個案分析-

發送垃圾郵件的郵件病毒分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/3

I. 事件簡介

1. 近期接獲國外通知說，本單位疑似有 email 大量發送垃圾郵件，造成許多困擾。
2. 通知信中對方有附上垃圾郵件夾的附加檔案 document.zip，本單位將進行虛擬主機測試。
3. 由於對方並無提供原始垃圾郵件的原始碼，檢查後本單位並無有濫發垃圾郵件事實，初步判定應該是被偽造成的郵件地址。

From: schnews@brighton.co.uk [mailto:schnews@brighton.co.uk]
Sent: Saturday, January 16, 2016 10:20 AM
To: service@cert.tanet.edu.tw
Subject: Delivery reports about your e-mail

Dear user service@cert.tanet.edu.tw,

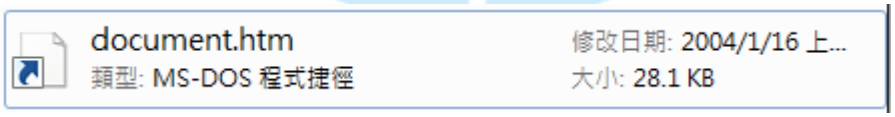
We have found that your e-mail account was used to send a huge amount of junk email messages during this week.
We suspect that your computer had been infected by a recent virus and now contains a hidden proxy server.

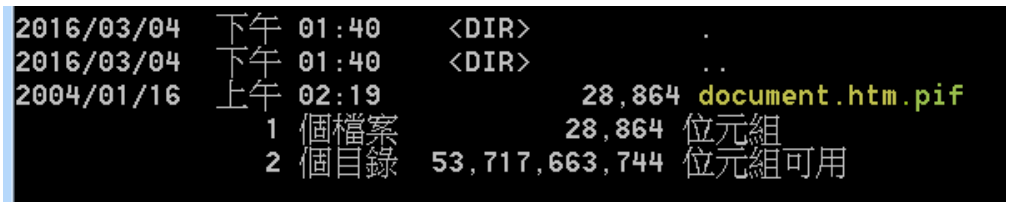
We recommend you to follow instruction in order to keep your computer safe.

Have a nice day,
The cert.tanet.edu.tw team.

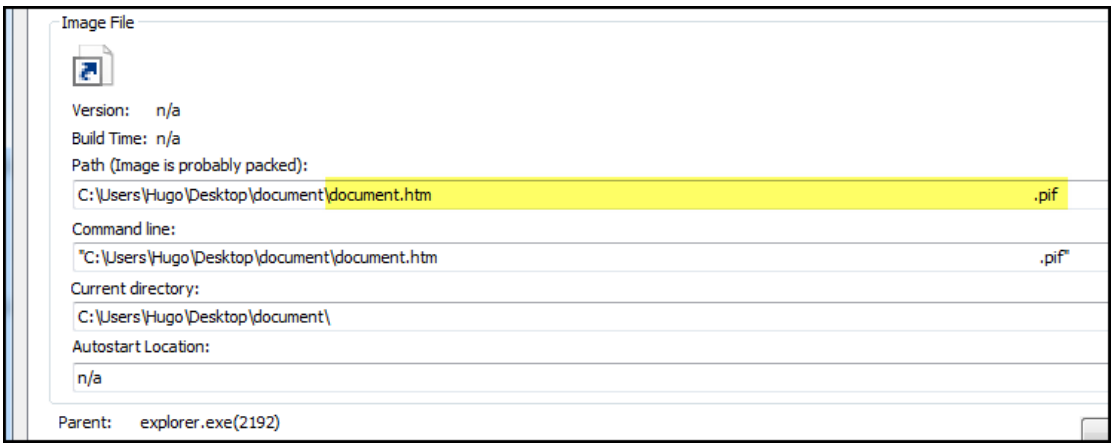
II. 事件檢測

1. 首先將 document.zip 解壓縮後，產生出一個名為 document.htm 的 PIF 檔案，在 windows 檔案顯示中的附檔名 PIF 不會顯示出來，藉而隱藏偽裝成 htm 的文件檔。事實上它是一個 MS-DOS 的執行檔，透過 MS-DOS 模式查詢就能看出其檔名。

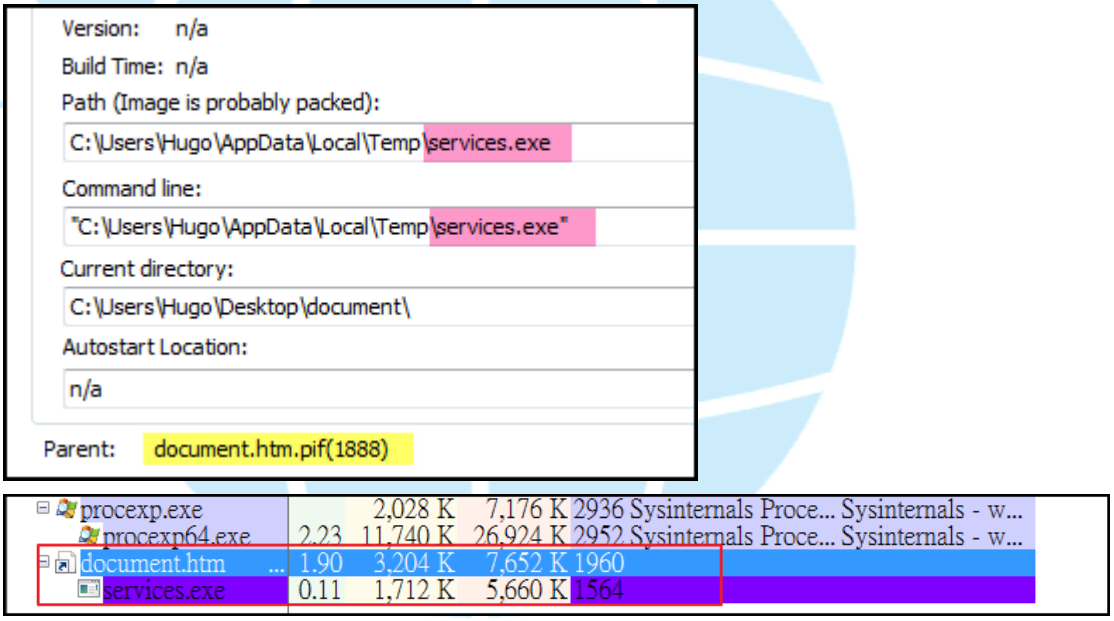




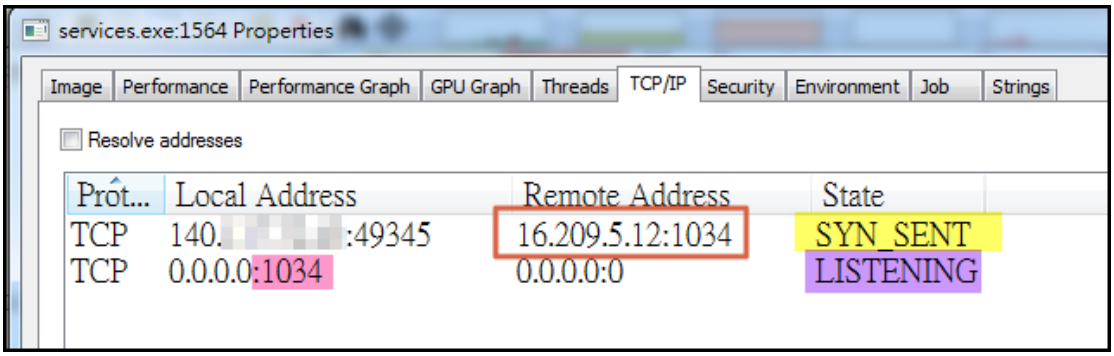
2. 實際測試執行該惡意程式 document.htm.pif 後，可以在系統背景看到該程式的執行狀態。



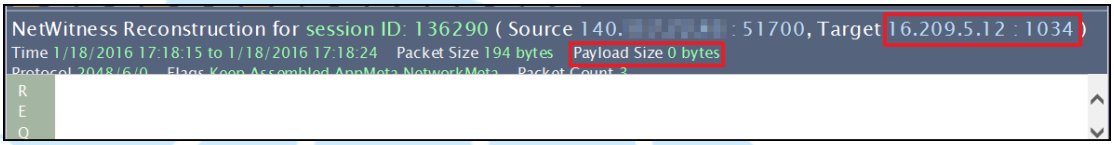
3. 該程式會在隱藏路徑資料夾中產生一個 services.exe，並且由父程式 PIF 檔呼叫執行。



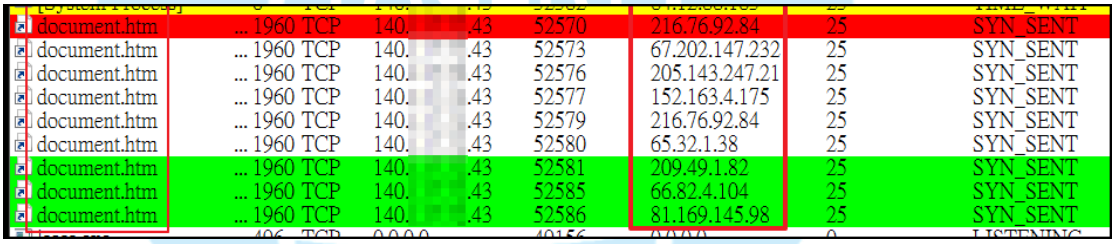
4. 惡意程式的網路行為主要是由 services.exe 進行對外通訊，會連線到外部 IP 的 port 1034 進行資料傳送，從紀錄中對外的連線 IP 就有 244 筆。同時該程式也會開啟 TCP port 1034 為 LISTENING 狀態，以便接收外來連線資料，約有 22 筆連線 IP 數。



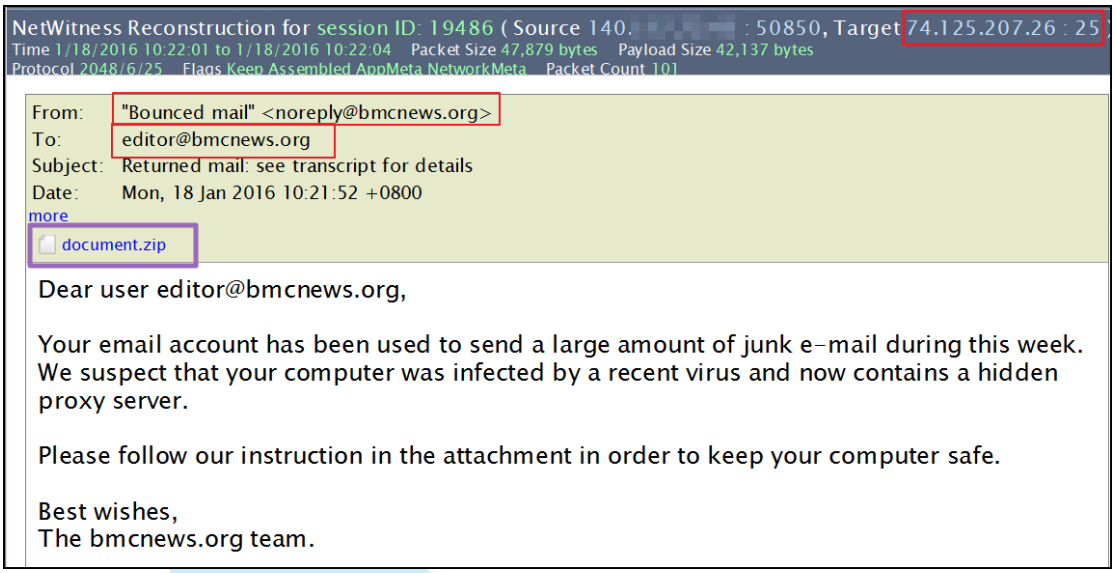
5. 從往來的 port 1034 連線紀錄中，例如連線到美國 16.209.5.12:1034 的封包，發現該連線封包的 payload size 皆為 0 bytes，表示該連線並沒有真正建立通訊，只是以封包做為探測監控用途。



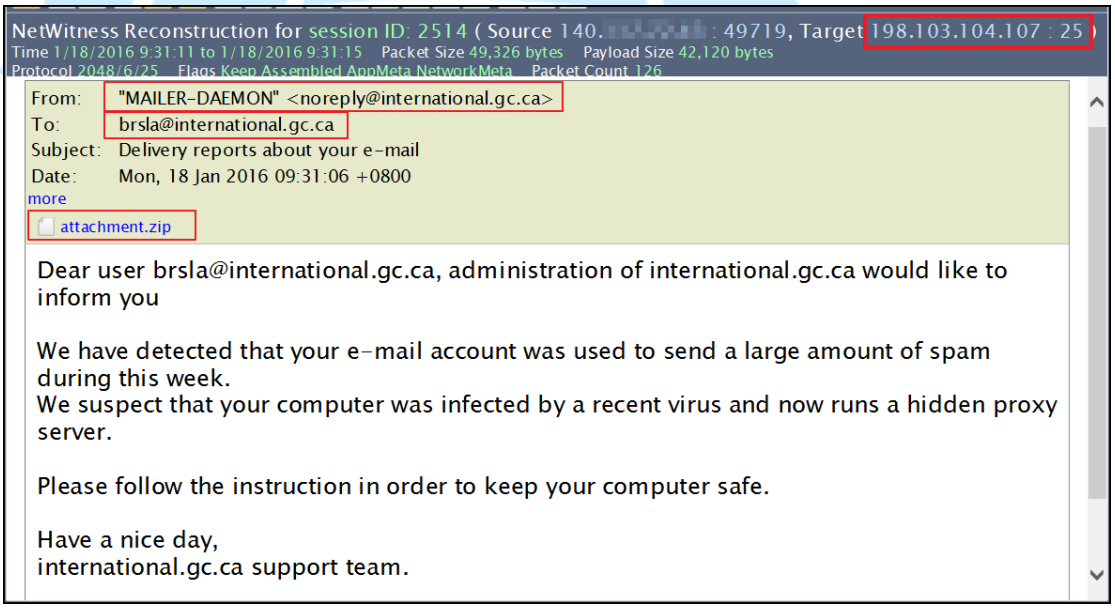
6. 從 Procexp 觀看主機背景程式運作情形得知，除了 services.exe 有網路行為之外，其父程式 document.htm.pif 更有大量的網路連線產生。並且占用大量頻寬開始對外郵件主機的 port 25 發送資料。



7. 從封包紀錄觀察中可以知道，該程式會對外主機進行 SMTP 協定的連線就有 3087 筆的 IP 數量，其原理就是發送大量的垃圾病毒郵件給一般電子郵件使用者，並且偽造發送者的位址給對方並且夾帶同樣的病毒誘使對方開啟。



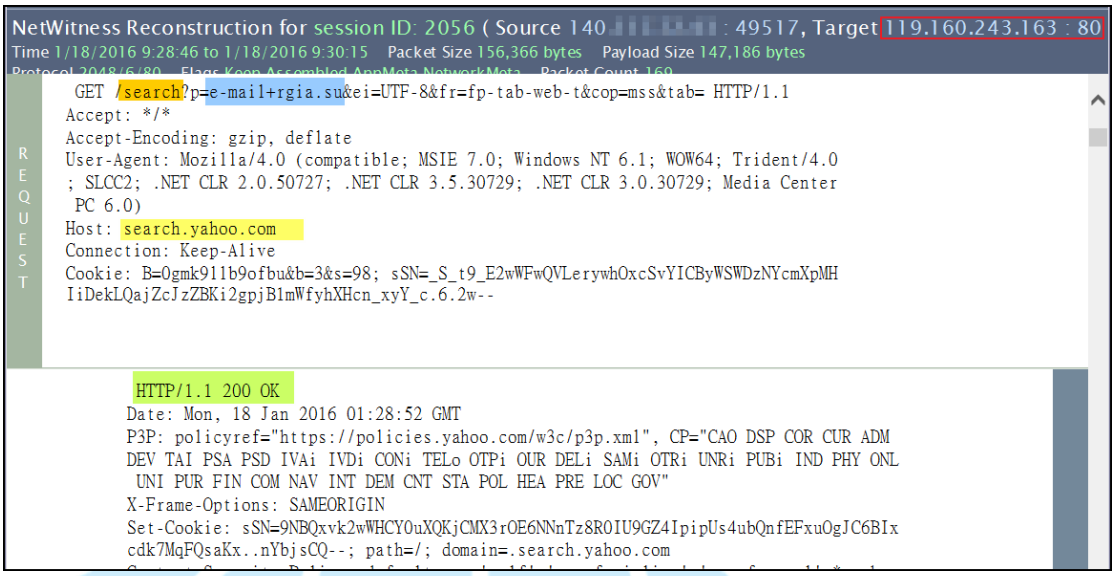
8. 惡意郵件在發送時，寄件者都會偽造成與收件者同網域的位址，且內容主要都是訴說收件者可能中毒再發送大量垃圾郵件，並請打開附件檢查主機安全。而事實上附件本身就是造成此影響的惡意程式。



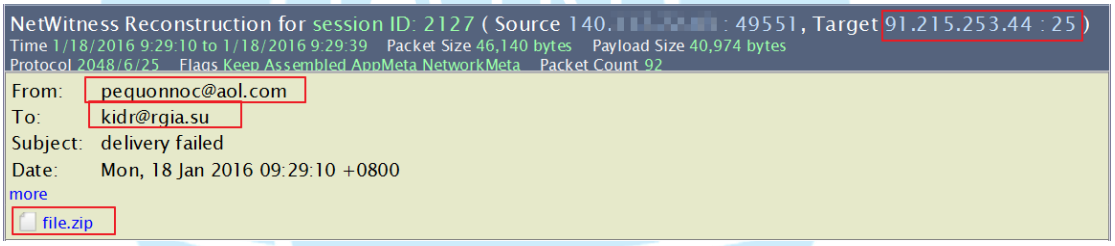
9. 既然 document.htm.pif 會大量發送惡意電子郵件，則收件者地址必有規則可循。從封包紀錄中可以看到有大量 HTTP 的封包進行 search request 的動作，主要都是連線到 「search.lycos.com、 search.yahoo.com、www.google.com、www.altavista.com」等常見的收尋引擎網站進行收件地址查詢。

10. 例如其中一筆資料是惡意程式向 search.yahoo.com 進行 HTTP GET 進

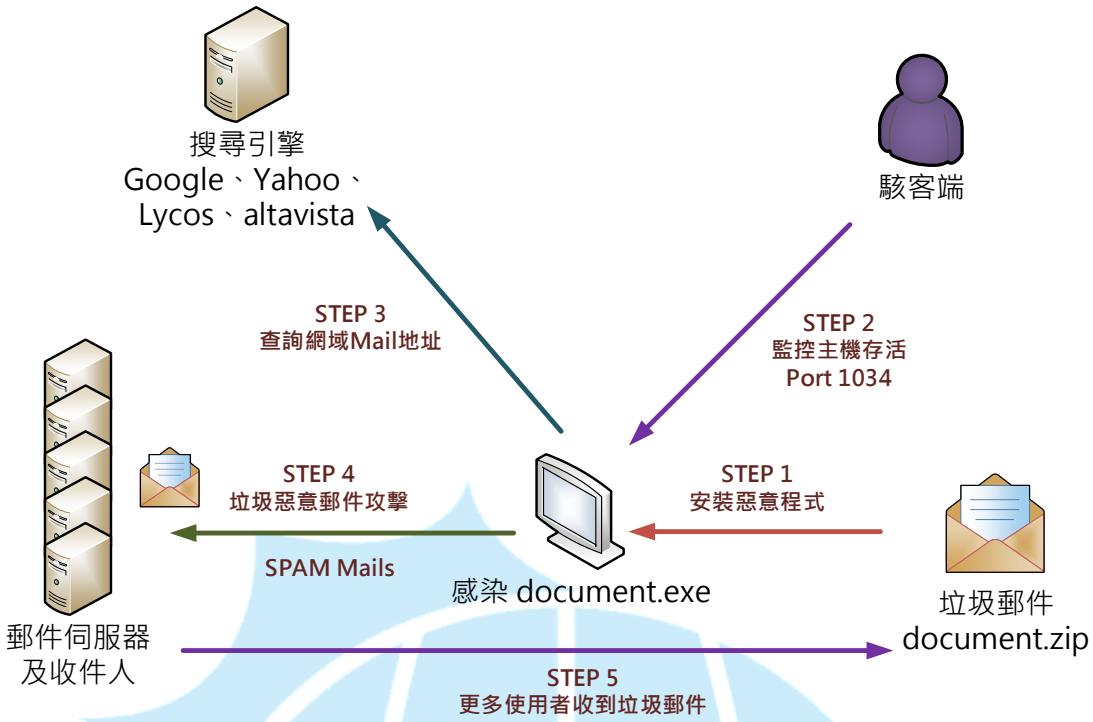
行關鍵字“e-mail+rgia.su”搜尋，將找尋到的網域電子郵件列為收件人清單發送，因此只要能被搜尋到的電子郵件都有可能會接收到垃圾郵件。



11. 搜尋網域 riga.su 的郵件紀錄，有一筆垃圾郵件是透過偽造寄件者 pequonnoc@aol.com 寄給 kidr@rgia.su ，並且主旨是“delivery failed”和附件 file.zip 的病毒。



III. 網路架構圖



1. 收到夾帶惡意程式 document.zip 的電子郵件。
2. 主機感染惡意程式後開啟 port 1034 讓駭客端可以連線。
3. 感染主機會向特定的搜尋引擎網站查找可攻擊的電子郵件網域。
4. 感染主機開始向這些網域的郵件伺服器發送垃圾郵件給使用者。
5. 使用者感染到垃圾郵件中的惡意程式進而擴散。

IV.建議與總結

1. 此個案主要是透過惡意的 SPAM 郵件進行傳播感染，而且會偽造郵件寄件人地址誘使對方上鉤開啟郵件附件。
2. 惡意附件檔案會偽造成 htm 文字檔案，事實上是 pif 的 MS-DOS 執行檔案。
3. PIF 在 Windows 系統中的視窗瀏覽下副檔名是隱藏不顯示，就算是開啟顯示副檔名功能也是如此。
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，並且大量發送惡意郵件給其他使用者。
5. 感染主機同時也會開啟 port 1034 接受駭客或其他主機的連線監控。
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。

7. 此案例的病毒並不會常駐在開機自動啟動，因此只要重新開機惡意程式就不會被執行。
8. 此類惡意程式大多能被防毒軟體偵測到，因此務必將防毒軟體更新至最新。