# 個案分析-

# 帶有惡意程式的垃圾郵件

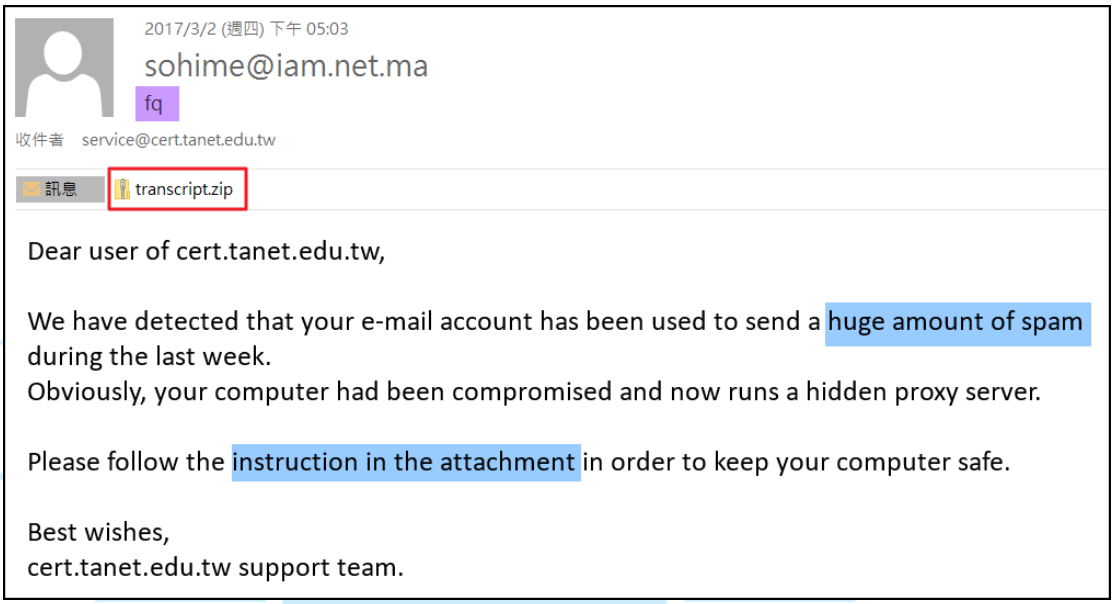
# SPAM 攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

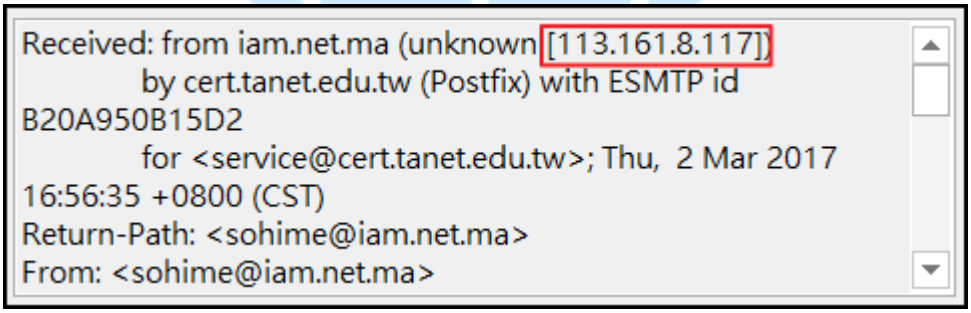
106 年 5 月

# I. 事件簡介

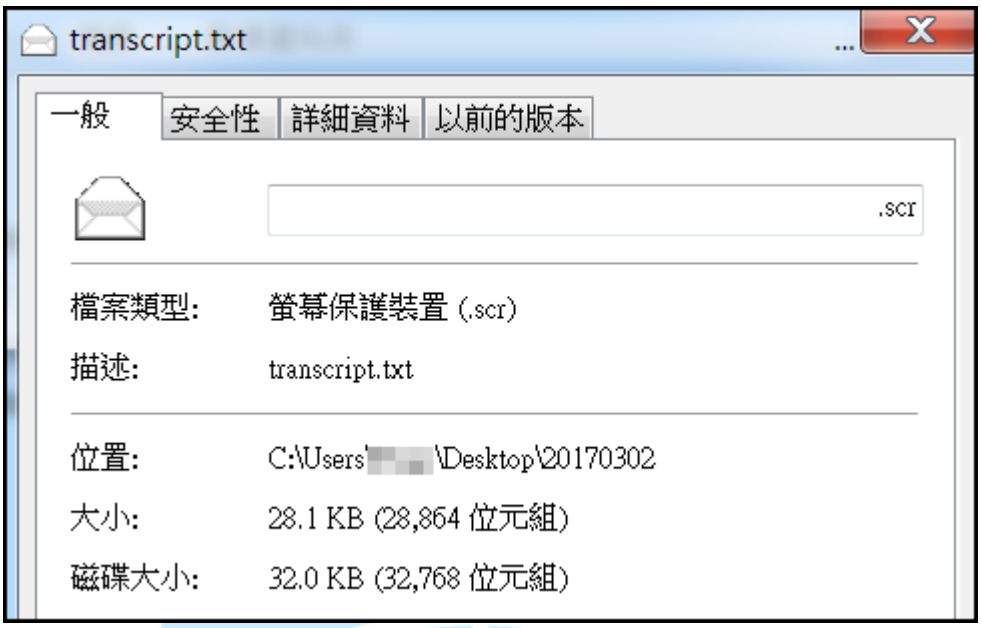
1. 近期發現有針對本單位進行垃圾郵件 SPAM 攻擊，其郵件以“fq”作為主旨，且內容為述說我們大量發送 SPAM 郵件，並要求依照信件內容開啟附加檔案進行修補感染，實質上為惡意程式的壓縮檔案“transcript.zip”。




2. 這次事件收件者位址為單位的公開服務地址，故有心人士會容易取得並且嘗試進行滲透。從郵件 Header 檢查發信者的 IP，為來自越南的 113.161.8.117，而非位於寄件者的網域(.ma)國家摩洛哥，表示寄件者名稱是偽造的。

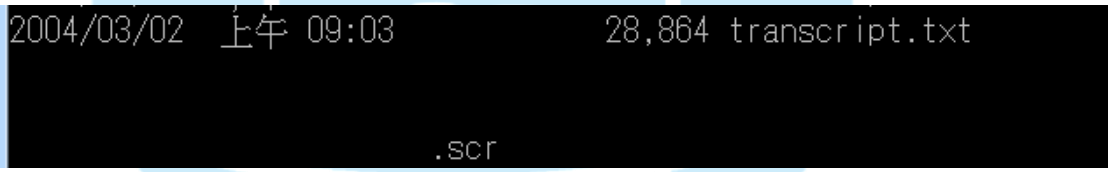



3. 郵件附加檔案解壓縮後，為一支偽裝成文件檔 TXT 的 SCR 執行檔“transcript.txt….scr”，透過在檔案名稱尾端插入大量空白字元來遮蔽其附檔名 SCR，誘使使用者不注意執行。

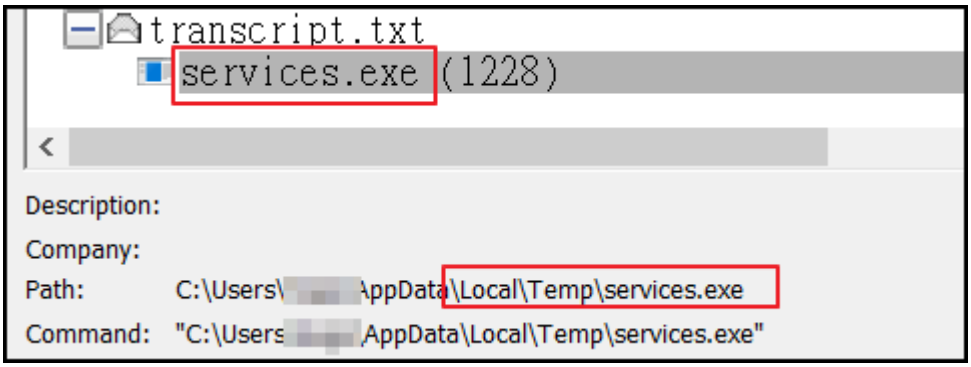



## II. 事件檢測

1. 在測試惡意程式時候，預先使用 Win7(x86)來開啟執行該惡意程式“transcript.txt.scr”，因為預設檔名插入大量空白過於冗長，導致 32 位元系統無法正常辨識執行。因此該惡意程式只對於 64 位元系統有效。

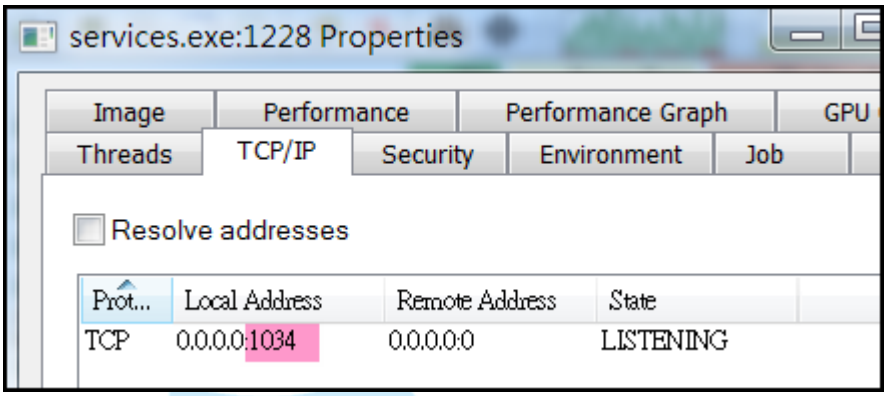



2. 實際執行惡意程式 scr 檔案後，在視窗上並無出現任何訊息，但透過 procexp 檢視背景程式狀態，可以看到 scr 惡意程式產生出新的子程式 services.exe。

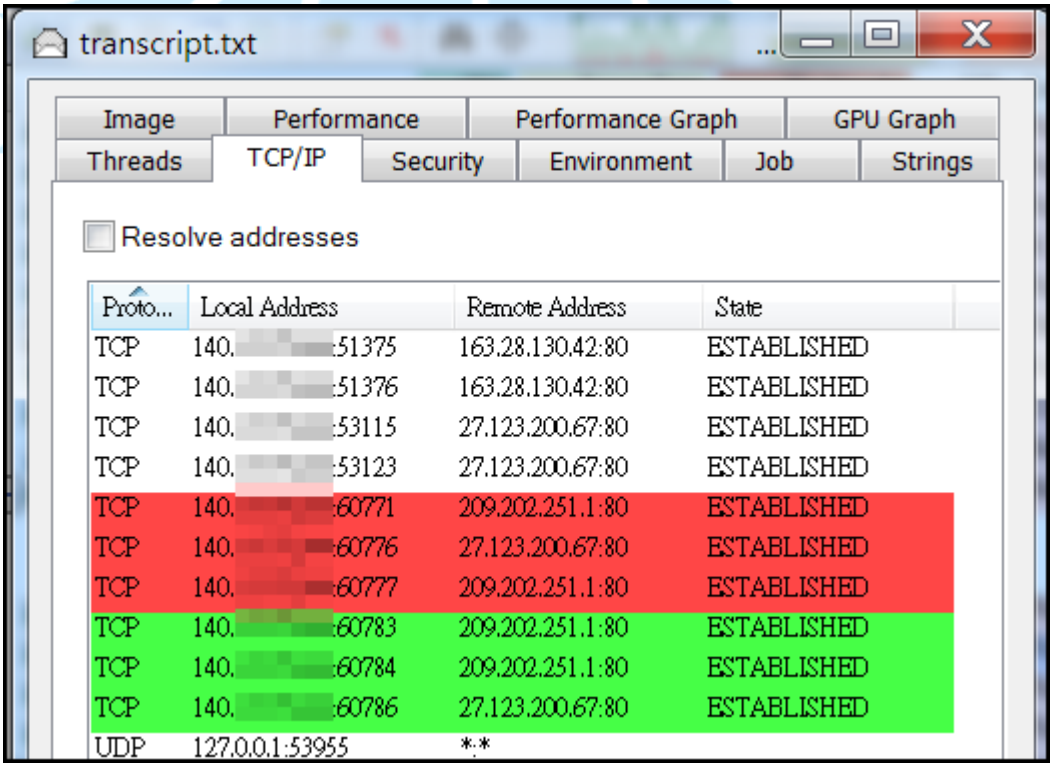



3. 該 services.exe 是由 transcript.txt.scr 所產生，並且位於暫存資料夾

內，檢查 services.exe 的連線狀態能看出有開啟 Port Listening，表示能夠讓駭客或 C&C 連入做控制。



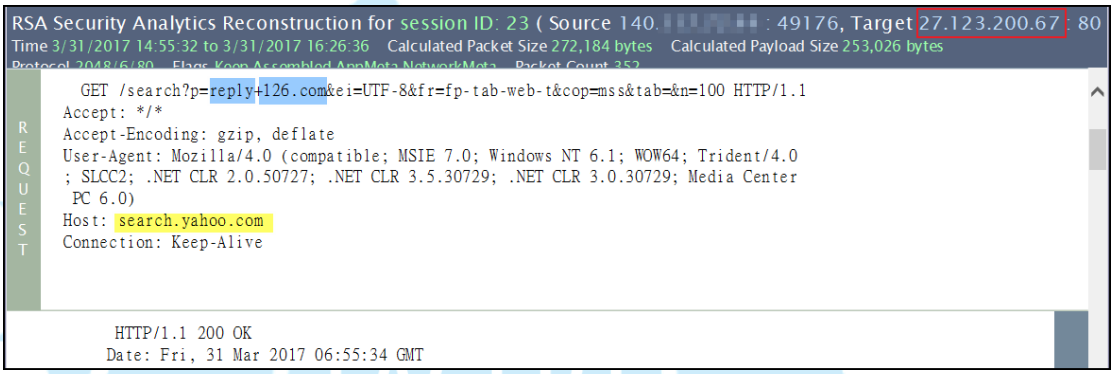

4. 在檢查父程式 transcript.txt.scr 的連線狀態，可以看到有大量的對外連線和流量，檢查以下連線 IP 幾乎都是搜尋引擎網站。

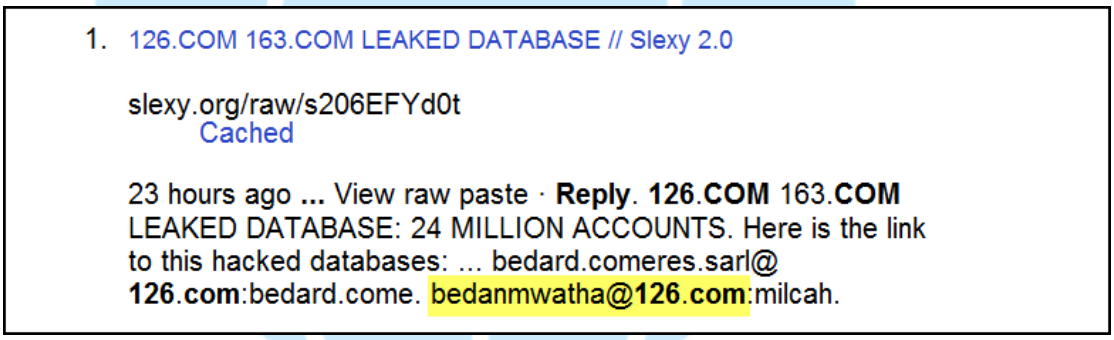



5. 除此之外還觀察到惡意程式 transcript.txt.scr 除了會連到搜尋引擎網站，還會產生大量對外 port 25 的連線，可能是正在對外發送 SPAM 郵件。

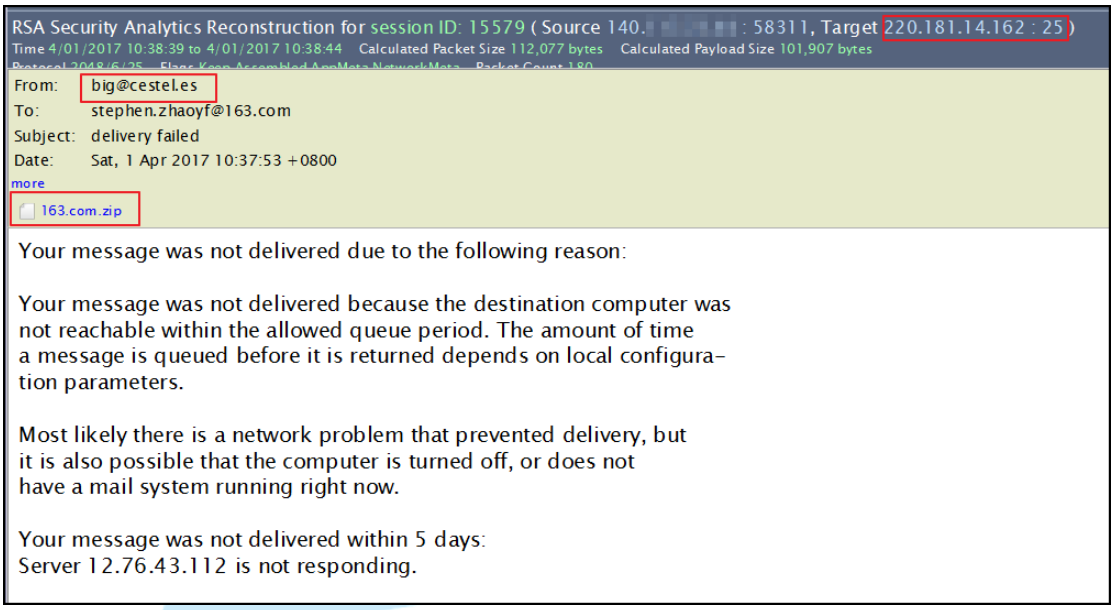
| Process | PID | Protocol | Local Address | Local Port | Remote Address | Remote Port |
|---|---|---|---|---|---|---|
| [System Process] | 0 | TCP | 140. | 62479 | 173.194.67.27 | 25 |
| [System Process] | 0 | TCP | 140. | 62487 | 74.125.201.26 | 25 |
| [System Process] | 0 | TCP | 140. | 62485 | 142.103.226.211 | 25 |
| [System Process] | 0 | TCP | 140. | 62482 | 164.15.128.114 | 25 |
| [System Process] | 0 | TCP | 140. | 62488 | 173.194.175.26 | 25 |
| [System Process] | 0 | TCP | 140. | 62489 | 64.233.189.26 | 25 |
| [System Process] | 0 | TCP | 140. | 62484 | 173.38.212.150 | 25 |
| [System Process] | 0 | TCP | 140. | 62490 | 173.194.219.26 | 25 |
| [System Process] | 0 | TCP | 140. | 62492 | 173.37.147.230 | 25 |
| [System Process] | 0 | TCP | 140. | 62491 | 134.184.129.114 | 25 |
| [System Process] | 0 | TCP | 140. | 62494 | 72.163.7.166 | 25 |
| [System Process] | 0 | TCP | 140. | 62503 | 134.58.240.2 | 25 |

6. 從封包內容來檢視，transcript.txt 連到的 port 80 幾乎都是各大家的搜尋引擎，並且大量搜尋可用的電子郵件網域，並且開始準備發送 SPAM。

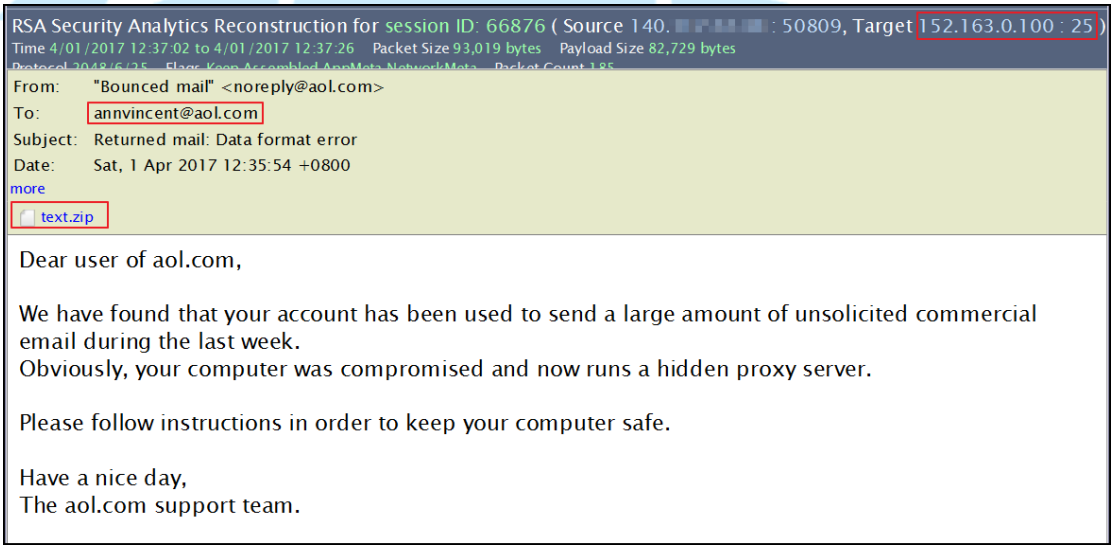


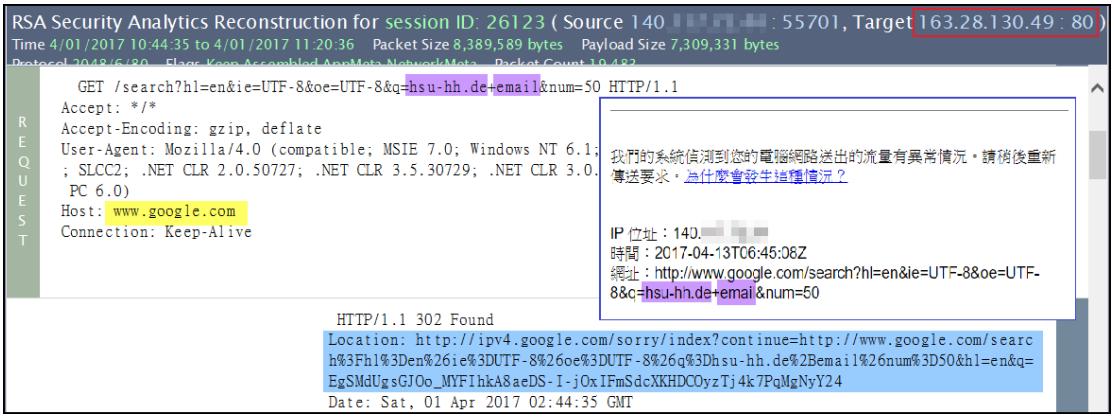

7. 檢查其中一比較完整的 SPAM 封包紀錄，得知惡意程式會偽造發信人地址，並且發送給搜尋到的 domain 為 163.com 收件者，通常會夾帶惡意檔案。



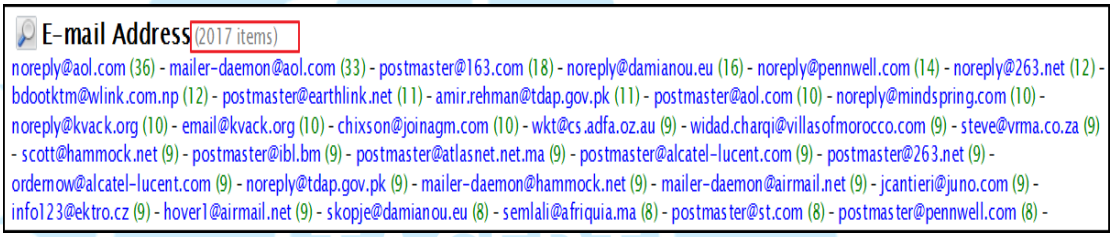

8. 檢查惡意程式發送較多的網域是 aol.com 的郵件來看，其內容格式來看與本事件收到的郵件內容相符，表示其不算是 APT 攻擊，只是亂槍打鳥方式的 SPAM 惡意郵件。




9. 惡意程式 Transcript.txt.scr 在大量向搜尋引擎查詢 domain 資料後，Google 的網站會開始進行存取封鎖，因為有異常大量連線的偵測機制。

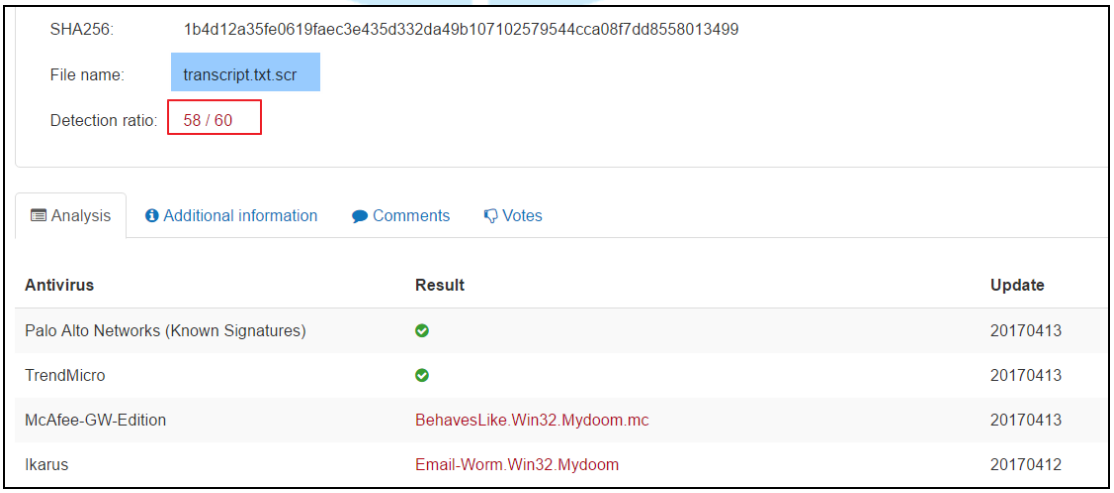



10. 從本次測試一周期間統計出，至少有對外部相異 2000 個 email 位址發送 SPAM 攻擊，以國別來說也有 59 個國家受害。發送 SPAM 期間也會消耗大量網路頻寬而可能造成網路壅塞。

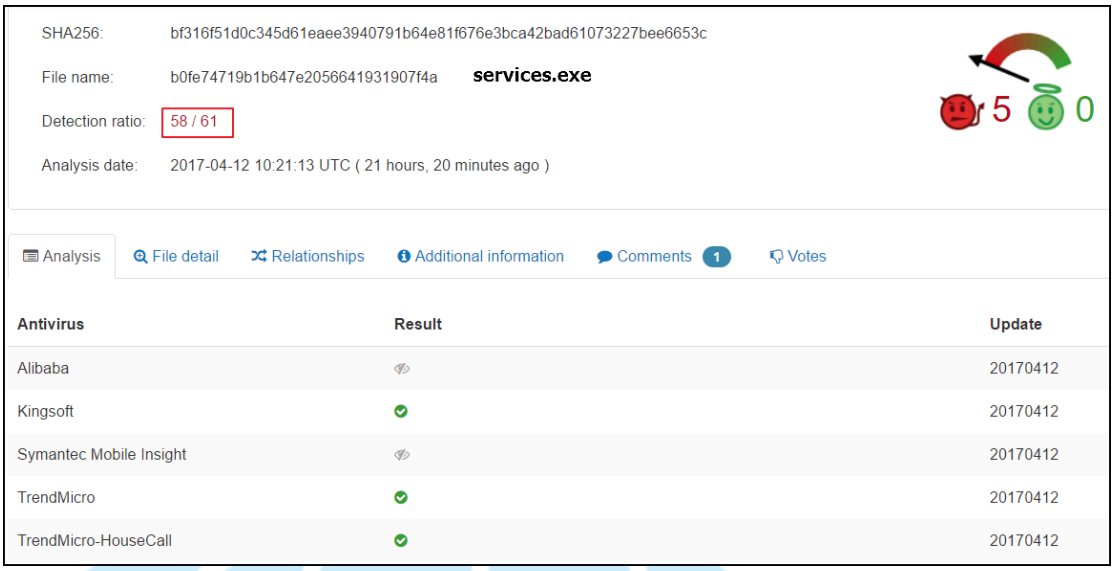




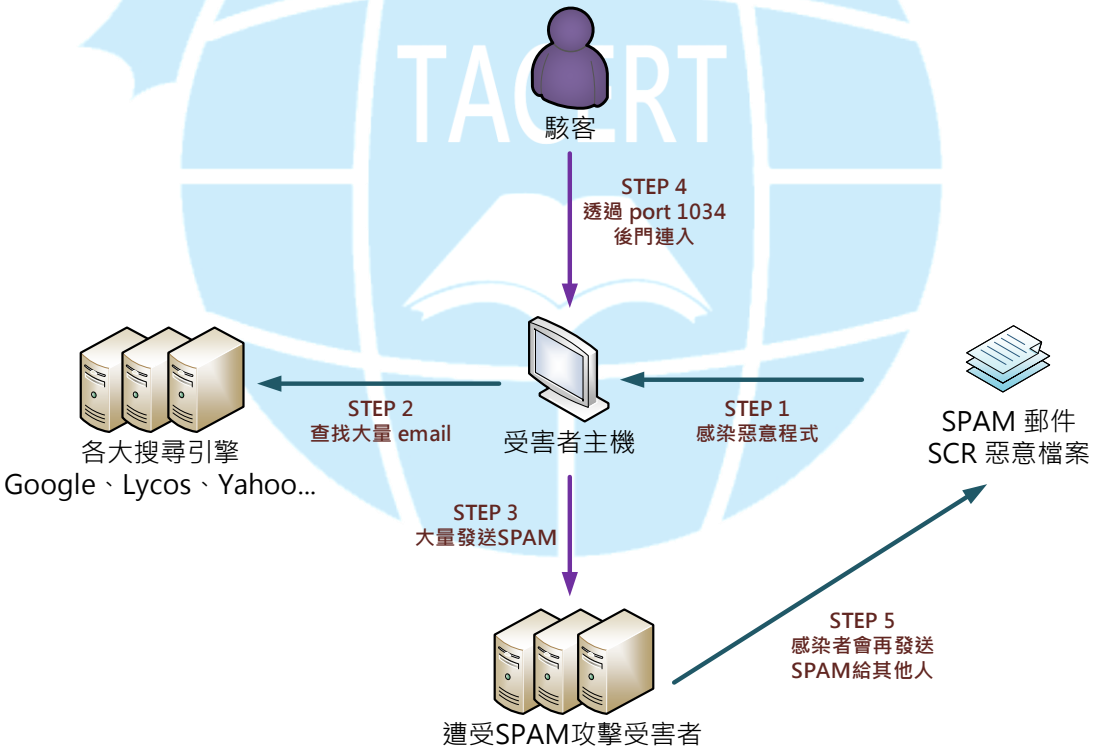
11. 最後將惡意程式樣本 transcript.txt.scr 送到 Virustotal 檢測，檢測為惡意的比例為 58/60 相當明顯，但也是有知名防毒廠商尚未檢測出。



12. 另一支程式 services.exe 透過 Virustotal 檢測，檢出比例為 58/61 相當高，不過依然還是有知名防毒廠商尚未檢測出。




## III. 網路架構圖




1. 受害者開啟 SPAM 郵件中的附加檔案，為偽造成 TXT 的 SCR 惡意程式。
2. 受害主機會開始向外部的各大搜尋網站查找可用的郵件網域名稱。
3. 受害主機開始向搜尋到的 mail 位址發送大量的惡意 SPAM。

4. 駭客 C&C 可能透過 port 1034 連入感染主機，並下達其他攻擊指令。
5. 當新的受害者也感染惡意檔案後，也會開始對外發送 SPAM 郵件並成為新的 Botnet。

## IV.建議與總結

1. 此案例為惡意 SPAM 郵件攻擊，並附加偽造成 TXT 文件檔的 SCR 執行檔惡意程式。
2. 該惡意程式在副檔名 SCR 前塞入.TXT 和冗長的空白字元進行偽裝，一旦執行後會開啟 port 1034 為 Listen 狀態。
3. 惡意程式 SPAM 攻擊之前會大量向搜尋網站查找可攻擊的電子郵件網域，並且再對外進行 port 25 的 SPAM 郵件攻擊。
4. SPAM 郵件有可能會偽造寄件者的郵件地址為相同網域的地址，增加後害者上當的機率。
5. 該事件受害者同時也會成為攻擊其他人的加害者，並且成為殭屍網路的主機讓駭客使用。
6. 所幸該惡意程式並不會寫入開機自動啟動區，當使用者重開主機後網路攻擊行為就不會再出現。
7. 此類型的社交工程郵件近年來一直很多，有的惡意程式多為加密勒索軟體，更應提高警覺避免誤觸。