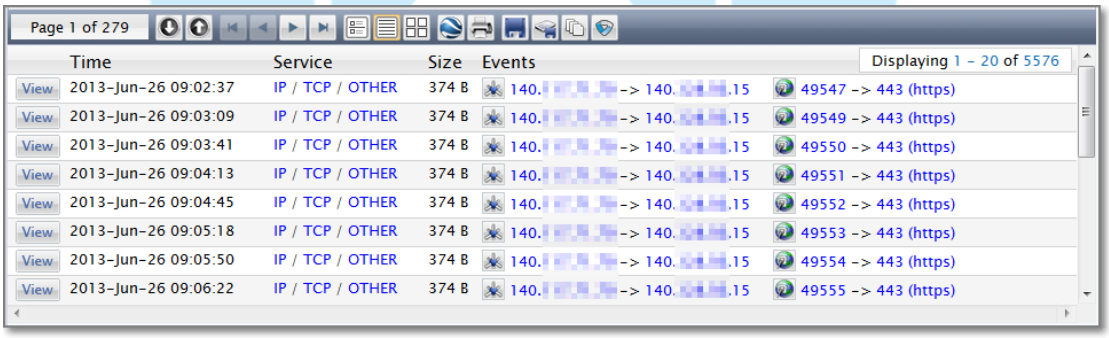



圖 10、感染主機單純發送 SYN request，但中繼站已無回應。

## 八、 惡意程式排除方式-E 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 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。

## 九、 兩事件上層為共同中繼站：

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。
3. 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。
3. 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。