



個案分析-

C&C 分析報告

TACERT



TACERT 臺灣學術網路危機處理中心團隊製

2013/1



目錄

前言.....	3
中繼站與上下層的網路架構.....	3
中繼站主機狀態.....	5
建議.....	6



前言

駭客在從事惡意活動時，為了掩藏自己的網路位址，會透過中繼站主機，對遠端的受害主機進行操控，透過中繼站活動，即使受害主機被發現，也只會得到中繼站主機的資訊，而不會知道駭客的真實網路位址。由於中繼站主機必須隨時都能讓駭客使用，所以中繼站多半是網路位址固定且二十四小時運轉的主機。本次的案例分析介紹一個典型的中繼站。

中繼站主機資訊：

- Windows2003
- 校務系統
- 另有 Database 主機與 Mail server 主機聯合提供服務

中繼站與上下層的網路架構

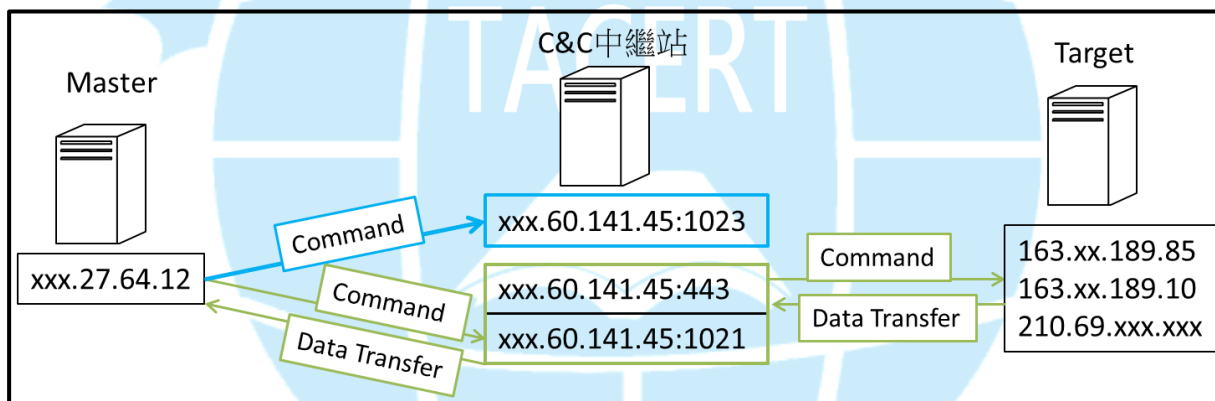


圖 1

經由側錄中繼站主機的網路流量，概略得出圖 1，主機的 port 443 與 1021 由同一個程式 mp.exe 佔用（綠色框部份），其程式執行的 command line 為[mp.exe -S:1021 -S:443]，這個程式主要擔當 Master 與目標主機間的命令與資料傳遞，Master 傳遞命令到 xxx.60.141.45 的 1021 埠後，再從 xxx.60.141.45 的 443 埠傳給目標主機。

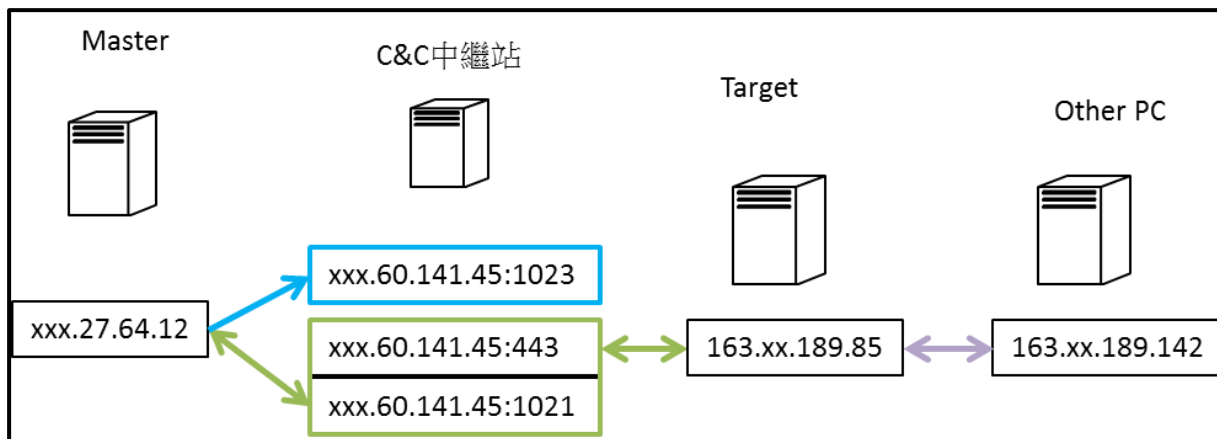


圖 2 Master 在 163.xx.189.85 主機上透過網芳竊取 163.xx.189.0 網段中其他主機的資料

Master 透過中繼站取得目標主機 (Target) 的控制權後，利用網路芳鄰，竊取 163.xx.189.0 網段中其他主機的資料。先用網芳將其他 PC 的資料傳到 163.xx.189.85 主機上，接著再從 163.xx.189.85 主機上用 xxx.60.141.45 的 443 port 將資料傳回給 Master。

```
mp.exe pid: 2392
Command line: mp -S:1021 -S:443

Base          Size          Path
0x00400000   0x5000        mp.exe
0x7c930000   0xd3000       ntdll.dll
0x7c800000   0x12c000      kernel32.dll
0x77b80000   0x5a000       MSUCRT.dll
0x71b70000   0x17000       WS2_32.dll
0x71b60000   0x8000        WS2HELP.dll
0x77f30000   0xaa000       ADVAPI32.dll
0x77c30000   0xa0000       RPCRT4.dll
0x76ec0000   0x13000       Secur32.dll
0x71a90000   0x40000       mswsock.dll
0x5e140000   0x57000       hnetcfg.dll
0x77be0000   0x49000       GDI32.dll
0x77e10000   0x90000       USER32.dll
0x76190000   0x1d000       IMM32.DLL
0x7f000000   0x9000        LPK.DLL
0x74af0000   0x65000       USP10.dll
0x71a50000   0x8000        wshtcpip.dll
```

圖 3 mp.exe 使用的參數以及 DLL

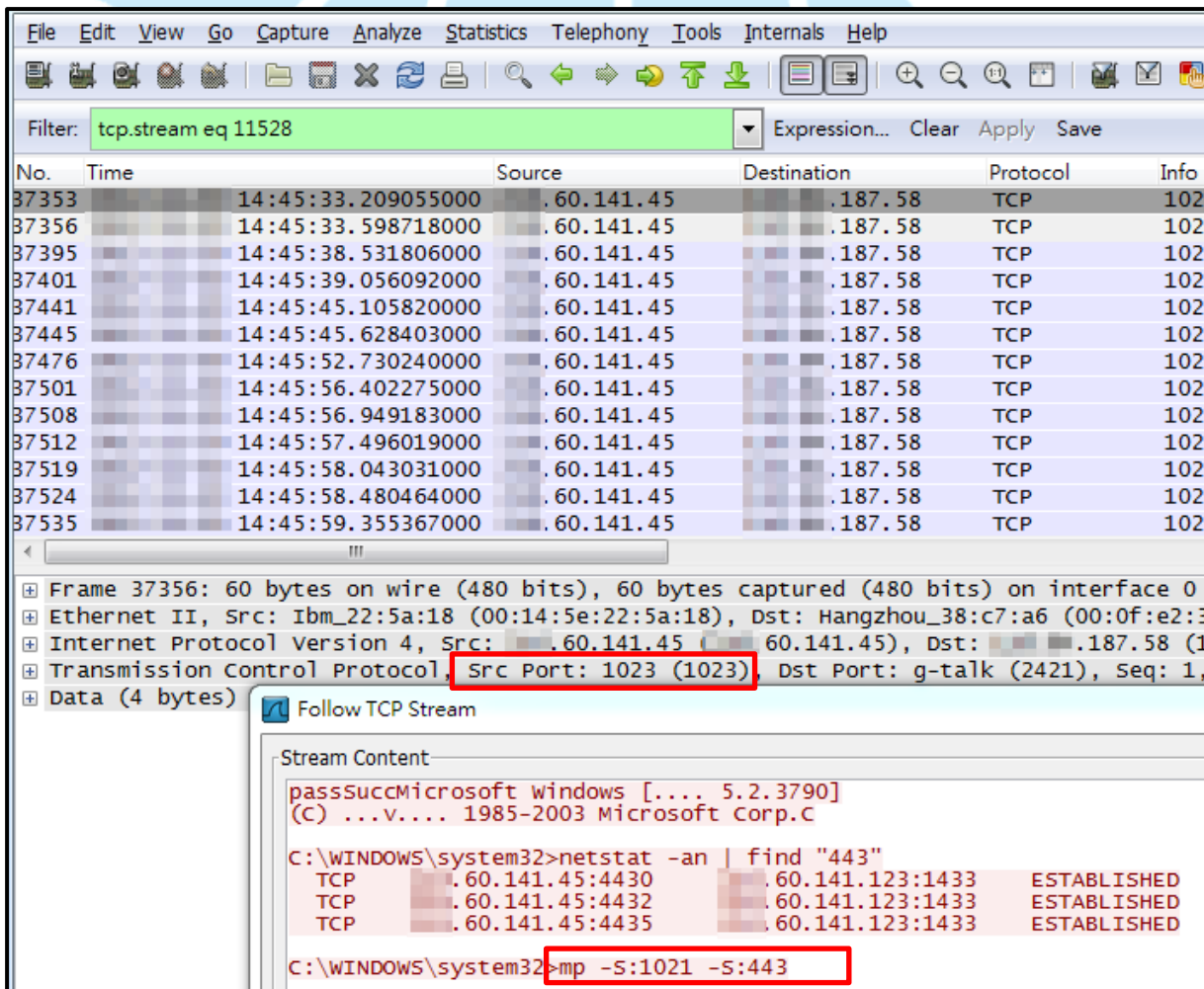
這個網路活動架構顯示，駭客並不一定需要感染每一台主機才能竊取資料，只要可以獲得同網段中的某一台主机的控制權，就可以利用網芳進行攻擊或是竊取資料。

中繼站主機狀態

在中繼站主機中，上段所介紹的 mp.exe 並沒有被寫到登錄檔中，主機重新開關機後並不會自動啟動。駭客僅在登錄檔中寫入（圖 4）[wmdmpmpsex.dll]這個惡意 DLL 檔，此 DLL 檔為後門程式，開啟 port 1023 供駭客控制中繼站主機。每當主機重新開關機，mp.exe 會被關閉，駭客透過 wmdmpmpsex.dll 提供的後門在主機上把 mp.exe 執行起來。圖 5 中可以看到駭客先是透過 port 1023 連進 xxx.60.141.45，用[netstat -an]和[find]指令找是否有 port 443 的活動，此時，主機上僅有 xxx.60.141.45 與其資料庫 xxx.60.141.123 的活動，接著駭客用指令[mp -S:1021 -S:443]將 mp.exe 啟動，透過該程式控制 Target。

Autorun Entry	Description	Publisher	Image Path
<input checked="" type="checkbox"/> WinHttpAutoPr...	為 Windows HTTP 服務 (WinHTTP) ...		File not found: winhttp.dll
<input checked="" type="checkbox"/> WmdmPmSp	傳送磁碟區資訊到邏輯磁碟管理系...		c:\windows\system32\wmdmpmpsex.dll

圖 4 後門程式在登錄檔中的登錄資料



The image shows a Wireshark capture of network traffic. The filter is set to 'tcp.stream eq 11528'. The packet list shows a series of TCP connections from source IP .60.141.45 to destination IP .187.58 on port 1023. The packet details pane shows the selected packet (Frame 37356) with the following information:

- Ethernet II, Src: Ibm_22:5a:18 (00:14:5e:22:5a:18), Dst: Hangzhou_38:c7:a6 (00:0f:e2:38:c7:a6)
- Internet Protocol Version 4, Src: .60.141.45, Dst: .187.58
- Transmission Control Protocol, Src Port: 1023 (1023), Dst Port: g-talk (2421), Seq: 11528
- Data (4 bytes)

The Stream Content pane shows the following commands being executed:

```
passsuccMicrosoft windows [... 5.2.3790]
(C) ...v.... 1985-2003 Microsoft Corp.C

C:\WINDOWS\system32>netstat -an | find "443"
TCP .60.141.45:4430 .60.141.123:1433 ESTABLISHED
TCP .60.141.45:4432 .60.141.123:1433 ESTABLISHED
TCP .60.141.45:4435 .60.141.123:1433 ESTABLISHED

C:\WINDOWS\system32>mp -S:1021 -S:443
```

圖 5 駭客透過 port 1023 進入主機下指令



中繼站主機上另有一個駭客拿來偷取中繼站主機上帳號密碼的惡意 DLL，完整名稱為 [qmgrxp.dll]，這個 DLL 也被註冊到登錄檔裡面，主要用來偷取中繼站主機上如網芳或遠端等網路活動時出現的密碼。

Autorun Entry	Description	Publisher	Image Path
<input checked="" type="checkbox"/> BITS	使用閒置網路頻寬於背景轉移檔案。如果...		c:\windows\system32\qmgrxp.dll

圖 6 qmgrxp.dll 在登錄檔裡面的名稱

這兩個惡意的 DLL 檔案，在登錄檔裡面的註冊描述，分別為：

- BITS c:\windows\system32\qmgrxp.dll
 - 使用閒置網路頻寬於背景轉移檔案。如果服務停止的話，Windows Update 和 MSN Explorer 等功能將無法自動下載程式或其他資訊。如果此服務被停用的話，任何依賴它的服務如果沒有防止失敗的機制，在 BITS 被停用的情況下，利用 IE 直接轉移檔案的話，它們將無法轉移檔案。
- WmdmPmSp c:\windows\system32\wmdmpmspex.dll
 - 傳送磁碟區資訊到邏輯磁碟管理系統管理服務以供設定。如果這個服務被停止，動態磁碟狀態和設定資訊可能會過時。如果這個服務被停用，任何明確依存於它的服務將無法啟動。

駭客利用人們害怕犯錯的心理狀態，尤其是管理主機的管理者，必須對主機上的服務負責，在登錄檔描述的地方寫了很多關於這個項目如果被移除會發生什麼後果的敘述，使得主機管理者不敢輕易移除，以確保惡意程式的存活時間。

建議

- 利用線上搜尋引擎和線上掃毒引擎

當我們發現主機上有可疑的程式或是 DLL 檔案時，最快速的檢查方法就是把名稱放到 Google 去搜尋，或是將檔案傳到 VirusTotal 上檢查。若是由作業系統或應用程式所使用的 DLL，通常都可以在 Google 上找到許多資料（如圖 7），而本例子中出現的兩個惡意 DLL，在 Google 搜尋引擎中僅有不到 50 筆的資料（如圖 8 圖 9），當搜尋引擎的結果讓這個 DLL 看起來很可疑時，就可以進一步把它們放到 VirusTotal 上檢查，這個例子出現的 DLL 被超過一半的防毒引擎偵測出有問題（如圖 10 圖 11）。

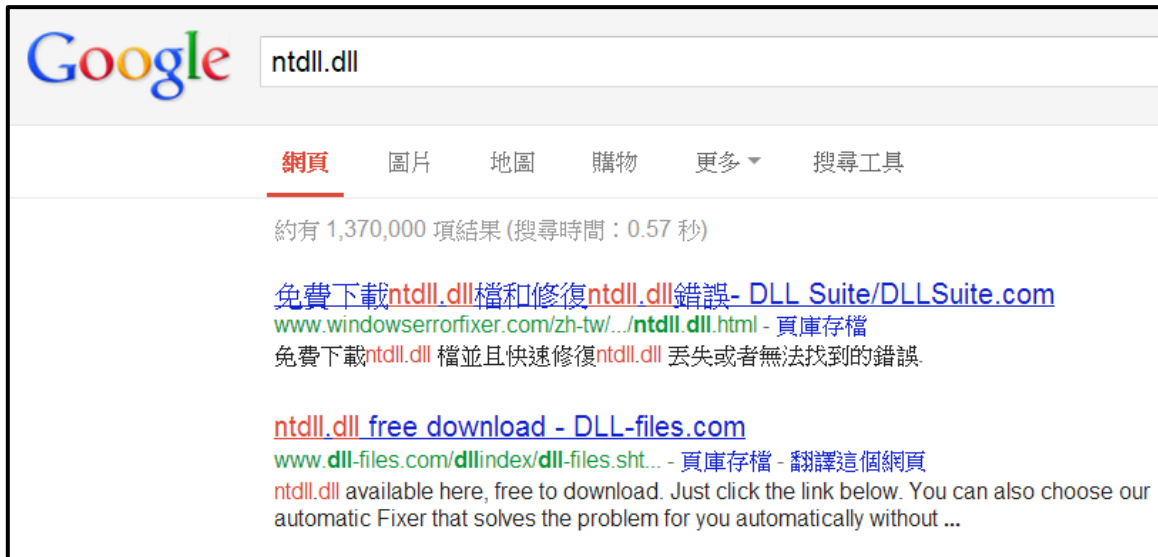


圖 7 正常的 DLL 在 Google 上面可以找到許多資料



圖 8 有問題的 DLL 在 Google 搜尋的結果很少



圖 9

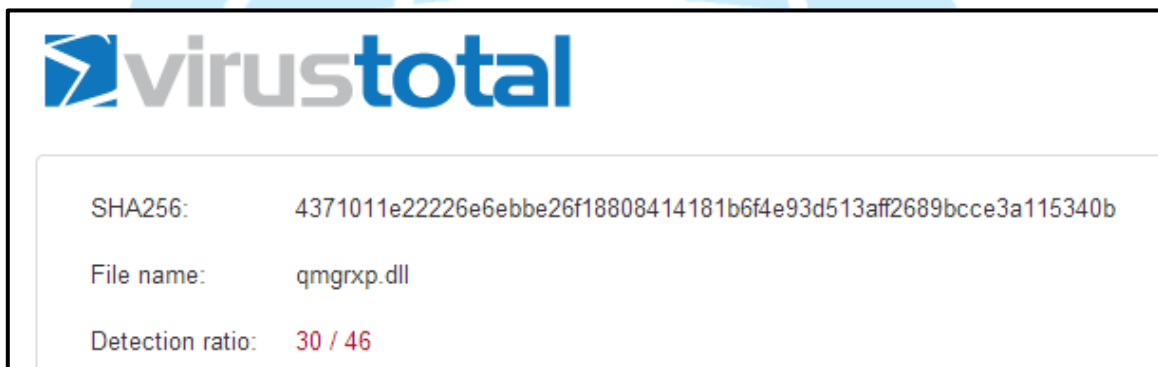


圖 10 VirusTotal 對 qmgrxp.dll 的掃描結果

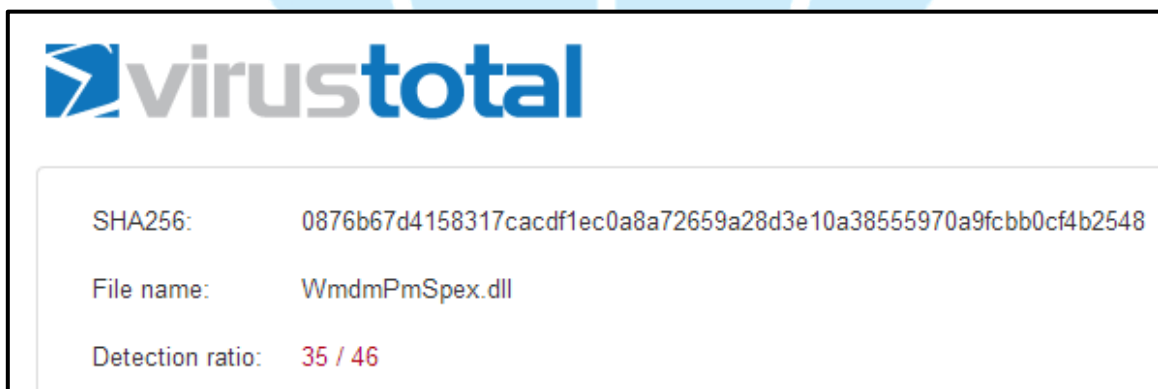


圖 11 irusTotal 對 WmdmPmSpex.dll 的掃描結果



- 備份主機開啟的埠號，定期檢查

如果主機被開了後門，在網路狀態上面通常可以發現多餘的埠號被開啟，但是對管理多台主機的管理人員而言，記憶每一台主機的應該開啟的埠號是不可能的，建議在主機完成安裝及服務設定，上線前備份埠號的開啟狀態，此時主機的網路狀態應該是最「正常」的，主機上線後，在沒有新增其他服務的條件下，定期比對網路埠號的使用狀態，如有新增的異常埠號，很容易就可以發現。

