臺灣大學計資中心檢查個人電腦惡意程式標準作業程序

2015.02.04 Ver0.86

技術支援請洽臺大計資中心北區教育資訊安全維運中心
電話(02)23651106
臺大校內分機 65013

本文件的目的在於協助使用者快速檢查出 Microsoft Windows 個人電腦中的惡意程式,以利清除及回報網路管理者,回復個人電腦之正常工作環境.

標準作業程序共有 3 個步驟,分別為

1. **接獲網管人員通知**
2. **查找可疑程式**
3. **結果回報.**

使用者需依順序進行每一個步驟,若未依順序或是減少步驟,將導致檢查結果錯誤.

下列為標準作業程序:

1 接獲網管人員通知

代表您的電腦,可能在您不知情的情況下,正自動執行未經您許可的程式,進行惡意活動;
當接獲通知時,請勿再執行任何動作,如檔案開啟或關機等作業,以免影響調查結果.

註:
本文件適用 Microsoft Windows 版本包含
Windows XP,
Windows Vista, Windows 7,
Windows Server 2003,
Windows Server 2008;
包含 32bits/64bits.

2 查找可疑程式

查找可疑程式分成四個子步驟(章節)進行檢查：

2.1 「檢查已知惡意程式」，經由此步驟找出已知之惡意程式並移除；

2.2 「查找可疑網路連線」，經由此步驟檢測找出可疑之程序；

2.3 「查找可疑程序」，針對正在執行之可疑程序進行檢查；

2.4 「由系統啟動區查找惡意程式」，找出系統啟動區已掛載之可疑程序；

此外，本文件提供查找可疑網路封包(packet)與線上掃毒相關操作資訊，請參考附件。

2.1 檢查已知惡意程式

本步驟目的在於利用微軟提供之「惡意軟體移除工具」(MRT)以檢查您的電腦是否有特定、常見、已知的惡意程式 (包括 Blaster、Sasser、Mydoom 等)，並協助移除找到的惡意程式。微軟並將於每個月第二個星期二發佈更新本工具的版本，目前版本為 4.2 版。此工具除了可以自己下載更新之外，也可直接利用 Windows Update 的方式自動下載更新。(適用作業系統包括 Windows 7、Windows Vista、Windows XP、Windows 2000 和 Windows Server 2003)

2.1.1 請下載下列程式

如果您電腦的作業系統是 Windows 7、Windows Vista、Windows XP SP2 以上，則微軟已經將此惡意軟體移除工具安裝在您的電腦上，請直接跳至「2.1.2 執行程式」；否則請手動下載下列程式：

程式名稱 : windows-kb890830-v4.2.exe
下載路徑 :
http://www.microsoft.com/downloads/details.aspx?displaylang=zh-tw&FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356

若您使用 64 位元作業系統，則下載 64 位元程式：

程式名稱 ： windows-kb890830-x64-v4.2.exe

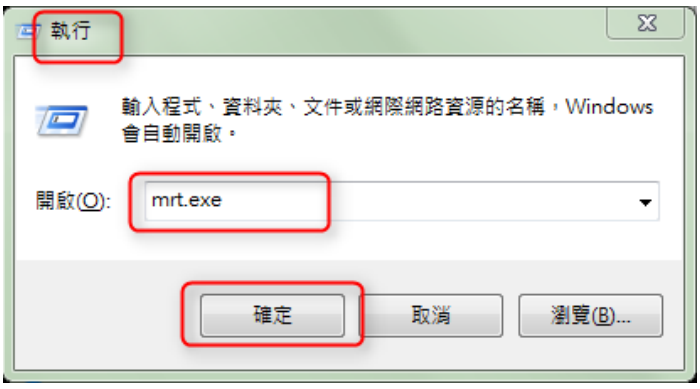
下載路徑 ：

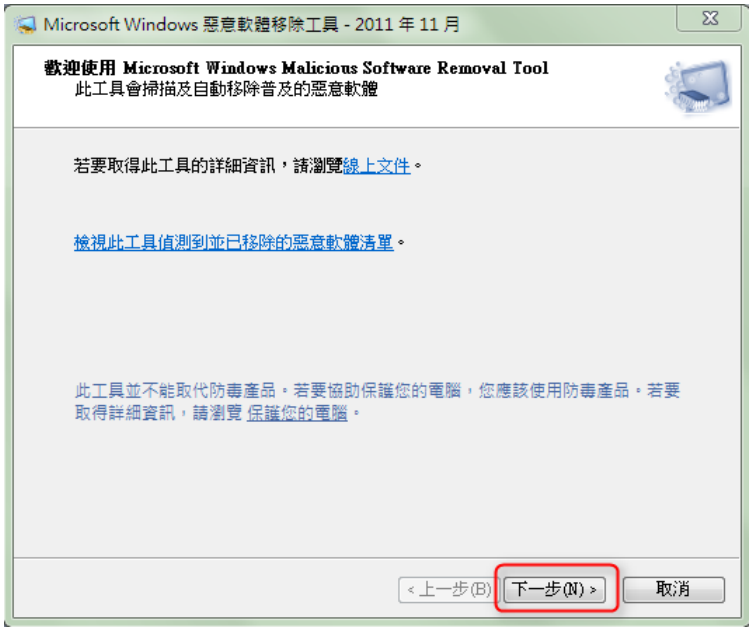
http://www.microsoft.com/downloads/zh-tw/details.aspx?familyid=585d2bde-367f-495e-94e7-6349f4effc74&displaylang=zh-tw

2.1.2 執行程式

2.1..1　執行程式,步驟如下

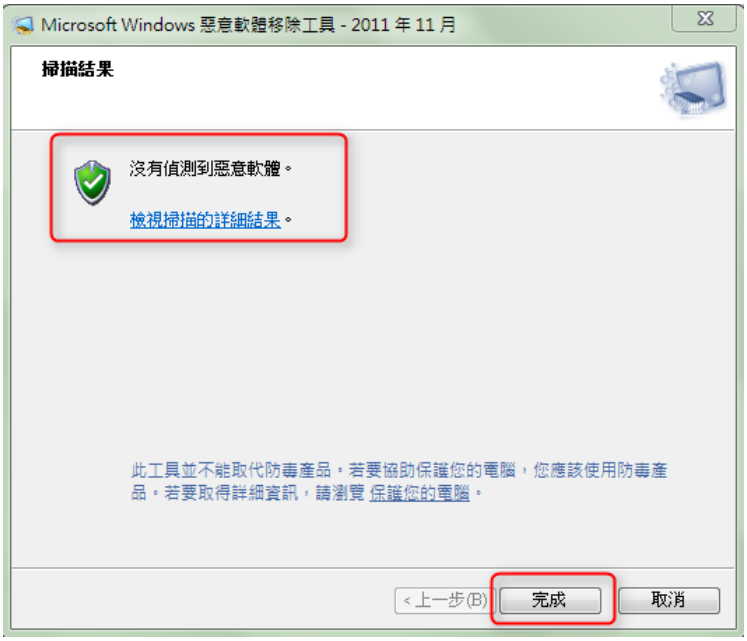
步驟一:按鍵盤上的「視窗鍵」+「R」開啟「執行」視窗，輸入「MRT.exe」再按「Enter」鍵即可開啟程式；或將上述軟體下載回來並按兩下執行。開啟後直接按「下一步」。





步驟二:選擇掃描類型，可選擇「快速掃描」，再按「下一步」，開始掃描。

步驟三:完成掃描後會在視窗中顯示掃描結果，如果沒找到惡意程式會告知「沒有偵測到惡意軟體」，請跳至步驟五；



步驟四:如果有偵測到惡意程式時,工具會提示您執行「完整掃描」。完整掃描時，系統會先執行快速掃描，然後再對電腦所有磁碟機全部檔案進行一次完整的掃描，因此可能需花費一段時間才會完成。同時，則此工具將會提示您從那些遭感染檔案移除

惡意程式，請再依照指示操作。

步驟五:執行此「惡意軟體移除工具」之後，您可能會收到下列表格中四種回報結果之一，請依「後續步驟」進行處理。此工具會在 %WINDIR%\debug 資料夾中(如:C:\Windows\debug 目錄下)，建立名為 mrt.log 的記錄檔以存放掃描結果。

	可能的掃描結果	後續步驟
1	未發現任何感染。	請繼續執行步驟 2.2 查找可疑網路連線。
2	至少發現一個感染，並且已經加以移除。	請跳至步驟 3 結果回報(回傳 mrt.log 檔)。
3	發現感染，但未加以移除。 在電腦上找到可疑的檔案時，就會出現這個結果。如果要協助移除這些檔案，請使用最新的防毒產品。	請使用防毒軟體(更新最新病毒碼)進行掃毒，並跳至步驟 3 結果回報 (回傳 mrt.log 檔及掃毒結果)。
4	發現感染，並移除部分感染。 如果要完成此移除作業，請使用最新的防毒產品。	請使用防毒軟體(更新最新病毒碼)進行掃毒，並跳至步驟 3 結果回報 (回傳 mrt.log 檔及掃毒結果)。

參考資料:

微軟網站 http://support.microsoft.com/?kbid=890830

2.2 查找可疑網路連線 (Port)

本步驟目的在於利用軟體工具查找出所有進出系統的連線資訊，包括連線的程序、協定、本機及遠端位址、連線狀態等，進而檢測主機是否存在可疑程序之網路連線。

2.2.1 請下載下列程式

程式名稱 ： TCPView

下載路徑 ：

http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx

2.2.2 解壓縮檔案

請將下載後的程式,進行解壓縮,步驟如下.

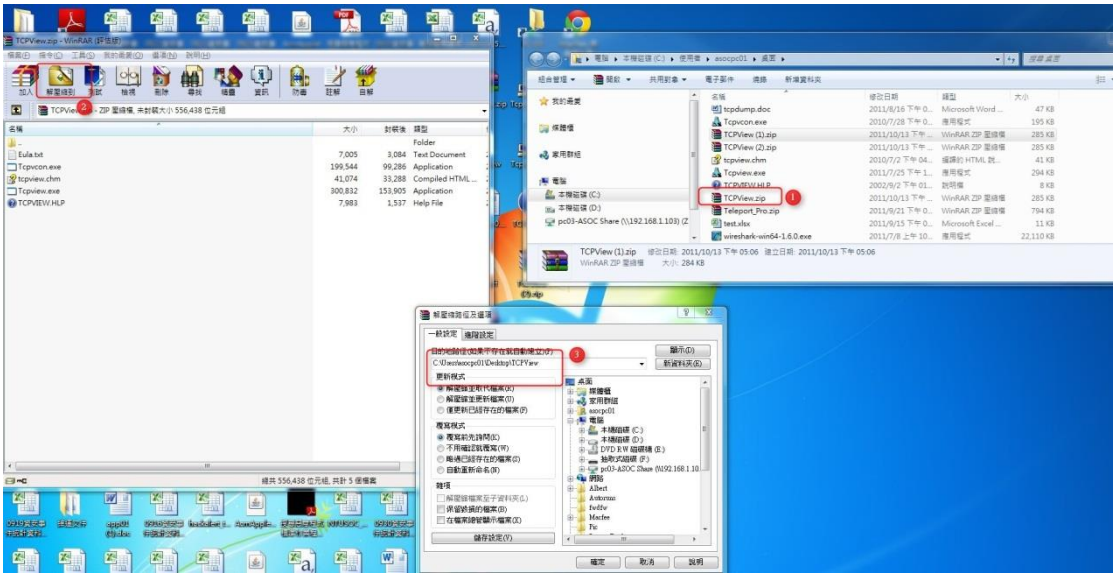
步驟一:滑鼠點選下載的程式兩下

步驟二:點選解壓縮檔案至此

步驟三:存放至指定位置

請參考下圖

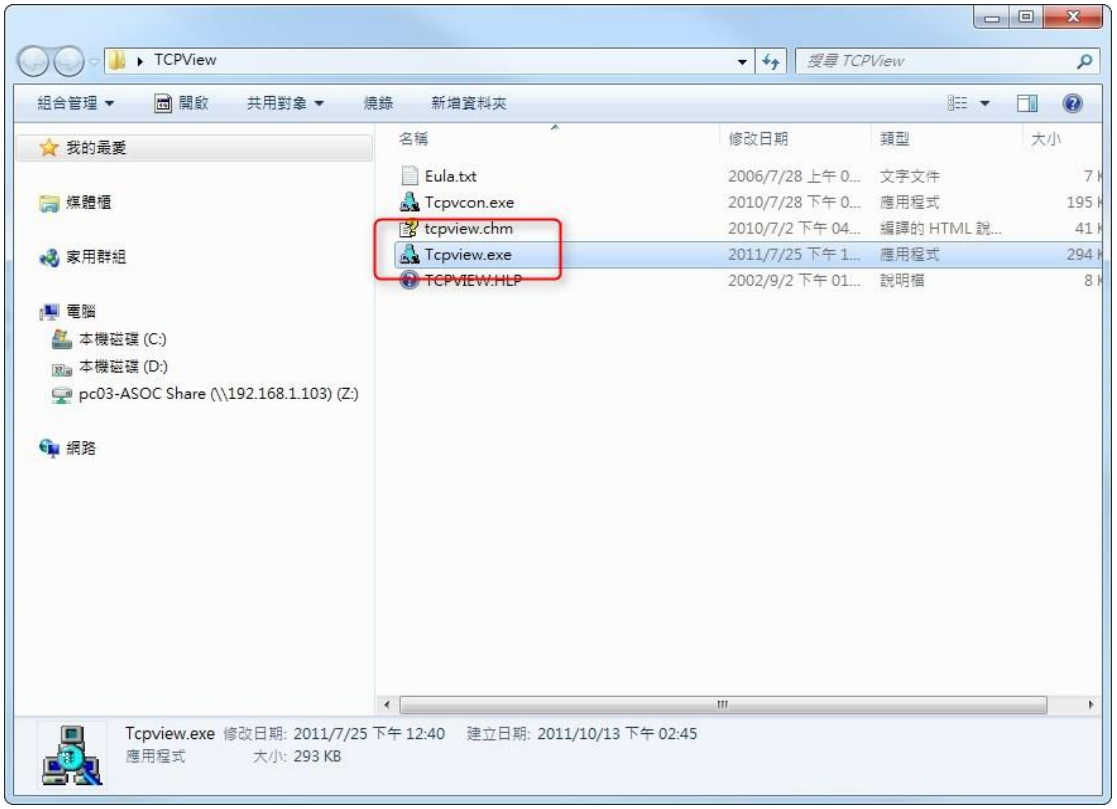
(各電腦因安裝的解壓縮軟體不同,可能有不同的解壓縮方式,本手冊以 WinRAR 解壓縮軟體作為範例)



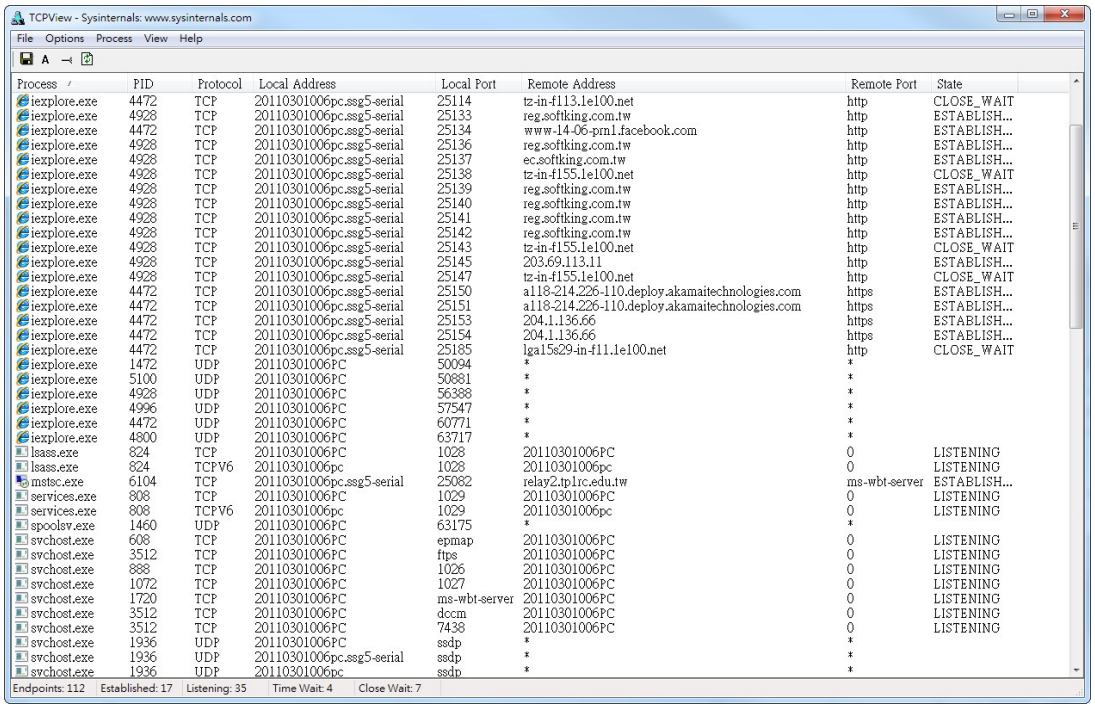
2.2.3 執行程式

2.2.3.1 執行程式,步驟如下

步驟一:點選安裝路徑下之 Tcpview.exe



點選後程式將會執行並將出現下列畫面,本畫面即為 TCPView 軟體執行之主畫面



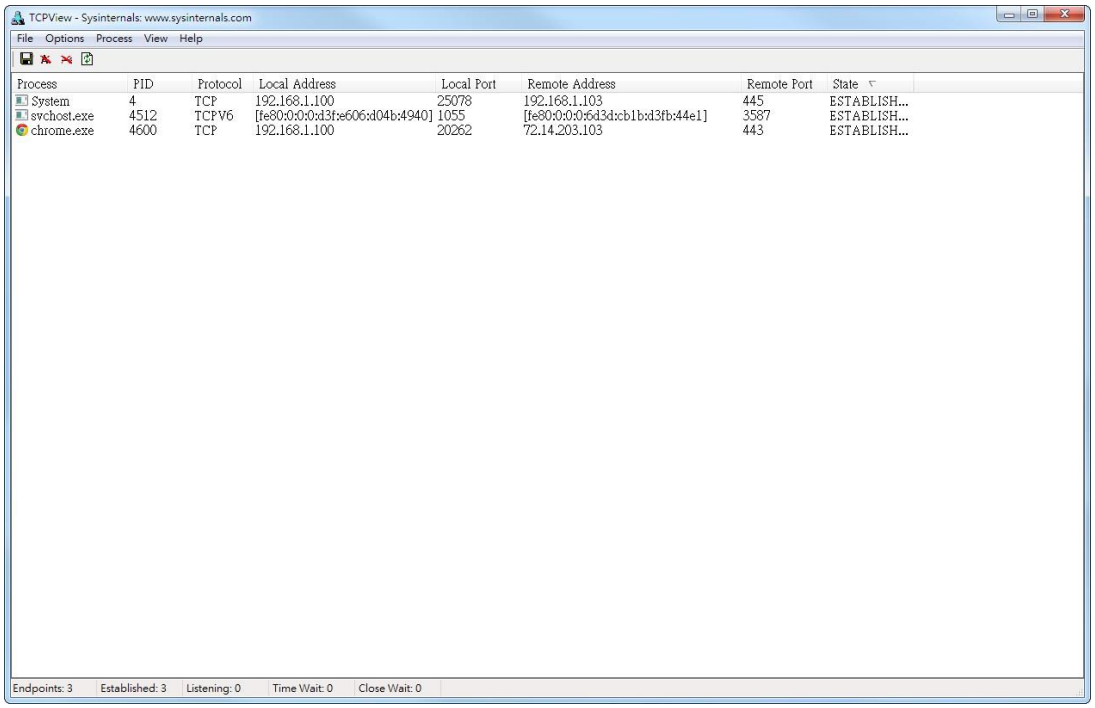
當我們執行了 TCPView 軟體後，會直接列出目前電腦的全部連線狀況，並自動將 IP 位址解析成正確的網域名稱，方便我們確認該軟體的連線目的。此外還可設定每 1 秒、2 秒、5 秒等新一次連線狀態，或者按暫停讓我們檢查程式或軟體的連線細節。

2.2.3.2　欄位簡介：

- Process（程序）：顯示目前正在連線的程序名稱。
- PID(編號)：顯示目前正在連線的程序識別編號。
- Protocol（協定）：顯示該程序使用的通訊協定，如 TCP 及 UDPV6 。
- Local Address（本機位址）：顯示該連線的本機位址。
- Local Port（本機通訊埠）：顯示該連線的本機通訊埠號碼。
- Remote Address（遠端位址）：顯示該連線的遠端目的位址。
- Remote Port(遠端通訊埠)：顯示該連線的遠端通訊埠號碼。
- State(狀態)：顯示連線狀態為何，如 LISTENING、TIME_WAIT。

2.2.4 查找可疑連線之程序

步驟一:找出目前連線的程序：按下快速鍵 "Ctrl+U" ，則只會出現出目前連線的程序：



步驟二:進行資安告警事件單或佐證資料中的 PORT 與步驟一查得目前連線的程序 PORT 作一比對，如有符合之項目即為此事件的疑似惡意程式：若未能找到符合事項，請跳至步驟五。

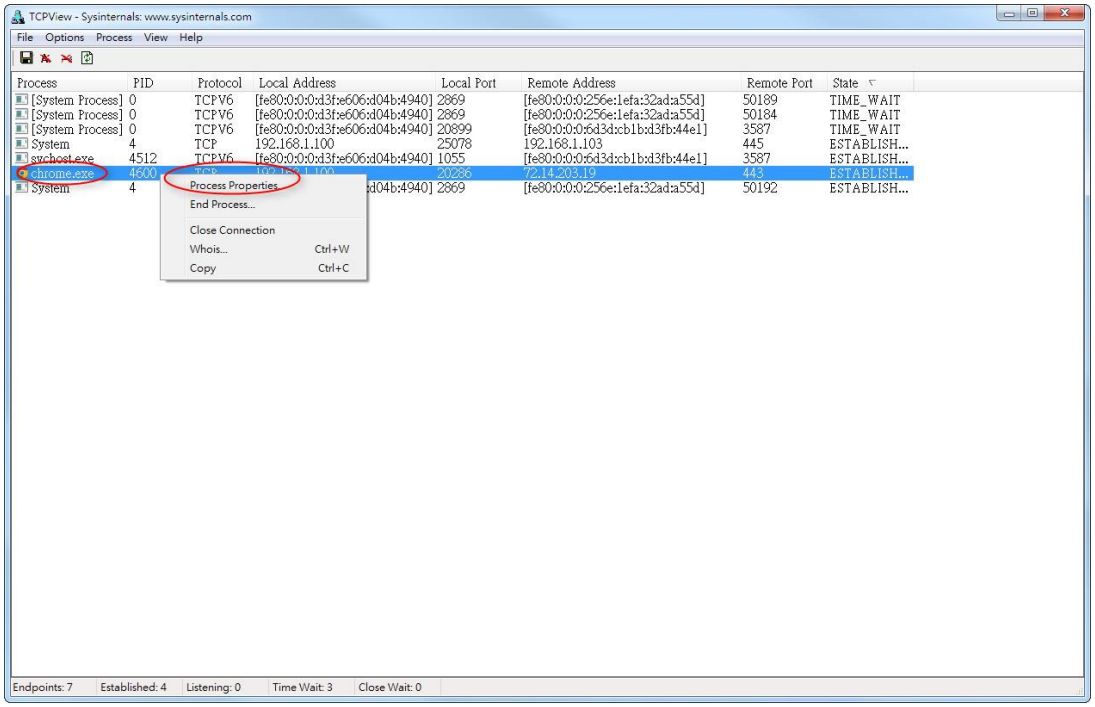
事件類型	對外攻擊	風險等級	第1級事件
發生時間	2011-10-09 15:36:59.000	發生次數	16
擊來源IP	[redacted]	攻擊來源PORT	63230
目標IP	[redacted]	目標PORT	21

步驟三:查詢程序相關資訊：

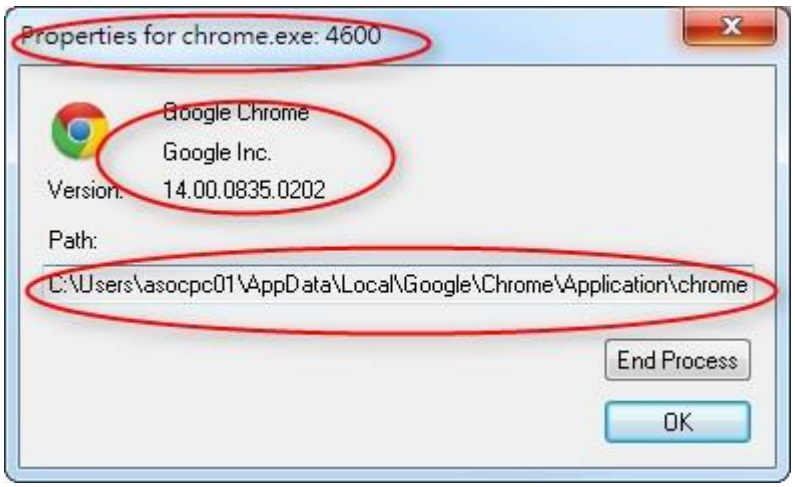
在欲查詢的程序上按右鍵 -> Process Properties，可查得該疑似惡意程序的相關資訊。請針對此程序進行判別：

(a) 如果使用者確定其為自己安裝且正常使用之軟體(應用程式)，如 MSN、Dropbox、PPTV、P2P 軟體等等，則此事件可能是誤判，可直接跳至「步驟 3.結果回報」以告知檢測結果並註記為誤判事件；

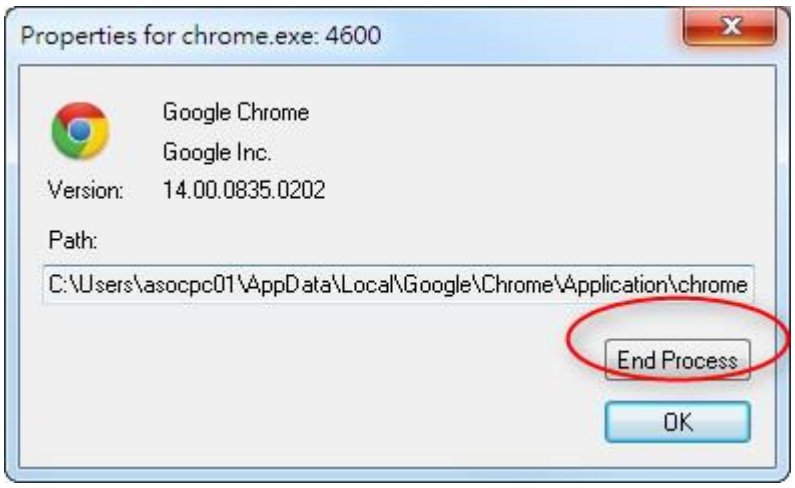
(b) 否則，此該程序即為惡意程序，請繼續進行底下步驟以便立即終止其執行並予以移除。



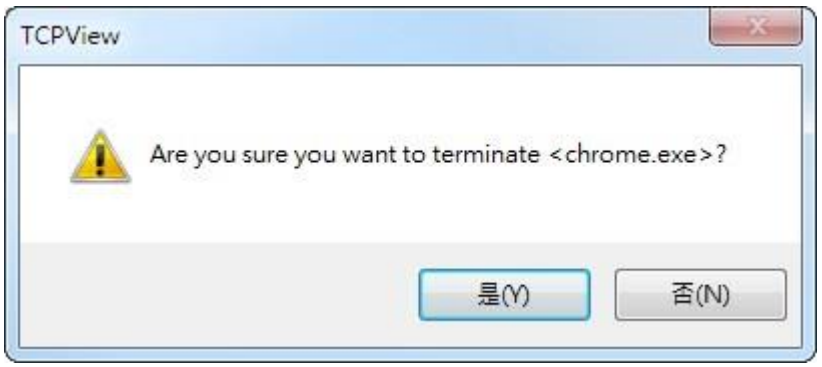
即可查到序相關資訊：



步驟四:請利用視窗中的 End Process 按鈕或者是直接在程序上按右鍵 -> End Process 來終止執行。並依視窗中的 Path 欄位資訊，即為此程序的目錄檔案位置，將該程序的檔案予以刪除。刪除後請跳至「步驟 3. 結果回報」以告知檢測結果。(注意：必須先將該程序終止執行，作業系統才允許刪除檔案。)



跳出確認視窗，按下「是」，該程序會立即終止。



步驟五:若未能找到符合項目，並不代表是誤判或不存在惡意程式，可能是在查找時間點該惡意程式沒有活動，所以未建立連線，請依照下面 2.3 章節繼續進行檢測。

2.3 查找可疑程序 (Process)

利用檢測主機正在執行的服務與程序，可判別是否有可疑或多餘之服務或程序在您不知情的狀況下遭載入，此可能是造成您的主機發生異常網路行為或流量的原因。

2.3.1 請下載下列程式

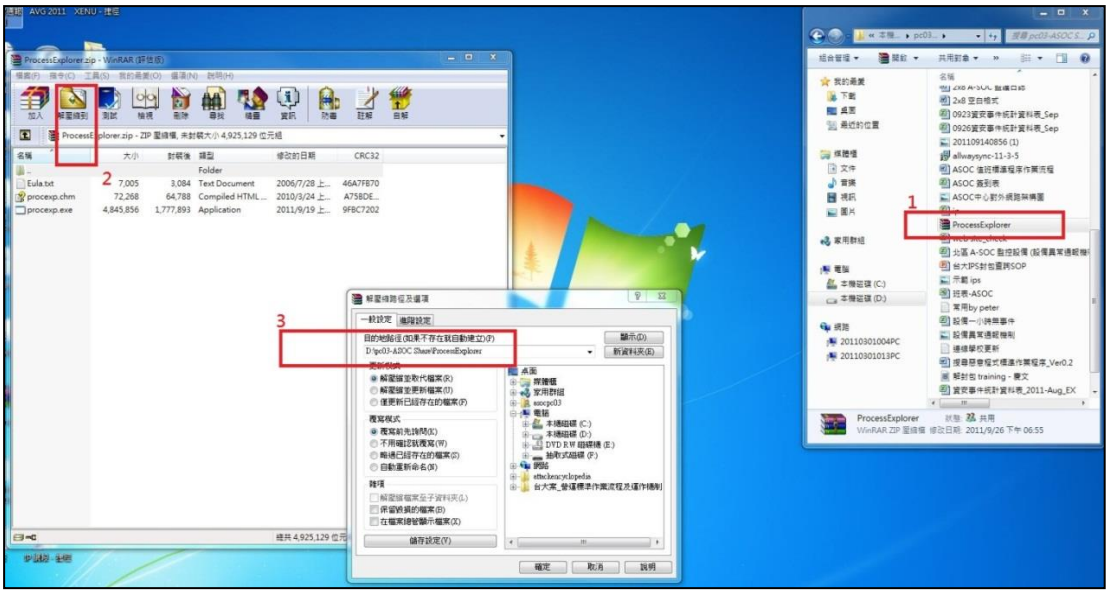
程式名稱 : Process Explorer
下載路徑 :
http://technet.microsoft.com/en-us/sysinternals/bb896653

2.3.2 解壓縮檔案

2.3.2.1 請將下載後的程式,進行解壓縮,步驟如下.

步驟一:滑鼠點選下載的程式兩下
步驟二:點選解壓縮檔案至此
步驟三:存放至指定位置

請參考下圖
(各電腦因安裝的解壓縮軟體不同,可能有不同的解壓縮方式,本手冊以 WinRAR 解壓縮軟體作為範例)



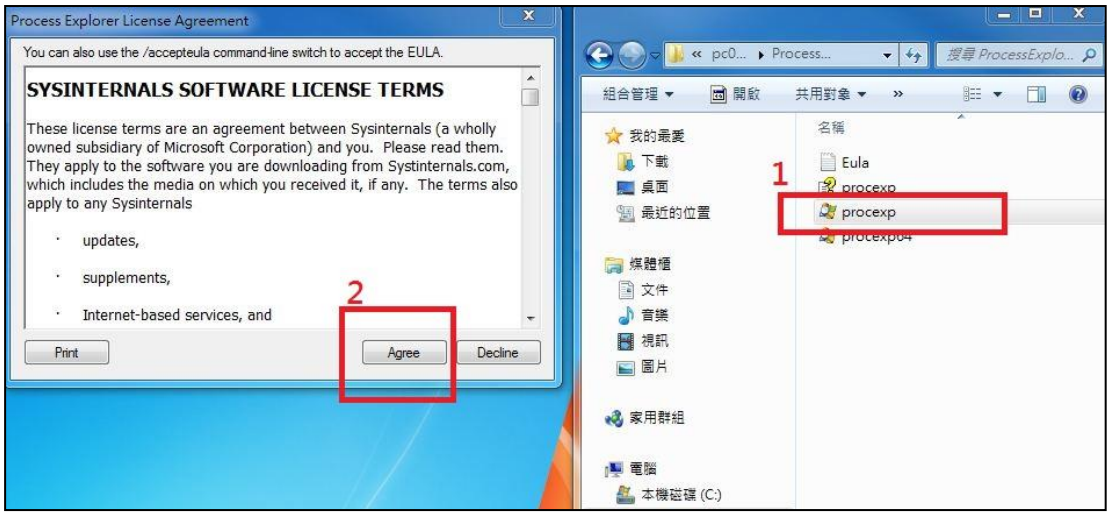
2.3.3 安裝程式

2.3.3.1 安裝程式步驟如下

步驟一:點擊已解壓縮檔案夾內之 procexp.exe

步驟二:出現版權說明頁後,再點擊 Agree

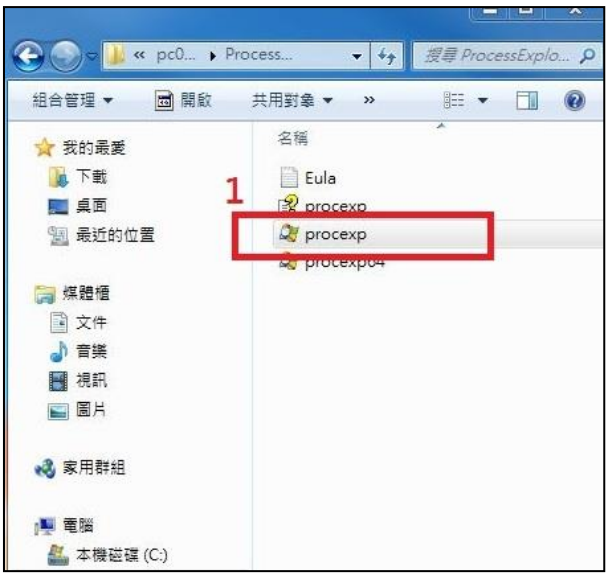
請參考下圖



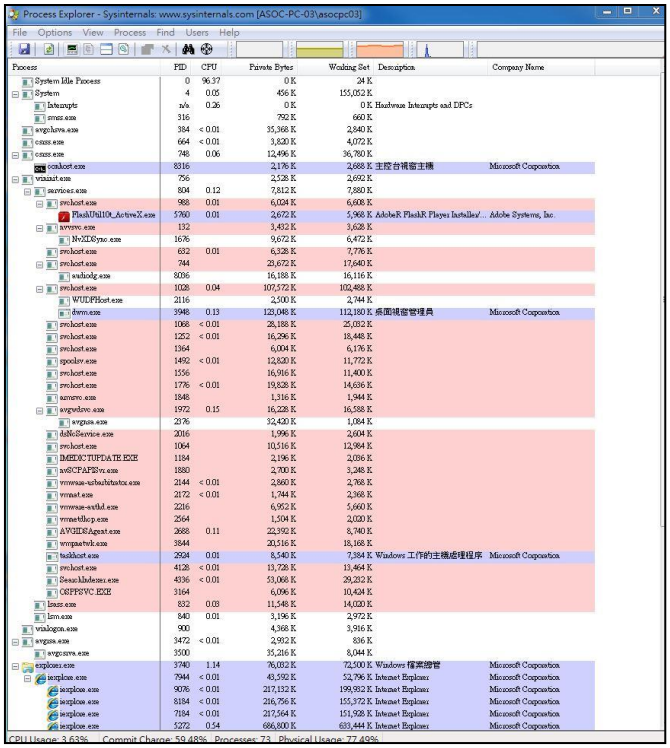
2.3.4 執行程式

2.3.4.1 執行程式,步驟如下

步驟一:點選安裝路徑下之 procexp



點選後程式將會執行並將出現下列畫面,本畫面即為 procexp 軟體執行之主畫面



2.3.5 查找可疑程序

本步驟的目的在於找尋有無可疑的程式,在此工具中,您可找到目前電腦中,所有正在執行的程式,我們要從這些執行的程式中,尋找可疑的惡意程式.

2.3.5.1 檢查執行程式之存放路徑

惡意程式常會修改其檔案名稱,使其檔案名稱與正常程式一致,但檔案置放位置則無法與正常程式一致.

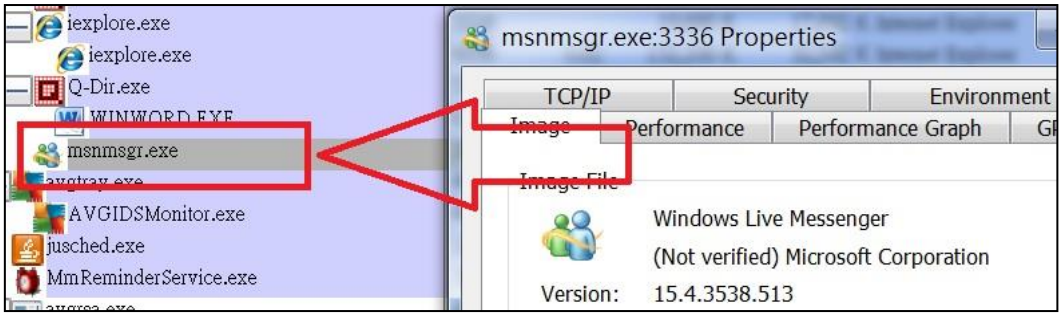
本步驟可查找出上述情況之惡意程式.

步驟一:

請逐一點選執行中的程序(Process),確認該程式安裝路徑是否與原廠設計之路徑不同,若有不同,很可能代表程序假造相同名稱,很可能為惡意程式,

本範例以 Msnmsgr.exe 為例.

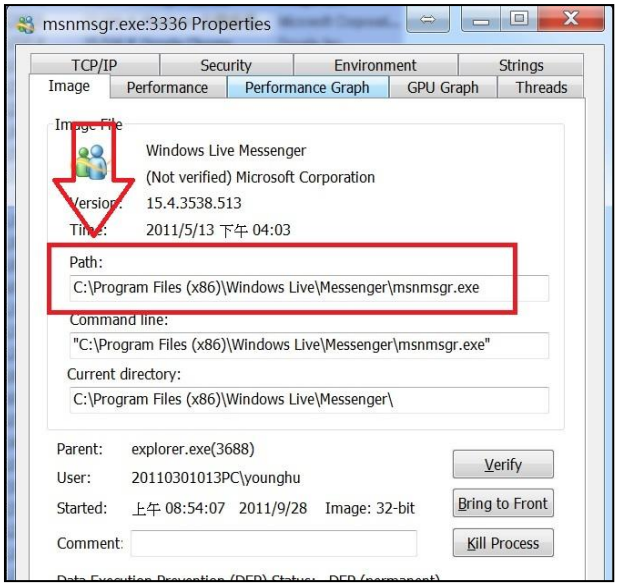
請於 Process 欄位中,點選 msnmsgr.exe 此執行中之程序



步驟二:

點選 Image 頁籤,並查看 Path:項目,此項目為該程式存放位置,本範例路徑為

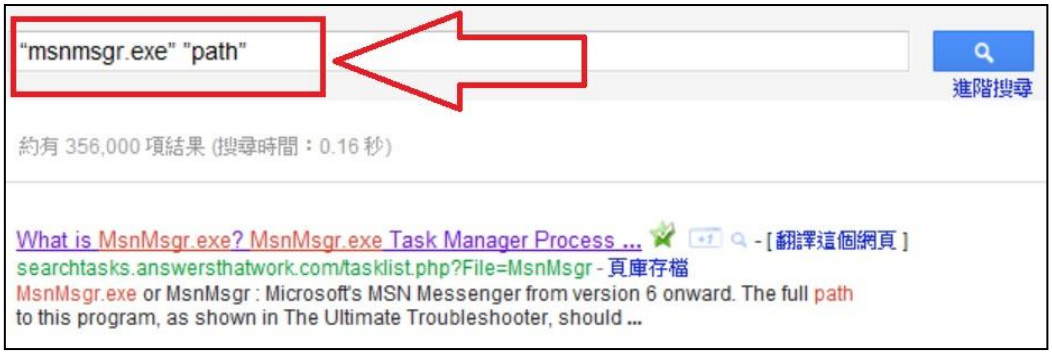
C:\Program Files (x86)\Windows Live\Messenger\msnmsgr.exe



步驟三:

請至Google查詢該程式正確之路徑為何,可於Google 搜尋列中打入下列關鍵字

“msnmsgr.exe” ” path”



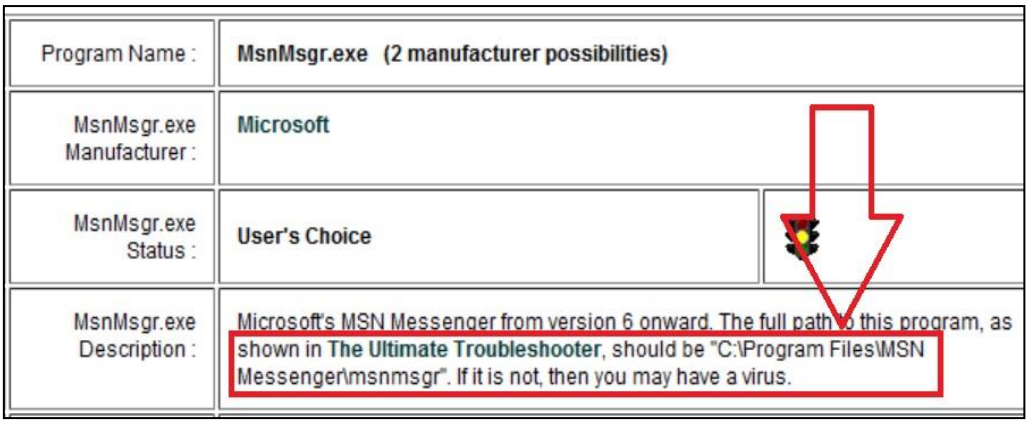
步驟四:

查詢搜尋結果,並確認 msnmsgr.exe 正確安裝路徑.

搜尋結果其路徑如下.

注意:

依據作業系統版本不同(如 Windows XP, Windows Vista, Windows 7 等)C:\Program\此路徑名稱會有所不同.



步驟五:

比對 Google 查詢結果及步驟二所獲得之路徑,兩者為相同路徑,此代表此程序與原廠設計之路徑相同,可初步排除其為惡意程式.

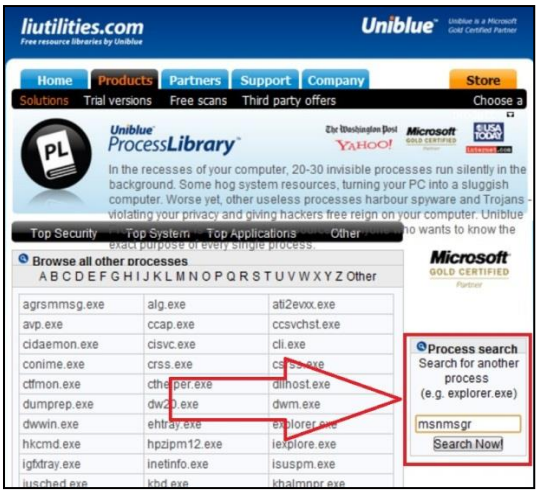
步驟六:

若於 Goolge 查無相關資訊,可於下列網站進行查詢

http://www.liutilities.com/products/wintaskspro/processlibrary/

步驟七:

進入該網站後,使用 Process search 進行該程序搜尋,於 Process search 置入程序名稱,如 **msnmsgr**,並點擊下方 Search Now 按鈕,請見下圖



步驟八:

由此搜尋結果可獲得此程序更完整的說明,請見下圖.

步驟九:

請紀錄 Google 查詢結果與步驟二結果,路徑不一致者.

2.3.6 紀錄可疑程序

請將發現的可疑程序紀錄,並於 3 結果回報時,一併回報給網管人員.

2.4 由系統啟動區查找惡意程式

系統啟動區常可發現惡意程式的蹤跡,本區檢查重點在於是否有未經數位簽章或是異常程序.

2.4.1 請下載下列程式

程式名稱 : Autoruns for Windows

下載路徑 :

http://technet.microsoft.com/en-us/sysinternals/bb963902

2.4.2 解壓縮檔案

2.4.2.1 請將下載後的程式,進行解壓縮,步驟如下.

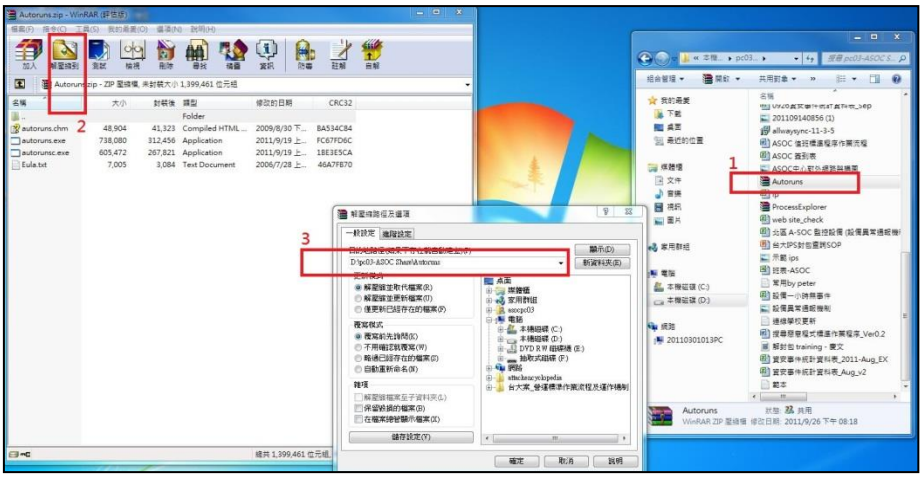
步驟一:滑鼠點選下載的程式兩下

步驟二:點選解壓縮檔案至此

步驟三:存放至指定位置

請參考下圖

(各電腦因安裝的解壓縮軟體不同,可能有不同的解壓縮方式,本手冊以 WinRAR 解壓縮軟體作為範例)



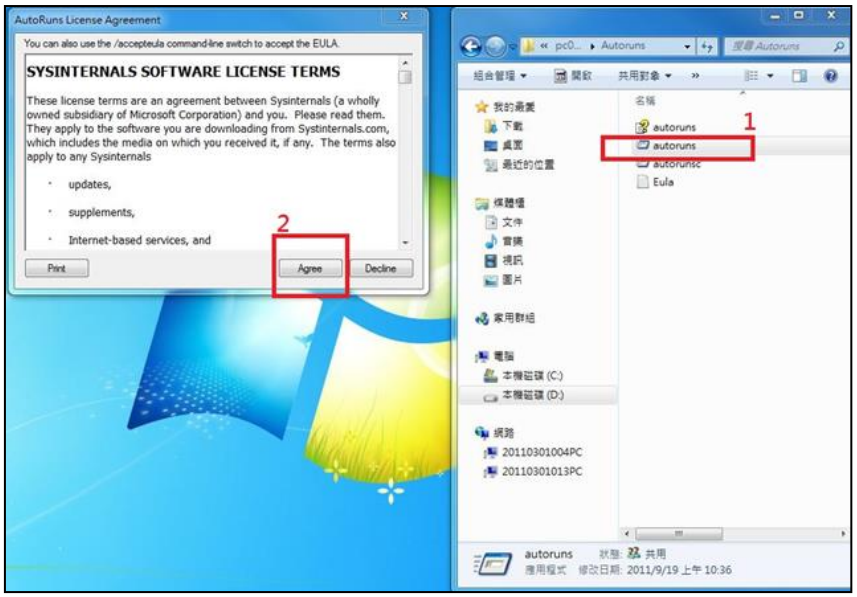
2.4.3 安裝程式

2.4.3.1 安裝程式步驟如下

步驟一:點擊已解壓縮檔案夾內之 Autoruns.exe

步驟二:出現版權說明頁後,再點擊 Agree

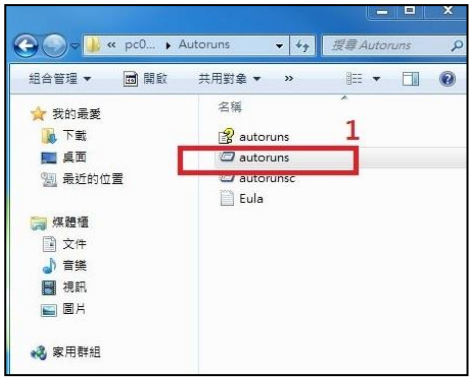
請參考下圖



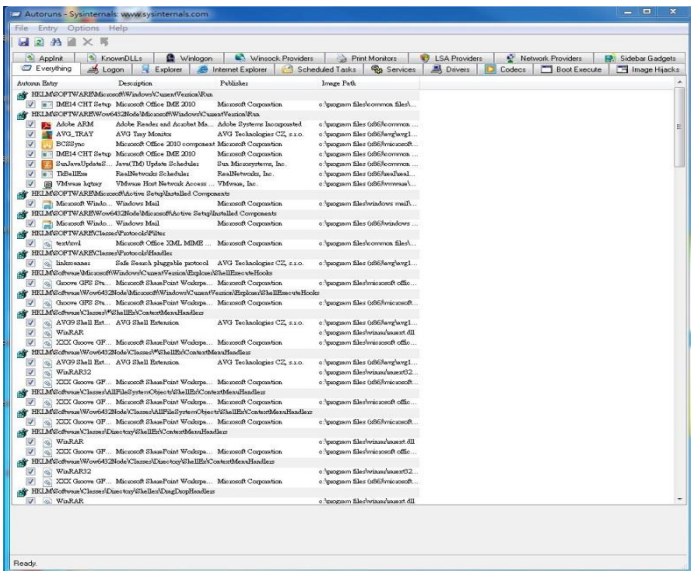
2.4.4 執行程式

2.4.4.1 執行程式,步驟如下

步驟一:點選安裝路徑下之 autoruns



點選後程式將會執行並將出現下列畫面,
本畫面即為 autoruns 軟體執行之主畫面



2.4.5 查找系統啟動區可疑程序

2.4.5.1 請點選軟體最上方 Options 頁籤,並勾選下列兩個選項,分別如下

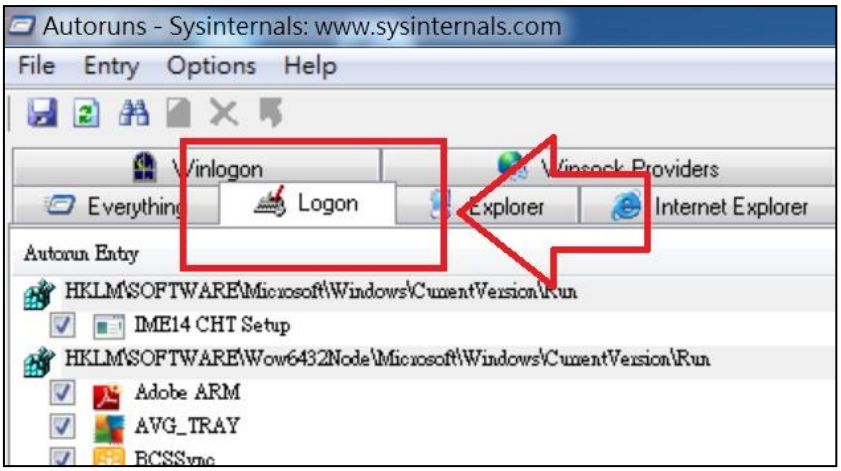
2.4.5.1.1.1 Verify Code Signatures

2.4.5.1.1.2 Hide Microsoft and Windows Entries

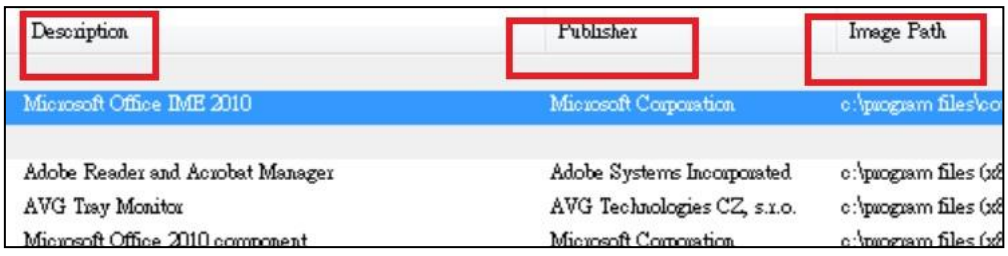
勾選後,則軟體會檢查每個程式的數位簽章並隱藏 Microsoft 所提供之項目,以加速查找可能之惡意程式.

如下圖

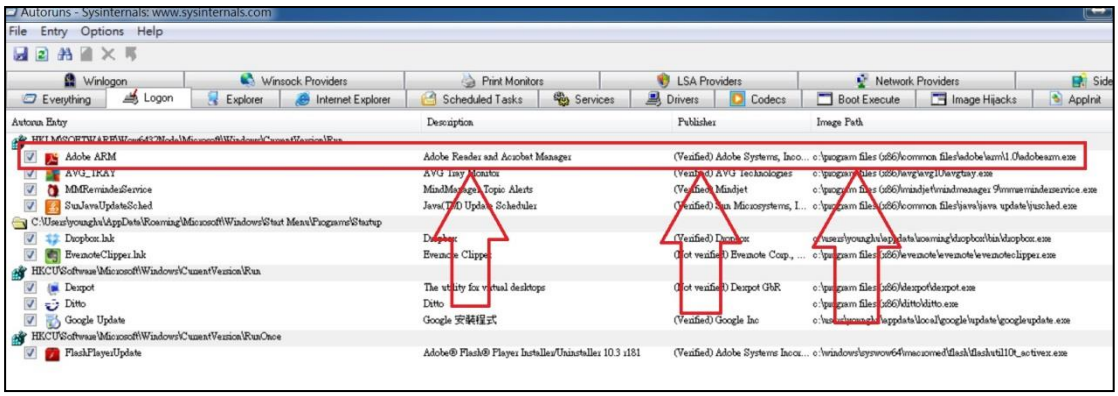
2.4.5.2 將頁面移動至『Logon』，
準備進行查找惡意程式,如下圖



2.4.5.3 於『Logon』頁面下,查找 Description, Publisher, Image Path 三項目.請參考下圖.



2.4.5.4 請記錄 Description, Publisher, Image Path 三欄位中任一為空白者,這可能是惡意程式.請參考下圖.



2.4.6 紀錄系統啟動區可疑程序

請將 2.1.6 及 2.2.5.4 兩項目之記錄內容, 整理後進入「步驟 3. 結果回報」流程.

3 結果回報

請將步驟 2.1 至 2.4 所發現之惡意程式或誤判作紀錄, 並回報給網路或系統管理者, 若需技術支援, 請洽臺大計算機中心北區教育資訊安全維運中心.

電話(02)23651106

臺大校內分機 65013

附件 1、查找可疑網路封包(Packet)

SmartSniff 是一款可擷取通過網路卡之 TCP/IP 封包的免費軟體，並可讓您檢視所擷取的客戶端與伺服器之間溝通傳輸的資料。您可以 ASCII 模式檢視文字型通信協定（如 HTTP, SMTP, POP3 和 FTP）或以 16 進位模式檢視非文字型通信協定（如 DNS）的 TCP/IP 溝通傳輸資料。

系統需求：
只要系統安裝了 WinPcap 擷取驅動程式且 WinPcap 與網路（配接）卡相容，那麼 SmartSniff 就可在任何 32 位元 Windows 作業系統（Windows 98/ME/NT/2000/XP/2003/Vista/2008/7）上擷取 TCP/IP 封包。
在 Windows 2000/XP（或以上）的作業系統下，SmartSniff 亦可在不安裝任何擷取驅動程式的情況下採用 'Raw Sockets' 法來擷取 TCP/IP 封包。

1.1.1 請下載下列程式

程式名稱 : Smssnif
下載路徑 : http://www.nirsoft.net/utils/smsniff.zip

1.2.1 解壓縮檔案

請將下載後的程式,進行解壓縮,步驟如下.

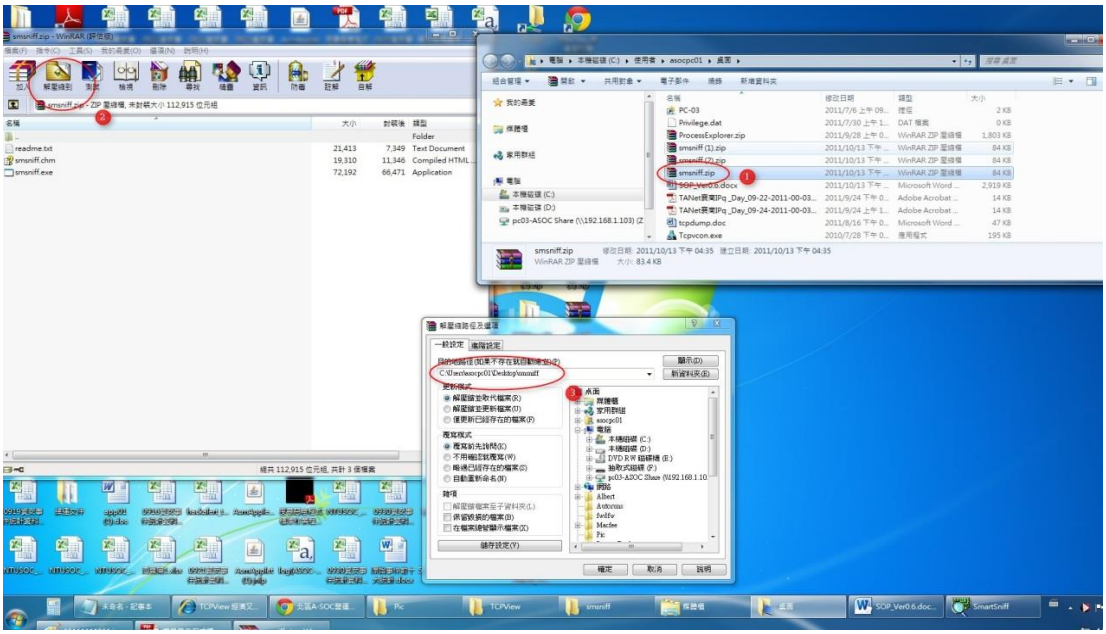
1.2.2　步驟一:滑鼠點選下載的程式兩下

1.2.3　步驟二:點選解壓縮檔案至此

1.2.4　步驟三:存放至指定位置

請參考下圖

(各電腦因安裝的解壓縮軟體不同,可能有不同的解壓縮方式,本手冊以 WinRAR 解壓縮軟體作為範例)



1.3.1　安裝程式

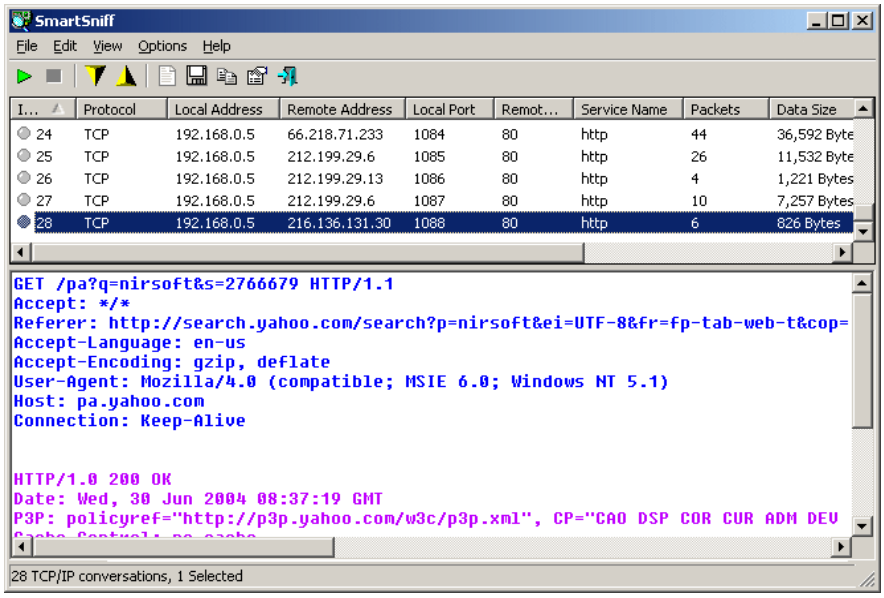
安裝程式步驟如下.

1.3.2　步驟一:點擊已解壓縮檔案夾內之Smssniff.exe

1.3.3　步驟二:出現版權說明頁後,再點擊Agree執行程式

1.3.4　步驟三:選擇安裝路徑後即可完成安裝

本畫面即為 Smssniff 軟體執行之主畫面

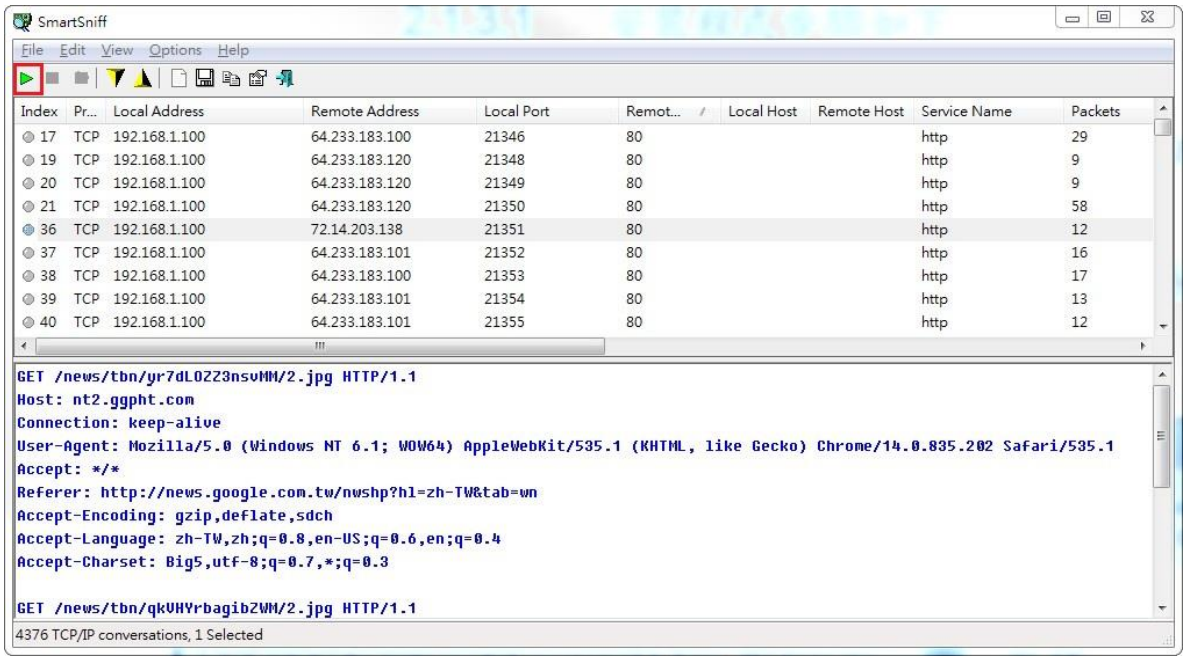


1.4.1 查找可疑網路封包

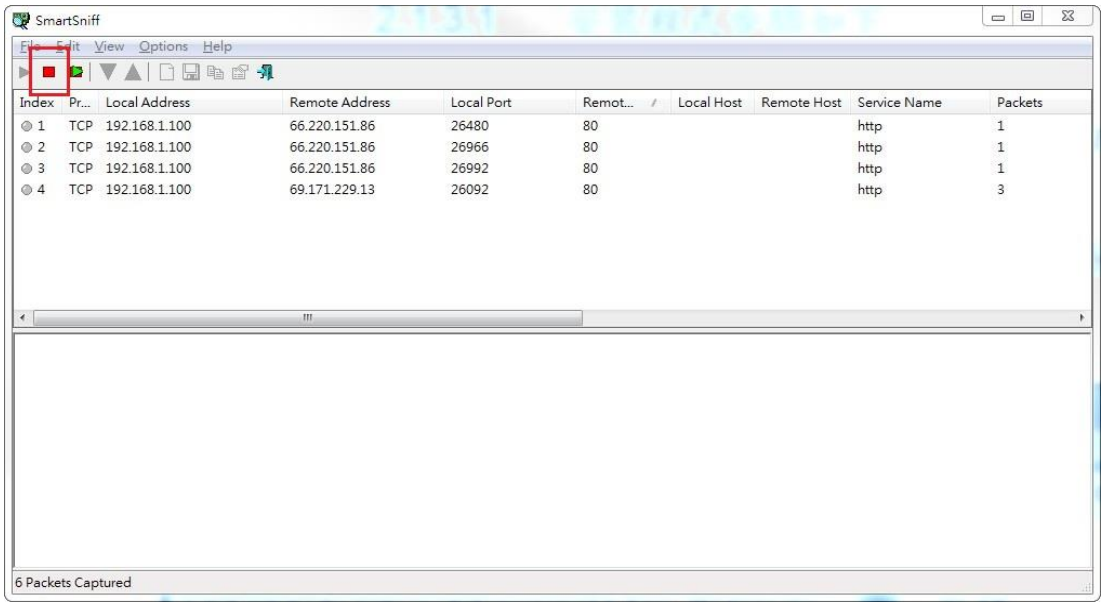
1.4.2 步驟一：從本中心所發出的資安告警信中可得知攻擊來源 IP 的位置及 Port 跟目標 IP 及 port

事件類型	對外攻擊	風險等級	第1級事件
發生時間	2011-10-09 15:36:59.000	發生次數	16
擊來源IP	[redacted]	攻擊來源PORT	63230
目標IP	[redacted]	目標PORT	21

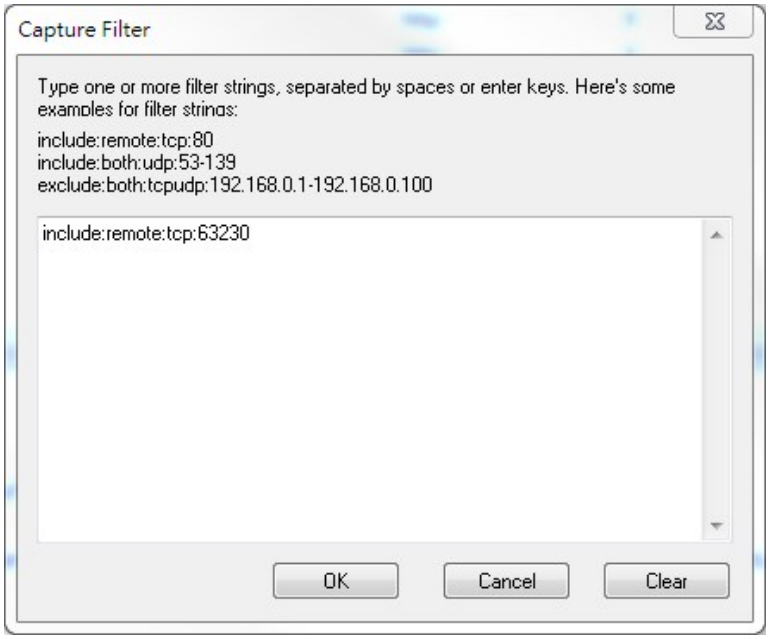
1.4.3 步驟二:開啟 SmartSniff 主程式並點選左上綠色箭頭開始執行封包擷取作業，使用者可在封包執行擷取時，正常的使用電腦



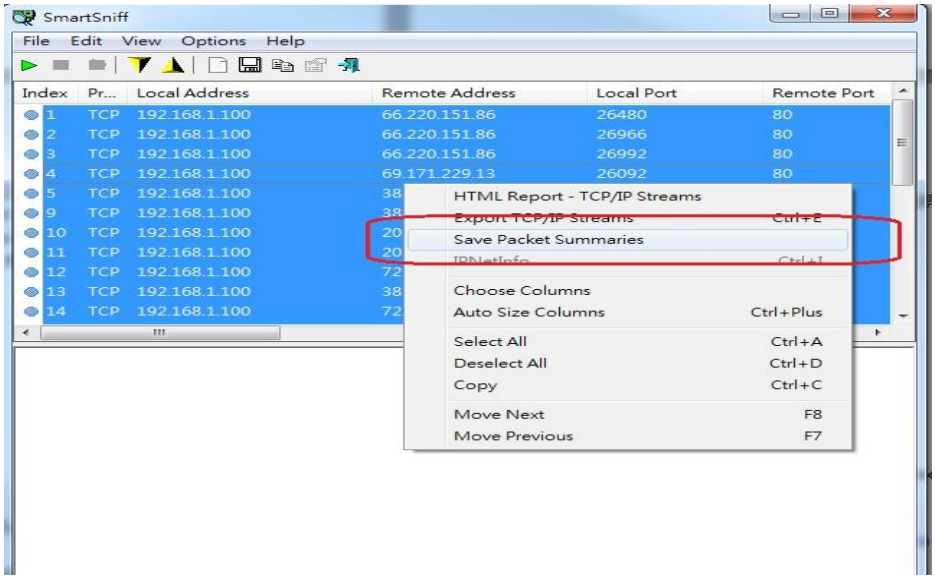
1.4.4 步驟三:待一段時間後，請點選左上方紅色方形按鈕來停止封包的擷取

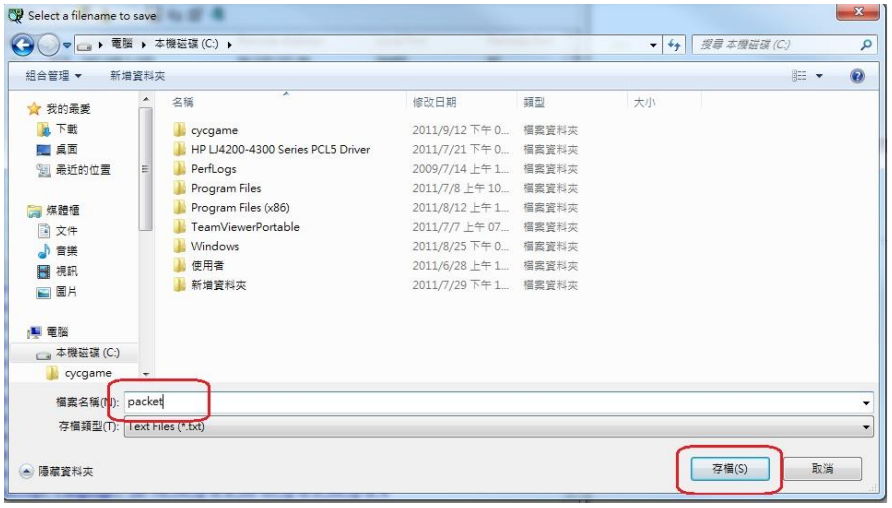


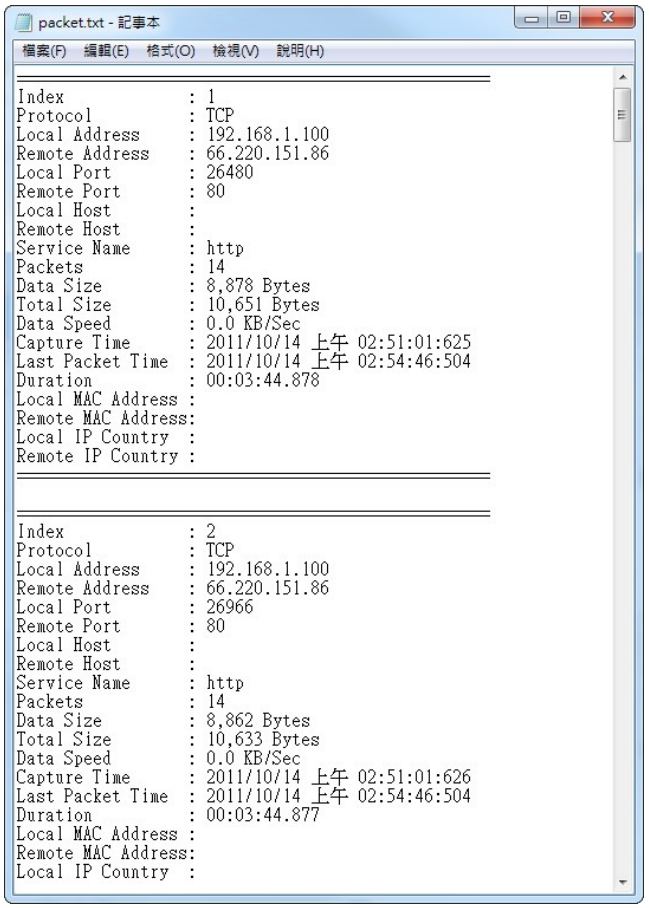
1.4.5　步驟四:在經過一段時間的擷取後，便會累積一定的封包數量，而此時則必須過濾所擷取的封包資料，可使用快捷鍵 Ctrl+F8 來啟動過濾條件的對話框，在對話框中輸入”include:remote:tcp:63230”即可過濾相關資料封包



1.4.6　步驟五:將過濾出來的封包資料利用 Ctrl+A 全選後，點選右鍵並執行”Save Packet Summaries”來儲存所選取的封包資料，並將封包資料 Email 至本中心電子郵件信箱(*ntuasoc@ntu.edu.tw*) 來過得更進一步的技術支援


SmartSniff
File Edit View Options Help
Index Pr... Local Address Remote Address Local Port Remote Port
1 TCP 192.168.1.100 66.220.151.86 26480 80
2 TCP 192.168.1.100 66.220.151.86 26966 80
3 TCP 192.168.1.100 66.220.151.86 26992 80
4 TCP 192.168.1.100 69.171.229.13 26092 80
5 TCP 192.168.1.100
9 TCP 192.168.1.100
10 TCP 192.168.1.100
11 TCP 192.168.1.100
12 TCP 192.168.1.100
13 TCP 192.168.1.100
14 TCP 192.168.1.100
HTML Report - TCP/IP Streams
Export TCP/IP Streams Ctrl+E
Save Packet Summaries
Choose Columns
Auto Size Columns Ctrl+Plus
Select All Ctrl+A
Deselect All Ctrl+D
Copy Ctrl+C
Move Next F8
Move Previous F7


Select a filename to save
電腦 本機磁碟 (C:)
組合管理 新增資料夾
我的最愛
下載
桌面
最近的位置
媒體櫃
文件
音樂
視訊
圖片
電腦
本機磁碟 (C:)
cycgame
名稱 修改日期 類型 大小
cycgame 2011/9/12 下午 0... 檔案資料夾
HP LJ4200-4300 Series PCL5 Driver 2011/7/21 下午 0... 檔案資料夾
PerfLogs 2009/7/14 上午 1... 檔案資料夾
Program Files 2011/7/8 上午 10... 檔案資料夾
Program Files (x86) 2011/8/12 上午 1... 檔案資料夾
TeamViewerPortable 2011/7/7 上午 07... 檔案資料夾
Windows 2011/8/25 下午 0... 檔案資料夾
使用者 2011/6/28 上午 1... 檔案資料夾
新增資料夾 2011/7/29 下午 1... 檔案資料夾
檔案名稱(N): packet
存檔類型(T): Text Files (*.txt)
隱藏資料夾
存檔(S)
取消


packet.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
Index : 1
Protocol : TCP
Local Address : 192.168.1.100
Remote Address : 66.220.151.86
Local Port : 26480
Remote Port : 80
Local Host :
Remote Host :
Service Name : http
Packets : 14
Data Size : 8,878 Bytes
Total Size : 10,651 Bytes
Data Speed : 0.0 KB/Sec
Capture Time : 2011/10/14 上午 02:51:01:625
Last Packet Time : 2011/10/14 上午 02:54:46:504
Duration : 00:03:44.878
Local MAC Address :
Remote MAC Address:
Local IP Country :
Remote IP Country :
Index : 2
Protocol : TCP
Local Address : 192.168.1.100
Remote Address : 66.220.151.86
Local Port : 26966
Remote Port : 80
Local Host :
Remote Host :
Service Name : http
Packets : 14
Data Size : 8,862 Bytes
Total Size : 10,633 Bytes
Data Speed : 0.0 KB/Sec
Capture Time : 2011/10/14 上午 02:51:01:626
Last Packet Time : 2011/10/14 上午 02:54:46:504
Duration : 00:03:44.877
Local MAC Address :
Remote MAC Address:
Local IP Country :

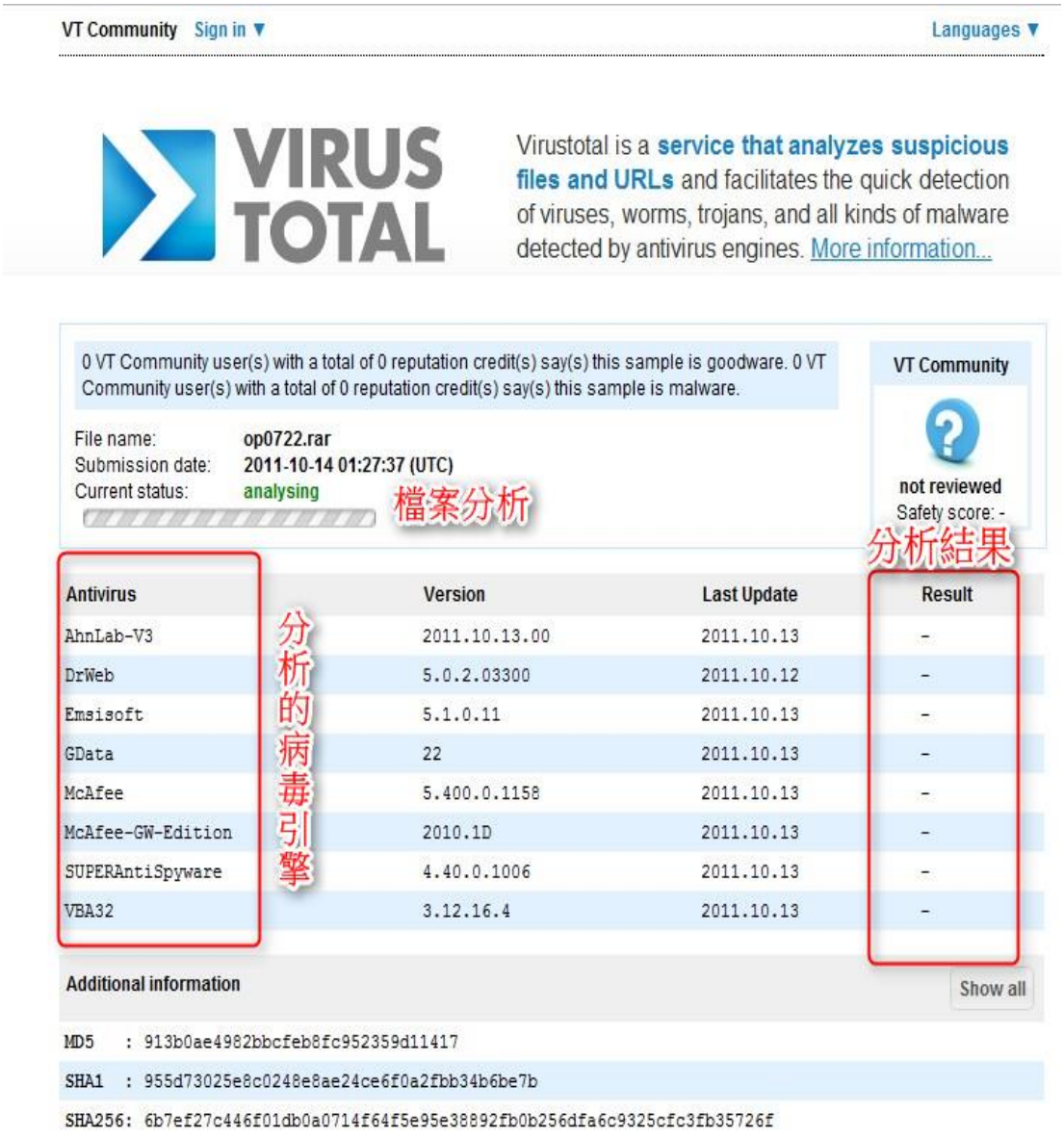
附件 2 線上掃毒

若使用者發現可疑檔案，想進一步確認檔案是否安全，則可以使用線上掃毒來達成單一檔案的掃瞄。VirusTotal 提供了免費的掃描服務，可同時提供多個病毒掃描引擎，使用方法如下:

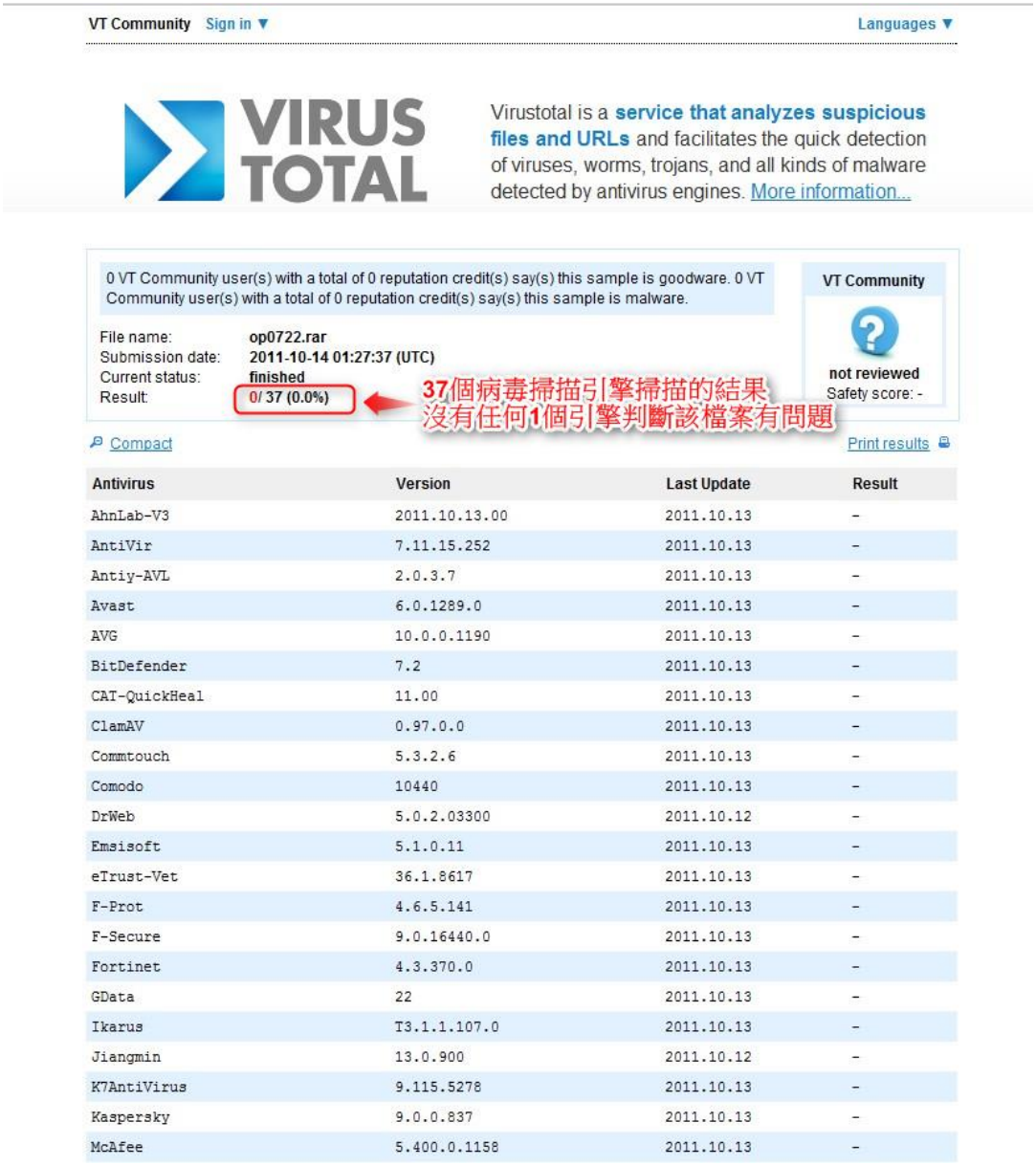
請以瀏覽器連接至：http:// www.virustotal.com/ ，要掃描檔案的話，請切換至「Upload a file」，接著選擇欲掃描的檔案後按「Send file」來上傳，待上傳完畢後就會自動開始掃描。若要掃描網頁則切換到「Submit a URL」。

下圖就是掃描的過程，VirusTotal 會一邊掃描一邊把掃描完成的結果列

出，如果 Result 一欄是「-」為正常，則代表並無中毒。

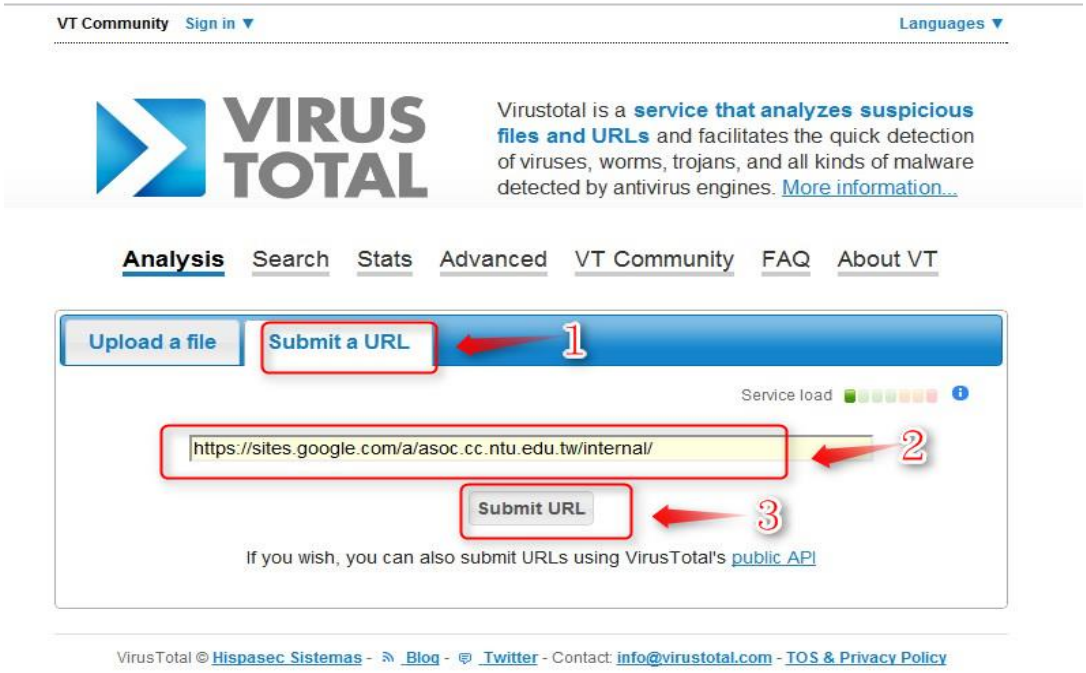


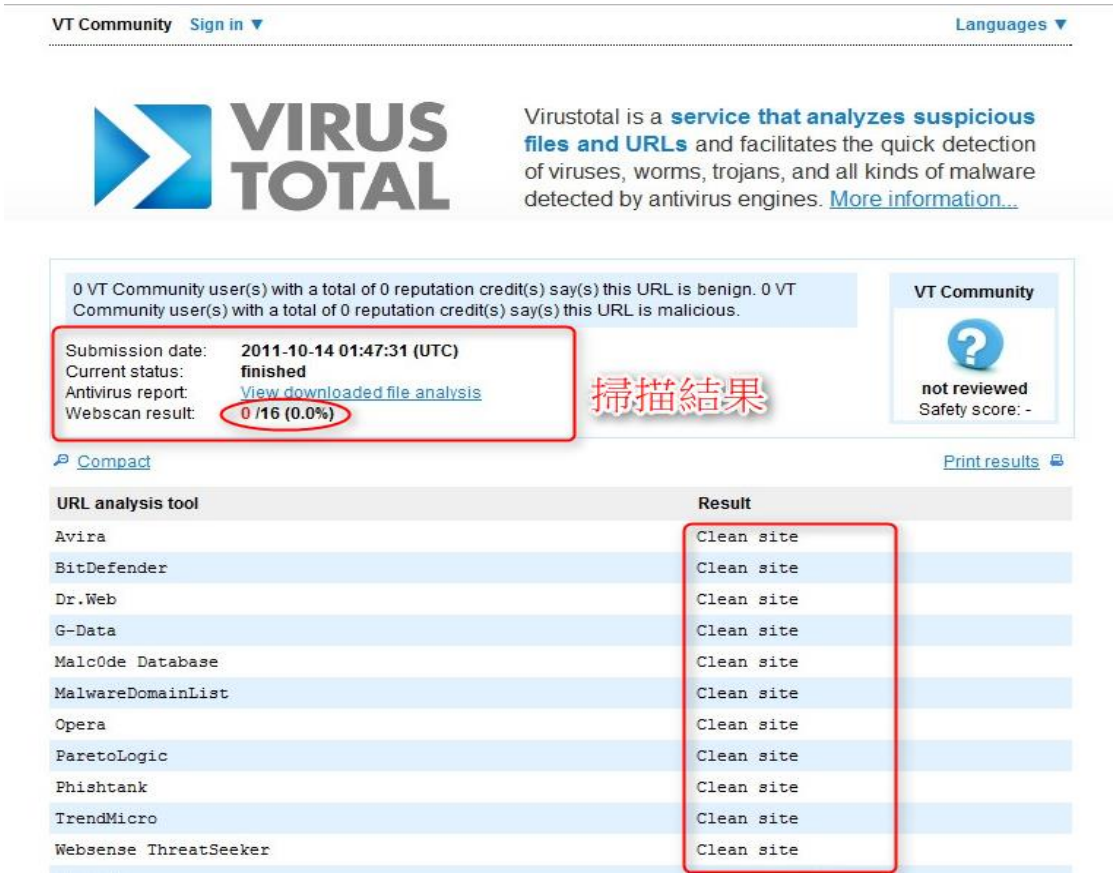
完全掃描完之後，便會將掃描的結果以簡單的報告方式呈現，以範例來看，在 37 個掃描引擎中，AntiVir 所有使用的掃毒病毒引擎都判定這個檔案是沒問題的。



Antivirus	Version	Last Update	Result
AhnLab-V3	2011.10.13.00	2011.10.13	-
AntiVir	7.11.15.252	2011.10.13	-
Antiy-AVL	2.0.3.7	2011.10.13	-
Avast	6.0.1289.0	2011.10.13	-
AVG	10.0.0.1190	2011.10.13	-
BitDefender	7.2	2011.10.13	-
CAT-QuickHeal	11.00	2011.10.13	-
ClamAV	0.97.0.0	2011.10.13	-
Commtouch	5.3.2.6	2011.10.13	-
Comodo	10440	2011.10.13	-
DrWeb	5.0.2.03300	2011.10.12	-
Emsisoft	5.1.0.11	2011.10.13	-
eTrust-Vet	36.1.8617	2011.10.13	-
F-Prot	4.6.5.141	2011.10.13	-
F-Secure	9.0.16440.0	2011.10.13	-
Fortinet	4.3.370.0	2011.10.13	-
GData	22	2011.10.13	-
Ikarus	T3.1.1.107.0	2011.10.13	-
Jiangmin	13.0.900	2011.10.12	-
K7AntiVirus	9.115.5278	2011.10.13	-
Kaspersky	9.0.0.837	2011.10.13	-
McAfee	5.400.0.1158	2011.10.13	-

在網頁掃描的部分也是相同操作，只要切換到「Submit a URL」並輸入網頁的網址就可以進行掃描了，以北區 A-SOC 營運中心網址為例，掃描的結果如下，「Clean site」代表是安全的。


VT Community Sign in ▼
Languages ▼
VIRUS TOTAL
Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...
Analysis Search Stats Advanced VT Community FAQ About VT
Upload a file
Submit a URL
1
Service load
https://sites.google.com/a/asoc.cc.ntu.edu.tw/internal/
2
Submit URL
3
If you wish, you can also submit URLs using VirusTotal's public API
VirusTotal © Hispasec Sistemas - Blog - Twitter - Contact: info@virustotal.com - TOS & Privacy Policy


VT Community Sign in ▼
Languages ▼
VIRUS TOTAL
Virustotal is a service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. More information...
0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this URL is benign. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this URL is malicious.
Submission date: 2011-10-14 01:47:31 (UTC)
Current status: finished
Antivirus report: View downloaded file analysis
Webscan result: 0 /16 (0.0%)
掃描結果
VT Community
not reviewed
Safety score: -
Compact
Print results
URL analysis tool
Result
Avira Clean site
BitDefender Clean site
Dr.Web Clean site
G-Data Clean site
Malc0de Database Clean site
MalwareDomainList Clean site
Opera Clean site
ParetoLogic Clean site
Phishtank Clean site
TrendMicro Clean site
Websense ThreatSeeker Clean site