個案分析-

偽裝成 Outlook 更新檔案之惡意程式事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/02

I. 事件簡介：

A. 近期網路上出現一個疑似 Outlook 郵件收發軟體的更新檔案，檔案解壓縮後為『Outlook.exe』，此檔已被 Virustotal 偵測出為惡意程式。

B. 其他相關事件報導網址

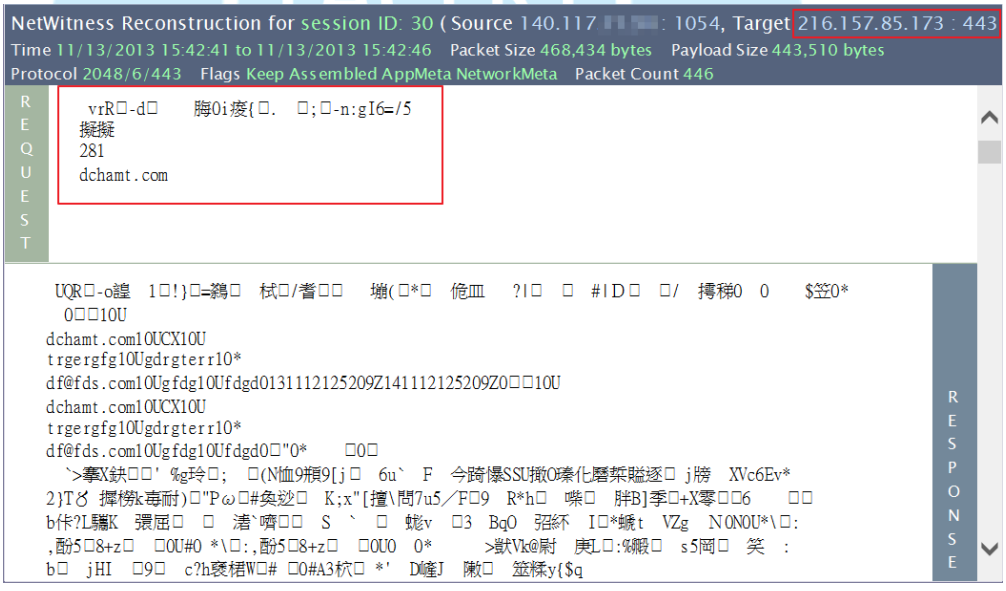
1. http://blog.dynamoo.com/2013/11/important-new-outlook-settings-spam.html
2. http://techhelplist.com/index.php/spam-list/383-important-new-outlook-settings-virus

II. 事件檢測：

A. 透過 VMware 虛擬機器，並使用 Win7 (x64)及 Wireshark 封包側錄。

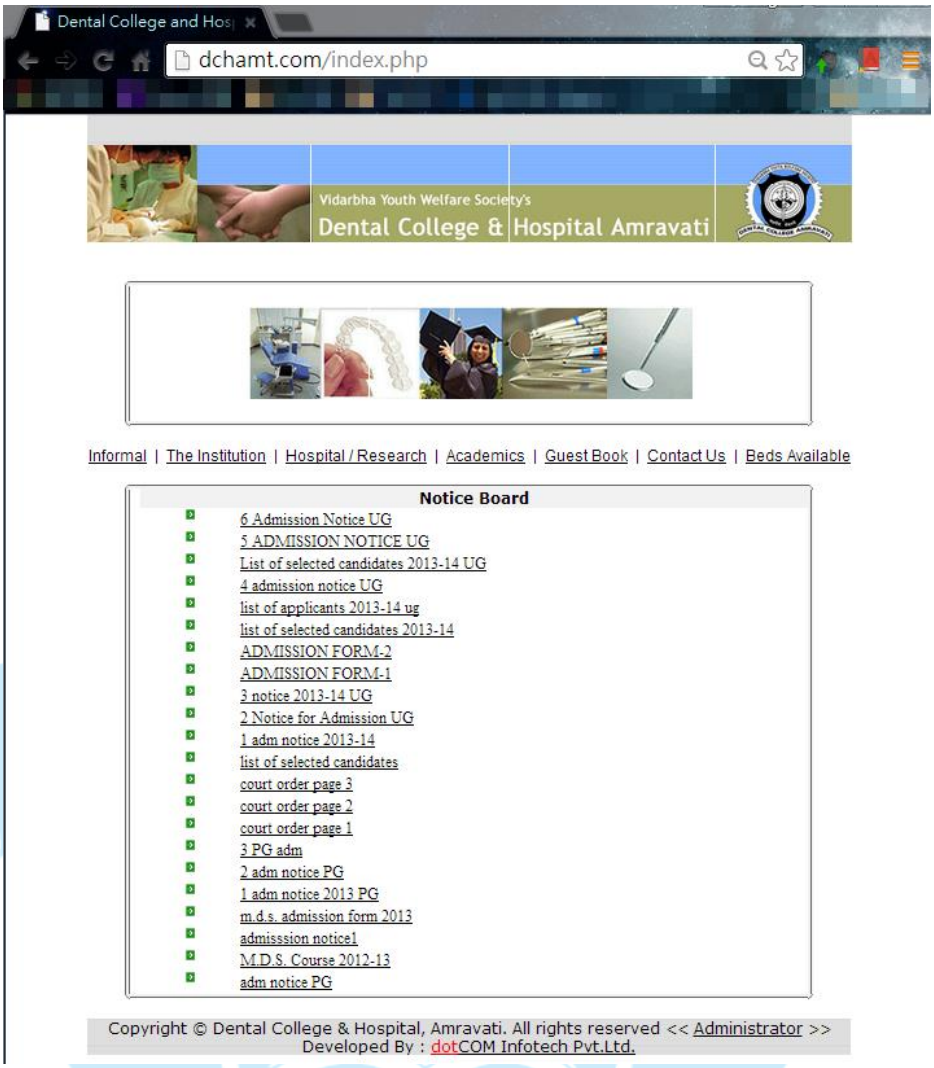
B. 執行惡意程式『outlook.exe』後，會呼叫 WinMail.exe 至「http://crl.microsoft.com/pki/crl/products/」取得 “microsoftrootcert.crl” 和 “MicCodSigPCA_08-31-2010.crl” 憑證撤銷清單。

1. 接著會透過 HTTPS 連線至『dchamt.com』，該主機 Port 443 疑似被利用來接受感染主機的報到訊息，加密訊息中帶有明文 dchamt.com。



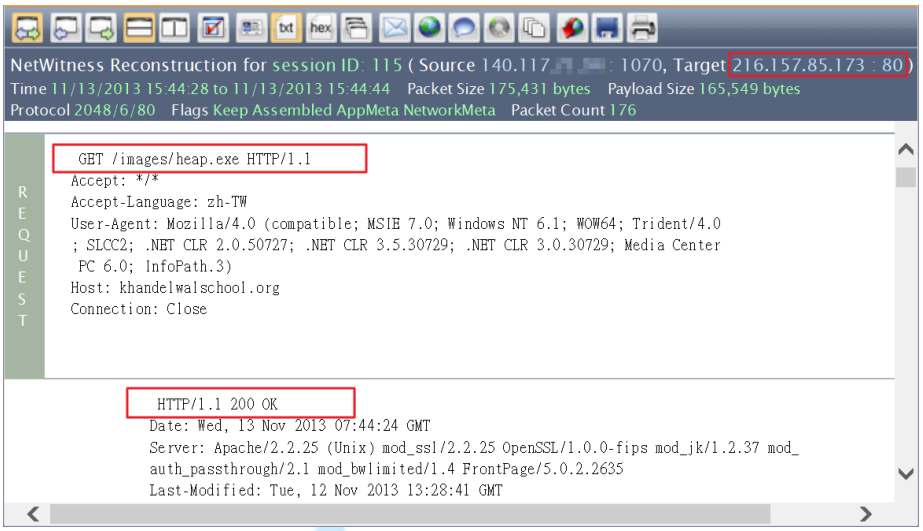
2. 此網域名稱已被部分的防毒軟體判定為惡意網址，解析出來是位於印度的 IP「216.157.85.173」，但反解析的網域名稱為「ns1.dotcominfotech.co.in」且 Port 53 是 OPEN，應同時為一台 DNS

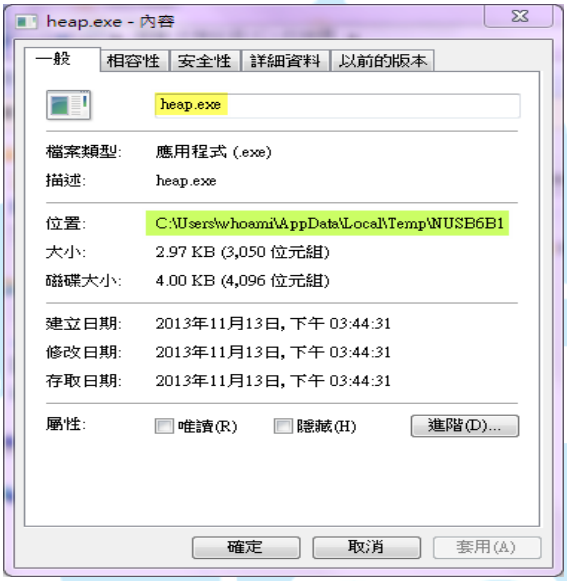
Server。



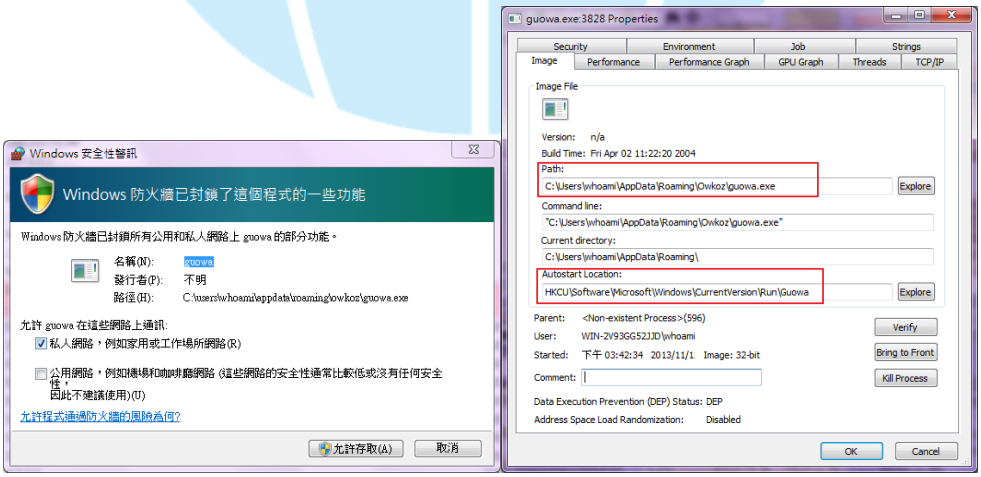
圖、此為上層報到用主機的頁面

3. 隨後會再向『http://khandelwalschool.org』下載 /images/heap.exe，網域名稱解析出的 IP 同為 216.157.85.173，明顯被駭客入侵註冊惡意網域做為跳板。

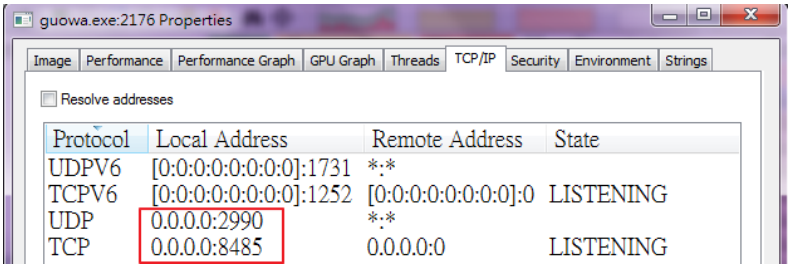




C. 執行惡意程式『outlook.exe』後，防火牆會詢問是否同意一個存取網路權限程式『guowa.exe』的執行，允許存取確認後該程式將於背景執行，讓使用者不易察覺異狀。

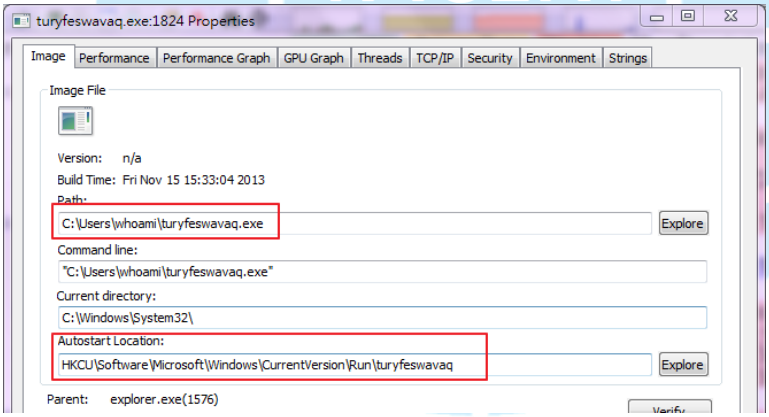


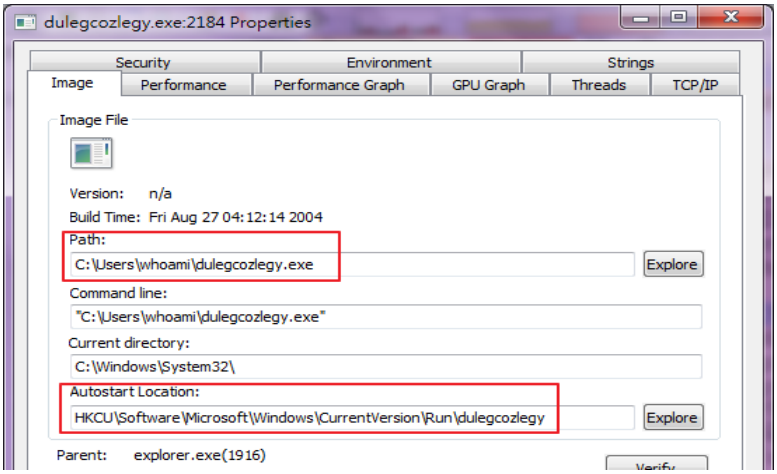
1. 透過 procexp 可以看到該程式『guowa.exe』的相關資訊，藏匿於隱藏目錄 C:\Users\XXX\AppData 底下，並會寫入註冊機碼開機自動執行。
2. 『guowa.exe』會開始進行網路的連線動作，會開啟本地端的 TCP port 8485 和 UDP port 2990 來接收命令資料。

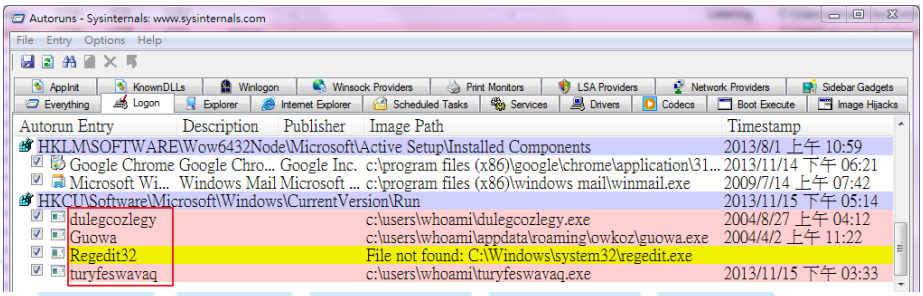


3. 從紀錄上發現至少有 43 個國家及 155 筆相異 IP 成功透過 tcp port 8485 傳入指令要求大量資料回覆，但指令及資料都經過駭客加密。
4. 從紀錄上發現至少有 163 個國家及 10000 筆相異 IP 成功透過 udp port 2990 傳入指令要求小量資料回覆，但指令及資料都經過駭客加密。
5. 『guowa.exe』也會向「http://crl.geotrust.com/crls/」GET “secureca.crl” 憑證撤銷清單。

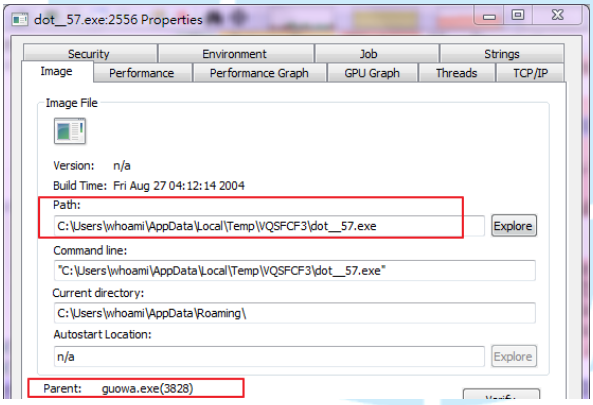
D. 過一段時間後會再產生兩個惡意程式於背景執行，分別為『turyfeswavaq.exe』和『dulegcozlegy.exe』，皆位在使用者的家目錄下，並且都會寫入註冊碼開機後自動執行。



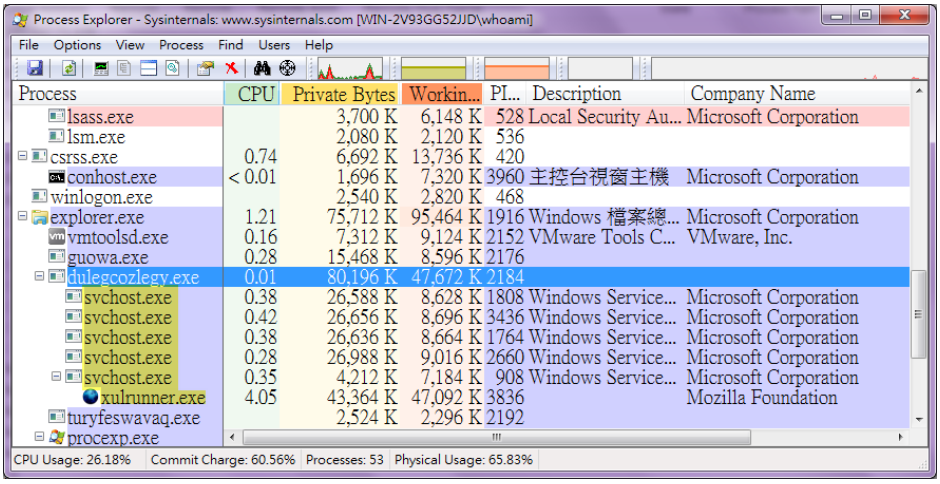


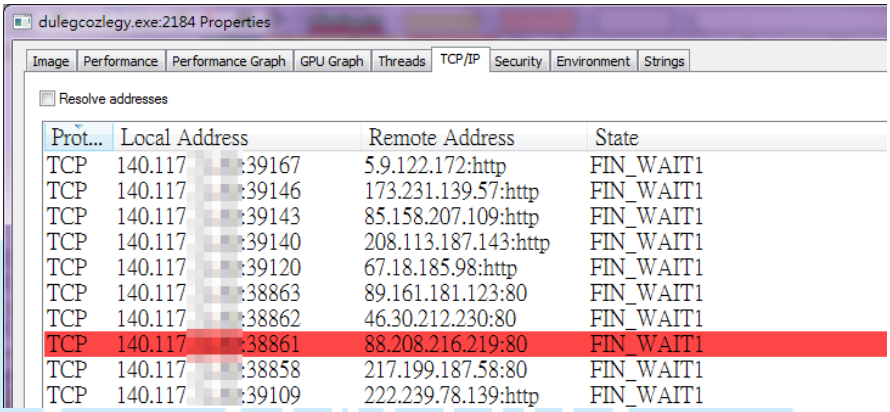


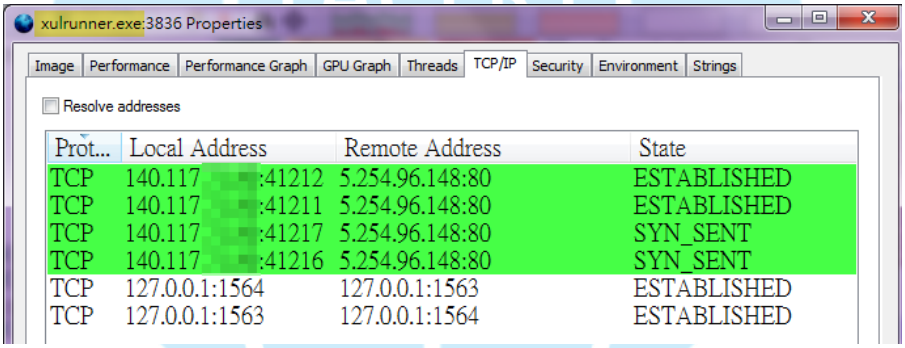
1. 『turyfeswavaq.exe』會開始感染系統的 svchost.exe，並且複製自己成另一檔案名稱『dot__57.exe』藏匿於隱藏目錄 C:\Users\XXX\AppData 下，並透過『guowa.exe』這支父程式進行呼叫。



2. 『dulegcozlegy.exe』與子程序『scvhost.exe』後期會開始有大量網路行為，並且惡意程式會於“ C:\Users\whoami\AppData\Local\Temp\ ” 建立一個工具資料夾「~tmp9C4642」，並執行裡面的檔案『xulrunner.exe』來對外進行大量的資料傳送。


Process Explorer - Sysinternals: www.sysinternals.com [WIN-2V93GG52JJD\whoami]
File Options View Process Find Users Help
Process CPU Private Bytes Workin... PI... Description Company Name
lsass.exe 3,700 K 6,148 K 528 Local Security Au... Microsoft Corporation
lsm.exe 2,080 K 2,120 K 536
csrss.exe 0.74 6,692 K 13,736 K 420
conhost.exe < 0.01 1,696 K 7,320 K 3960 主控台視窗主機 Microsoft Corporation
winlogon.exe 2,540 K 2,820 K 468
explorer.exe 1.21 75,712 K 95,464 K 1916 Windows 檔案總... Microsoft Corporation
vmtoolsd.exe 0.16 7,312 K 9,124 K 2152 VMware Tools C... VMware, Inc.
guowa.exe 0.28 15,468 K 8,596 K 2176
dulegcozlegy.exe 0.01 80,196 K 47,672 K 2184
svchost.exe 0.38 26,588 K 8,628 K 1808 Windows Service... Microsoft Corporation
svchost.exe 0.42 26,656 K 8,696 K 3436 Windows Service... Microsoft Corporation
svchost.exe 0.38 26,636 K 8,664 K 1764 Windows Service... Microsoft Corporation
svchost.exe 0.28 26,988 K 9,016 K 2660 Windows Service... Microsoft Corporation
svchost.exe 0.35 4,212 K 7,184 K 908 Windows Service... Microsoft Corporation
xulrunner.exe 4.05 43,364 K 47,092 K 3836 Mozilla Foundation
turyfeswavaq.exe 2,524 K 2,296 K 2192
procexp.exe
CPU Usage: 26.18% Commit Charge: 60.56% Processes: 53 Physical Usage: 65.83%

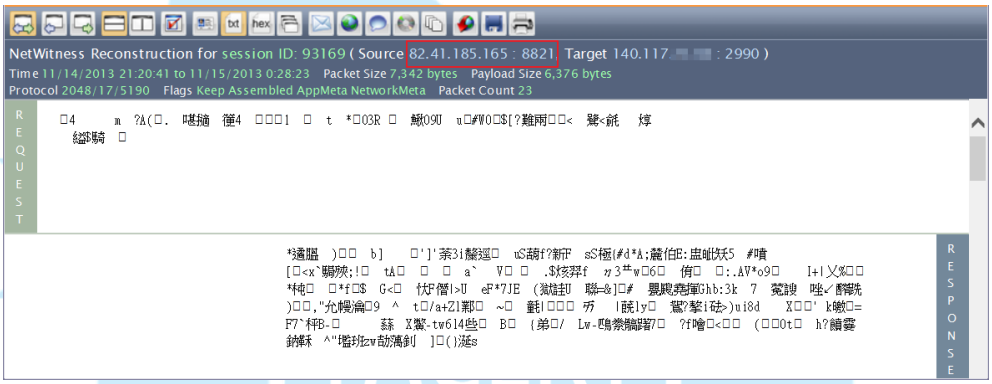

dulegcozlegy.exe:2184 Properties
Image Performance Performance Graph GPU Graph Threads TCP/IP Security Environment Strings
Resolve addresses
Prot... Local Address Remote Address State
TCP 140.117 :39167 5.9.122.172:http FIN_WAIT1
TCP 140.117 :39146 173.231.139.57:http FIN_WAIT1
TCP 140.117 :39143 85.158.207.109:http FIN_WAIT1
TCP 140.117 :39140 208.113.187.143:http FIN_WAIT1
TCP 140.117 :39120 67.18.185.98:http FIN_WAIT1
TCP 140.117 :38863 89.161.181.123:80 FIN_WAIT1
TCP 140.117 :38862 46.30.212.230:80 FIN_WAIT1
TCP 140.117 :38861 88.208.216.219:80 FIN_WAIT1
TCP 140.117 :38858 217.199.187.58:80 FIN_WAIT1
TCP 140.117 :39109 222.239.78.139:http FIN_WAIT1


xulrunner.exe:3836 Properties
Image Performance Performance Graph GPU Graph Threads TCP/IP Security Environment Strings
Resolve addresses
Prot... Local Address Remote Address State
TCP 140.117 :41212 5.254.96.148:80 ESTABLISHED
TCP 140.117 :41211 5.254.96.148:80 ESTABLISHED
TCP 140.117 :41217 5.254.96.148:80 SYN_SENT
TCP 140.117 :41216 5.254.96.148:80 SYN_SENT
TCP 127.0.0.1:1564 127.0.0.1:1563 ESTABLISHED
TCP 127.0.0.1:1563 127.0.0.1:1564 ESTABLISHED

III.側錄流量分析

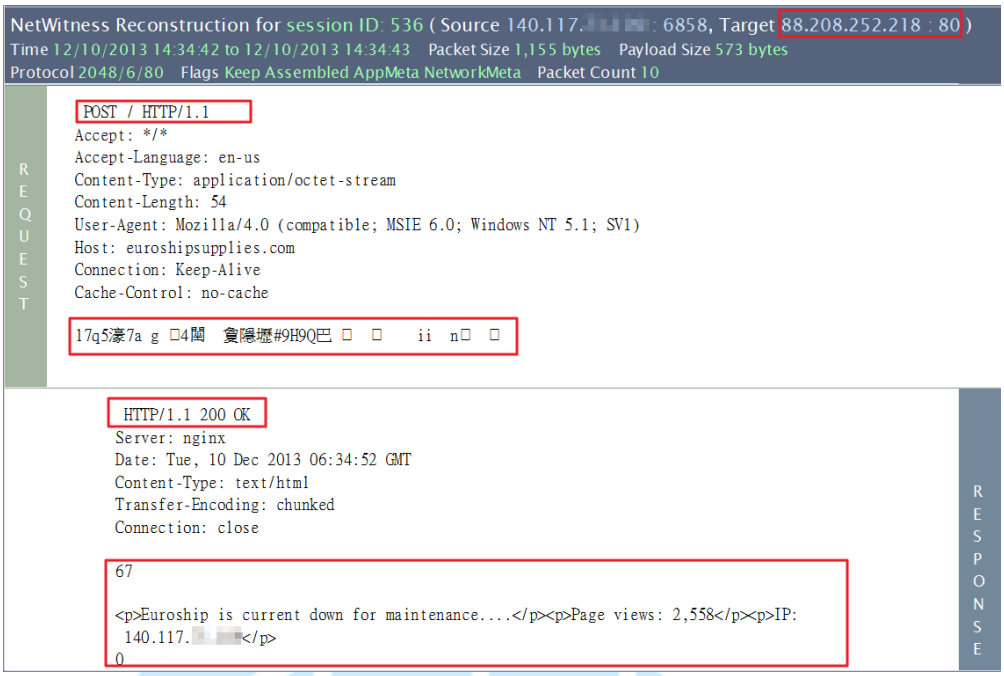
A. 感染主機主要透過被開啟的 Port 8485 和 2990 來跟駭客的主機做溝通。
   1. Port 2990 為 UDP 方式，收到 UDP 指令後會以 UDP 的方式回覆加密資料。
   2. Port 8484 為 TCP 方式，收到 TCP 指令後會回覆較大量的加密資料。
   3. 因為 UDP 的連線數遠大於 TCP 的連線數，可能作為對底層殭屍電腦的通訊方式，而 TCP port 的則是上層駭客主機用來下達指令的方式。

B. 目前有觀察到一個明確通訊協定特徵為「AOL IM」，也是透過 UDP Port 2990 與 IP: 82.41.185.165 (英國)進行通訊，此為一種即時通 Instant Messenger 的通訊協定，通訊內容也經過加密無法得知。



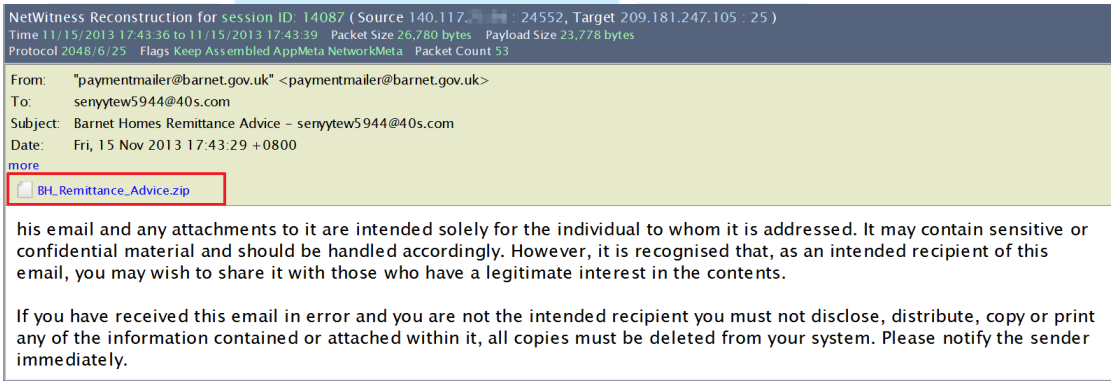
C. 感染的主機會對沒有來源設限的 DNS Servers 進行大量的 DNS query，可能造成“DNS 放大攻擊”而影響正常服務。
   1. 目前觀察到至少有 119 個國家和 5889 個 DNS 主機 IP 遭受影響。
   2. 觀測連至臺灣主要的 DNS 主機為
      a. 140.117.X.X (本單位)
      b. 168.95.X.X (中華)
      c. 210.201.X.X (亞太)
      d. 119.160.X.X (Yahoo)
      e. 61.220.X.X , 203.73.X.X (TWNIC)
      f. 220.135.X.X (中華)

D. 感染的主機對一些已知的惡意網站透過 HTTP 的 POST Method 傳送加密資料，可能是主機的個人機密資料。目的端至少有 40 個國家及 535 個 IP 位址。

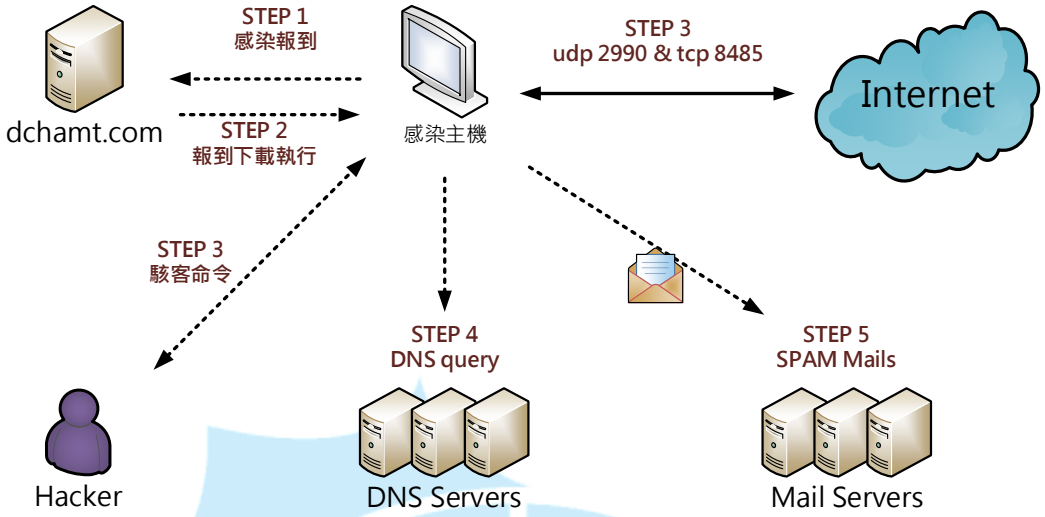


E. 感染的主機會偽造寄件者名稱，大量發送惡意 SPAM 郵件，至少有 10000 個目的地郵件地址和 83 個國家，檢查發現 SPAM 郵件內裡查夾帶 zip 壓縮檔，解壓縮後為『BH_Remittance_Advice.pdf.exe』的病毒。誤執行就會遭受感染成為殭屍電腦。

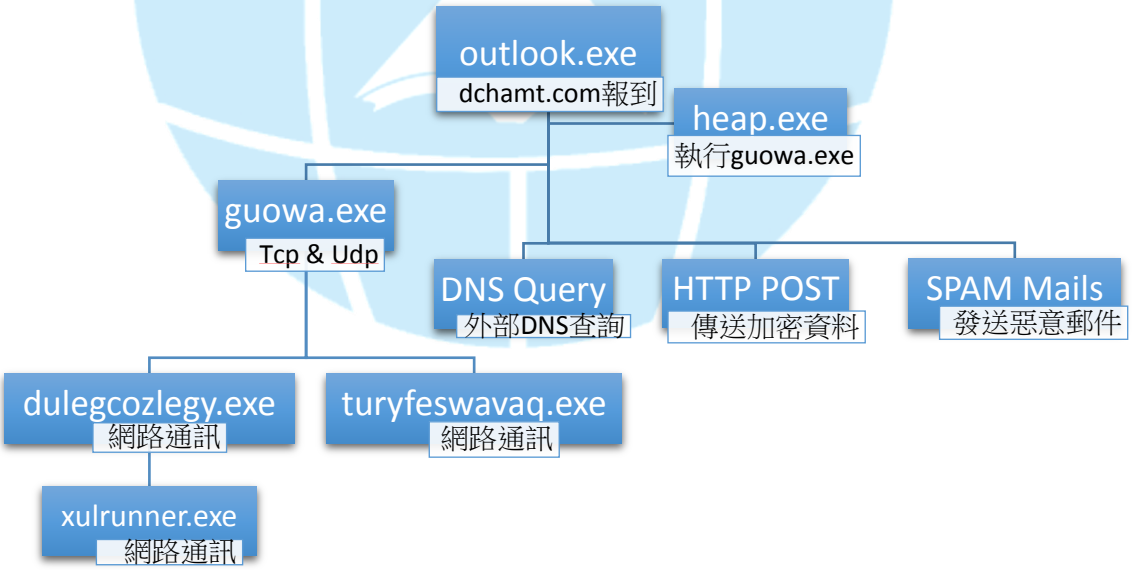
1. 其他郵件的惡意程式還有『Invoice.PDF.exe、Invoice_111813.exe』兩種。



IV. 網路行為架構圖



STEP 1：感染主機透過 HTTPS 向 dchamt.com 進行報到。
STEP 2：報到後會下載一個惡意程式 heap.exe 並執行。
STEP 3：感染主機會開啟埠號 UDP 2990 和 TCP 8485 與外部主機和駭客進行通訊。
STEP 4：感染主機會對無設限制的DNS主機進行DNS查詢放大攻擊。
STEP 5：感染主機會發送大量的SPAM Mails，並且夾帶惡意檔案。



V. 結論

A. 此程式 Outlook.zip 主要誤導使用者以為是 Office Outlook 更新檔案，實質上為惡意的後門程式。
B. 該惡意程式會在資料夾下產生許多子程式來控制網路的行為，也可能成為駭客的中繼站或 C&C 主機。
C. 駭客透過該檔案感染使用者主機後取得該主機個人資料，並且成為殭屍跳板主機對其他主機進行攻擊，例如 DNS Query 放大攻擊或發送惡意釣魚郵件。

VI. 建議措施

A. 若不幸誤點此惡意程式後可以先拔除網路線或關閉網路，以降低損害程度。
B. 安裝並更新防毒軟體進行系統磁槽的病毒掃描。
C. 利用工作管理員或 Procexp 工具來強制關閉背景的惡意程式，並且手動刪除。
D. 利用 autoruns 工具或執行 msconfig 來關閉開機自動執行的惡意程式登錄檔。
E. 使用 Tcpview 檢查網路連線狀態是否還有異常。
F. 若擔心無法完整清除，建議備份檔案後重新安裝作業系統，以確保無惡意程式殘留。