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 已下載更新之外,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: <u>http://www.microsoft.com/downloads/details.aspx?displaylang=z</u> h-tw&FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356

Microsoft [®] Download Cen	ter		下載項目 А-2▼	產品系列▼ 下載類別▼	說明 ▼
and the second second	<i>發尋鳌個下載中心</i> ⊙ 繁體中文 ⊙ 英文	bing 👂 🖡	2		
Microsoft® Windo	ws® 惡意軟體移除:	工具 (KB890830)		A Windows	5
簡 單 說 明 本工具會給查您的電腦是否有特定、 Sasser、Mydoon 等),並保助務保稅 個月第二個星期二發行本工具的更新	常見的惡意軟體(包括 Blaster、 响的惡意軟體。 Microsoft 將於每 版本。	本頁內容 ↓ 快速詳細說明 ↓ 塗驗 ↓ 孟絲要求 ↓ 說明 ↓ <u>相純連結</u> ↓ 其他使用者正在下版的報	±	Windows•Internet Explorer 體驗 ⋅ 速度之美 立即下載	9
檔案名稱: windows-kb890830-v4.2.exe	檔案 7 14.4 N	大小: 1B 下載			

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

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」。

輸入程式、資料夾、文件或網際網路資源的名稱,Windows 會自動開設。
開啟(O): mrt.exe ▼
確定 取消 瀏覽(B)



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。

S Microsoft Windows 惡意軟體移除工具 - 2011 年 11 月 ₩
掃描類型
諸選擇掃描類型:
● 快速掃描。掃描系統中最有可能包含惡意軟體的區域。若找到惡意軟體,系統 ● 會提示您執行完整掃描。(Q)
○ 完整掃描。掃描整個系統。請注意,在部分電腦上此掃描可能會需要花費數小 時的時間。(F)
◎ 自訂掃描。除了快速掃描外,此工具也會掃描使用者指定的資料夾內容。(C)
選擇資料夾
<上一步(B)[下一步(N)>] 取消

icrosoft Windows 惡意軟體移除工具 - 2011 年 11 月	23			
在掃描您的電腦	5			
工具正在掃描您電腦中的普及惡意軟體,並會在找到後移除它。 在此操作完成後,工具將會提供您一份報告並列出值測到並且已移除的惡意軟體。				
目前正在掃描:				
C:\Windows\system32\DRIVERS\srvnet.sys 已掃描檔案數: 3303				
風染的檔案數:0 開始時間:下午 11:22				
經過時間: 00:00:50	J			
(<上一步(B)) (下一步(N) >) (取消			

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;

📢 Microsof	t Windows 惡意軟體移除工具 - 2011 年 11 月
掃描結果	
	沒有偵測到惡意軟體。
	<u>檢視掃描的詳細結果。</u>
	此工具並不能取代防毒產品。若要協助保護您的電腦,您應該使用防毒產 品。若要取得詳細資訊,請瀏覽 <u>保護您的電腦</u> 。
	<上一步(B) 完成 取消

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。

S Microsoft Windows 惡意軟體移除工具 - 2011 年 11 月	23
掃描類型	
請選擇掃描類型 :	
○ 快速掃描。掃描系統中最有可能包含惡意軟體的區域。若找到惡意軟體,系統 ●提示您執行完整掃描。(Q)	
◎ 完整掃描。掃描整個系統。請注意,在部分電腦上此掃描可能會需要花費數小 ● 時的時間。(F)	
○ 自訂掃描。除了快速掃描外,此工具也會掃描使用者指定的資料夾內容。(C)	
選擇資料夾	
<上一步(B) (下一步(M) >) 取()	5

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。	請使用防毒軟體(更新最新病毒碼)進行掃
	在電腦上找到可疑的檔案時,就會出現這	毒,並跳至步驟3結果回報(回傳 mrt.log
	個結果。如果要協助移除這些檔案,請使	檔及掃毒結果)。
	用最新的防毒產品。	
4	發現感染,並移除部分感染。	請使用防毒軟體(更新最新病毒碼)進行掃
	如果要完成此移除作業,請使用最新的防	毒,並跳至步驟3 結果回報 (回傳
	毒產品。	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/bb897

<u>437. aspx</u>

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

CPView		▼ 4 9 搜尋 TCF	View	\$
組合管理 👻 💼 開啟 共用對象 👻 🖉	堯錄 新増資料夾			
☆ 我的最愛	名稱	修改日期	類型	大小
	Eula.txt	2006/7/28 上午 0	文字文件	
ਡ 煤體櫃	🛃 Tcpvcon.exe	2010/7/28下午 0	應用程式	19
	👔 tcpview.chm	2010/7/2 下午 04	編譯的 HTML 說	4
3. 家用群組	🛃 Tcpview.exe	2011/7/25 下午 1	應用程式	29
	CPVIEW.HLP	2002/9/2 下午 01	說明檔	
♀ pc03-ASOC Share (\\192.168.1.103) (Z:)				
■ Topview.exe 修改日期: 2011/7/25	下午 12:40 建立日期: 2011/10/13	¹¹¹ 下午 02:45		

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(编號):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:

🛃 TCPView - Sy	ysinternals: www.s	ysinternals.con	n					
File Options	Process View	Help						
🕷 🛪 🗹)							
Process System	PID 4	Protocol TCP	Local Address 192.168.1.100	Local Port 25078	Remote Address 192.168.1.103	Remote Port 445	State ∇ ESTABLISH	
E svchost.ex	e 4512 e 4600	TCP V6 TCP	[re80;0;0;0;0;4];e606;d;04b;4940] 192:168:1.100	1055 20262	[fe8000.00.56184.cb1bx43fbx44e1] 72.14.203.103	3587 443	ESTABLISH ESTABLISH	
Federation C	Carline 2 C	L'assiss A	Territo de la compañía					
Endpoints: 3	established: 3	Listening: 0	rime wait u Close Wait: 0					Ť.

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	122.124.37.131	攻擊來源 PORT 63230
目標IP	100.00 114.0	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。

	ss View Help						
- * * 🕅							
Tocess	PID Protoco	l Local Address	Local Port	Remote Address	Remote Port	State 🗸	
System Process System Process System Process System sychost.exe	0 TCPV6 0 TCPV6 0 TCPV6 4 TCP 4512 TCPV6	[fe80:0:0:0:d3f:e60 [fe80:0:0:0:d3f:e60 [fe80:0:0:0:d3f:e60 192.168.1.100 [fe80:0:0:0:d3f:e60	6:d04b:4940] 2869 6:d04b:4940] 2869 6:d04b:4940] 20899 25078 6:d04b:4940] 1055	[fe80:0:0:0:256e:1efa:32ad:a55d] [fe80:0:0:0:256e:1efa:32ad:a55d] [fe80:0:0:0:6d3d:cb1b:d3fb:44e1] 192.168.1.103 [fe80:0:0:0:6d3d:cb1b:d3fb:44e1]	50189 50184 3587 445 3587	TIME_WAIT TIME_WAIT TIME_WAIT ESTABLISH ESTABLISH	
System	4 Process Pr End Proce	operties ss	:d04b:4940] 2869	[fe80:0:0:0:256e:1efa:32ad:a55d]	50192	ESTABLISH	
	Close Cor Whois	nection Ctrl+W					
	Copy	Ctrl+C					

即可查到序相關資訊:

Properties	for chrome.exe: 4600	>
	Boogle Chrome	
0	Google Inc.	
Version.	14.00.0835.0202	
Path:		
	asocpc01\AppData\Local\	Google\Chrome\Application\chrome
		End Process

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。)

	Google Chrome	
9	Google Inc.	
Version:	14.00.0835.0202	
Path:		
C:\Users\	asocpc01\AppData\Local\Google\(Chrome\Application\chrome
		End Process

跳出確認視窗,按下「是」,該程序會立即終止。

TCPView	X
<u> </u>	Are you sure you want to terminate <chrome.exe>?</chrome.exe>
	是(Y) 否(N)

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/bb896 653

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)

ANG 2011 XENU- 地位		
	(승) - 📕 et 국립 🕽 pc	03_ • • • # ## pc03-ASOC S_ P
Provide polymer for Viergan (1946)	10111 · 🗃 110 ·	##### - > = - □ 0
電気の 用き(C) 工具(S) 気的品質(C) 電道(N) 説明(H)		名稱 *
	TE	1 288 A-SUL 監護日応
	RE AR	四 2x8 空口恒利 (副 0923管安事件统计管科表 Sep
	1 最近的位置	④ 0926資安事件統計資料表_Sep
Let a Andrew and Andr		201109140856 (1)
※ 本 (1) 新発後 第2 (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	D TO	15 ⁹ aliwaysync-11-3-5
Eulatut 2 7.005 8.04 Text Document 2005/7/28 上 46A7F870	小音楽	副 ASOC 簽到表
Procesp.chm 72,268 64,788 Compiled HTML_ 2010/3/24 上 A75BDE_	■ सह 1	▲ ASOC中心對外網路架構圖
procexp.exe 4,845,856 1,777,893 Application 2011/9/19 上 9FBC7202	🔤 🕮 K 📥 📥	
	and the second sec	ProcessExplorer
	2 家用群組	
		图) 台大PS封句直跨SOP
	·····································	■ 示範 ips
■ 結果は時位決壊項 P 22		图 班表-ASOC
3	0.00	 高用by peter 記憶一小時無事件
目的地路信仰県不存在我自動建立の 離示の	● 開始 ● 20110201004PC	L 設備異常通報機制
D tpc03-ADOC ShareProcentExplorer 电前波转来应)	20110301013PC	■ 連線學校更新
		 型 授导感意程式標準作業程序_Ver0.2
● 解放建築時代構成(2) ● 課題種種		画 彩虹包 training - 使义 図) 安安国牛将针穿利表 2011-Aun FX
● 運更新已經存在的編集(F) ● 第 works/03		* *
● ● 単電話 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	ProcessExplorer	秋型 23 共用
● 夜寫前先說問(5) 中一二本總服權 (0-)	WinRAR ZIP 聖總有	I 修改日期: 2011/9/26下午 06:55
○ 市利用国ESKK(A)(7) お 品 DVD EF 開設機 (5) ○ 解除日常存在的需求(5) → 抽除(3)に関係(6)	e	
回顧重新命名(0) 田報重新命名(0) 田和和和和和和和和和和和和和和和和和和和和和和和和和和和和和和和和和		
日本 構成 日本 構成 日本 構成 日本 構成 日本 構成 日本 構成 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本		
— 解散線電業至子資料実(2)		
「本面積別が確実に」		
□ #〒4925,129 位元 備存設定(7) + "" +		
9-138-248 (87.5 (20.9)		
10°C 10°N 8871		

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

Process Explorer License Agreement	
You can also use the /accepteula command-line switch to accept the EULA.	④ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
SYSINTERNALS SOFTWARE LICENSE TERMS	組合管理 🔻 💼 開散 共用對象 🕶 » 🕮 💌 🗍 🔞
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals • updates, • supplements, • Internet-based services, and Print Agree Decline	★ 我的最美 名稿 ● 下載 □ Eula ■ 桌面 1 2 procexp ● 新述的位置 27 procexp ● かくれ ○ アのCEXP04 ● 常業 ● 常業 ■ 月 ●
	ℯ 象用群組
	[學 電腦 ▲ 本機磁碟 (C:)

2.3.4 執行程式

2.3.4.1 執行程式,步驟如下

🔾 🗢 📕 « pc0 🕨 F	rocess 👻 4 y	搜尋 Proce	essExplo 🔎
組合管理 👻 💼 開啟	共用對象 ▼ 》		
☆ 我的最愛 〕 下載 ■ 桌面	名稱 Eula 愛 procexp	*	
圖 最近的位置	🖉 procexp		
 □ 煤體櫃 ③ 文件 ♪ 音樂 副 視訊 	MC procexpo4		
 家用群組 電腦 			

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"

"msnmsgr.exe" "path"	٩
	進階搜尋
約有 356,000 項結果 (搜尋時間: 0.16 秒)	
What is MsnMsgr.exe? MsnMsgr.exe Task Manager Process, 💜 📧 Q - [翻譯這個網頁] searchtasks.answersthatwork.com/tasklist.php?File=MsnMsgr - 頁庫存檔 MsnMsgr.exe or MsnMsgr : Microsoft's MSN Messenger from version 6 onward. The full path to this program, as shown in The Ultimate Troubleshooter, should	

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.

Program Name :	MsnMsgr.exe (2 manufacturer possibilities)
MsnMsgr.exe Manufacturer :	Microsoft
MsnMsgr.exe Status :	User's Choice
MsnMsgr.exe Description :	Microsoft's MSN Messenger from version 6 onward. The full path this program, as shown in The Ultimate Troubleshooter, should be "C:\Program Files\MSN Messenger\msnmsgr". If it is not, then you may have a virus.

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/pro cesslibrary/ 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





由此搜尋結果可獲得此程序更完整的說明,請見下圖.





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 : <u>http://technet.microsoft.com/en-us/sysinternals/bb963</u> 902

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

🚱 🕘 🖉 🦇 pc0 • Autoruns 🔹 + + 🔊 🔊 🖉 Autoruns)
组合管理 • 🔜 開設 共用数象 • » 🖽 • 🛄 😧
 ★ 我的最美 ● 下数 ● 小数 ●

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

目合管理 🔻 💼 開啟	共用對象 ▼	8= -	- 💷	0
☆ 我的最愛	名稱	^		
🕠 下載	👔 autoruns	1		
📰 桌面	autoruns 🤤			
💹 最近的位置	😅 autorunsc			
煤體櫃				
文件				
→ 音樂				
🧾 視訊				
■ 圖片				

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

C Everything	aon 🧣 Explorer 🥭	nternet Explorer	duled Tasks	Ro Services	Daivers	Codecs	k Providers Boot Execute	Sidebar Gadget
atom Baty	Description	Publishes	Image Path	-				
HELMCOPTWAREMEN	notWindowsVCusentVessionWkn							
DME14 CHT Setup	Microsoft Office IME 2010	Missosoft Corporation	o 'program file	skommon files\				
HELMGOFTWAREWow	432Note Microsoft Windows/Cun	eatVenicalRua						
V Katobe ARM	Adobe Reader and Acushat Ma.	Adobe Systems Incorporated	o ipogaam file	s 6486/kcommon				
V AVG_TRAY	AVG Tasy Monitor	AVG Technologies CZ, sxo.	o 'program file	s (186)lavglavgl				
DCSSyno	Microsoft Office 2010 composes	Microsoft Corporation	o lpogasm file	e (s86/knicases#				
DME14 CHT Samp	Microsoft Office IME 2010	Microsoft Corporation	c:/program file	s (x86%common				
🔽 🞦 SunJavaUpdataS	Java(Thf) Update Schedules	Sua Miccorysteme, Inc.	o:\peogram file	s (186)kommas				
The line	RealNetworks Scheduler	RealNetworks, Inc.	c hpiogram file	s (185/heal/heal				
Vidwas hotay	VMwas Host Network Access	VMwas, Iac.	e l'program file	s 0/86/hmmeaa1				
HELM'SOFTWAREMOOR	cothictive Setuplizatalled Compo	nexts						
Microsoft Windo.	Windows Meil	Microsoft Corporation	e 'sprogram file	/Lism zvobaiwiz				
HELM'SOFTWAREWow	432NodeMicaosof(Active Setup)	installed Components						
📝 😭 Micuosoft Windo.	Windows Meal	Microsoft Corporation	o:/program file	s 0.06/windows				
HKLMGOPTWAREVCISES	er/Paotocols/Philter							
🗹 💿 text/sml	Microsoft Office XML MIME	Maccosoft Corporation	o l'program file	skommon files\				
HELMOOPTWAREVCLass	es/Protocols/Headler							
V 🔬 hislemeaner	Safe Search pluggable protocol	AVG Technologies CZ, s.s.o.	o:\poguem file	e (still)langlang1				
HKLM\Software Microsoft	Windows'CamentVersion/Explored	ShellEnec weHooks	100	1000 CO. 1000				
💟 🚳 Gacove GFS Sts	Microroft ShanPoint Workerps	Microroft Corporation	o:\poguem file	simic scenifi offic				
HELMEIGHPRONWOW6432	Node Watcoood W/Watcoood Work	emon/Erploser@hellEnerwheHook						
Gabowe GPS Str	Macrosoft SheasPoint Worksps	Macrosoft Corporation	e "geogram file	s (x89b/timecabelobt				
HELMWollwage Classes (*	ShellExV.oatertiferv.Haadlers							
Avoyshill Ed.	AVG Shell Extension	AVG Inchaologues C2, 5.1.0.	o typogram file	s USO/lavg'avg1				
WINKAR			e 'speognern fille	Sivian fan af a				
XAA Goowe GP	Maccooolt & Assertown Wooldps	Macrosoft Corporation	o tipeogram hile	Simesaceoff offac				
AWYO PL-11 R-4	ASI/1 02 - 10 Reducering	ANA Technologies (12 and	- Income the	- Collection and a second				
W WE-RARIO	Avo anti familiata	ATG HUMANAGES CA, S.LO.	o . geogram me	s outpening wegt				
W WURAROZ	Minand Class Brief Western	Manage Commission	o geoglam file	swaan wateroz.				
AND GOOVE OF	TEL Content of a second climation of the second sec	and the line for the second second	a - Awedoniu me	s Usergrame@20808t				
THE ADDRESS OF THE OWNER	Minand Class Daist Western	Minera Commission	a lanan file	Anis and all a				
WEI Mill affer and USDOVE OF	Madel/Claused & USD- Center Ohio	and the stand of t	o . program ma	serves almost OELC				
V AND XXX Choose OF	Microsoft ShamPoint Workers	Microsoft Convention	e burger file	a (vA5hoiceanA				
HEI Michman Classel	instantickellEr/ContextMansHan	flag	o . Seriftern me	a concerned adapted				
WirRAR			o honoram file	IIb transformingly				
XXX George OF	Microsoft ShareFrint Wedere	Mission Compation	e 'morrow file	Serie ward offic				
HELM'Sethman Woorfd'C	Node/Classes/Charters/ChallEr/C	atestMean Handleys		Contract Contract				
WaRAR12			o hoogaan file	dation chosent 12				
V XXXX Gaoove GF	Miccosoft ShasePoint Workspe	Microsoft Corporation	o 'spogaom file	s Gellinicuosoft				
HKLMWGoftware Classes D	nes tory Skellen Diag Diop Haadlen							
THE CO. ME. DAD			o 'pagaam file	IIb treachactive's				

- 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





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.

Description	Publisher	Image Path
Microsoft Office IME 2010	Microsoft Corporation	c:\piogiam files\co
Adobe Reader and Acrobat Manager	Adobe Systems Incorporated	c:\piogram files (x2
AVG Tray Monitor	AVG Technologies CZ, s.r.o.	c:\program files (x
Microsoft Office 2010 component	Microsoft Concustion	c \u00fcom files (x2

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.

Autoruns - Sys	internals: www.s	ysinternals.com								
File Entry Op	tions Help									
	×馬									
😫 Wi	nlogon	🔍 Winsi	ock Providers	Print Monitor	rs	😢 LSA Pri	oviders	Vetwork	Providers	📑 Side
Everything	🛛 🖽 Logon	S Explorer	Internet Explorer	🙆 Scheduled Tasks	Services	Drivers	Codecs	Boot Execute	📑 Image Hijacks	🔊 Applnit
Autorun Entry				Description		Publishe	a.	Image Path		
HELMOORTH	PRIMondal Solution	fin month Windows Vanne	Warring Pus							
📝 💽 Adobe A	RM			Adobe Reader and Acrobat I	Manager	(Venified)	Adobe Systems, Inco.	o:\puogram files (x86)\oo	mmon files\adobe\arm\1.0\ad	lobeazm.eze
AVG_II	CAY			AVG Inty Monstor		(Venind	AVG Technologies	o:\puogram tiles (x56)/lav	g'avg10'avgtay.exe	
🔽 🀧 MMRen	underService			MindManager Topic Alerts		(Venfied) Mindjet		o : lpuogram files (1860) mindje timindmenager Ammeminderservice.exe		ninderservice.exe
V 🛃 Sullava	UpdateSched			Java(TDD Update Scheduler		(Venified)	un Microsystems, I.	c:\puppeam files(x86)loo	mmon filesljavaljava updatel	jusched.exe
C:\Users\youngh	AppData Roaming	fic sosoft/Windows/Start	Menu\Piograms\Startup			1	A .			
V 12 Dropbon	lak			Daplac -		Venfied	Duomone	o vusers wounghulapadate	aluoaming/duopbost/bia/duopbo	00.e30e
V 🕅 Evenote	Clipper lak			Evenue Clipper Of ot verified) Evenue		fiel) Evenote Corp.,	ap., c.\putgram files (x86)/evenote/evenote/evenoteclipper.exe		per.exe	
HKCU Software	Microsoft/Windows/C	upentVersion\Run								
V (Despot				The utity for vitual deskto	ps	(Tot veni	fiel) Despot GbR	o:\pu <mark>n</mark> gram files (x86)\de	xpot\dexpot.exe	
V Ditto				Ditto				c:\putgram files (x86)\dit	tto/ditto.exe	
Google 1	Jpdate			Google 安朝程式		(Venfied)	Google Inc	o:husuchusungh lappdate	allocal/google/update/google	update.exe
HKCU'Software	Microsoft Windows VC	uzentVezzion\RunOnce								
V m FlashPla	verUpdate			Adobe® Flash® Player Inst	alley/Uninstaller 10.3 r18	1 (Venified)	Adobe Systems Incor.	c:\windows\syswow64hm	acuomed/dash/dashutil10t_ac	tivez.exe
1										

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 是一款可撷取通過網路卡之 TCP/IP 封包的免費軟體,並可讓 您檢視所撷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 : <u>http://www.nirsoft.net/utils/smsniff.zip</u>

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)

Alffzip - WinRAR (译信版)								
, 浩令(C) 工具(S) 共的最新(O) 編項(N) 批問(H)	11. ///		() · · · · · · · · · · · · · · · · · · ·	質 → asocpc01 → 展園 →		•	** 244 42	
Y 🛃 📓 🖾 🔰 🗰 🥻 👘 🖡	b 🗹 📆			電子影件 烧烧 新增管科夫				H • 0
新星級到 消費 预况 刑律 等效 检查 算时 107	四 紅柳 日祭		A some		修改日期	#11	大小	
amsortf.per-ZIP 星相相, 未對転大小112,915 但元祖			A MADRINE	PC-03	2011/7/6 上年 09	推信	2 K8	
	大小	封碳後 護型		Privilege.dat	2011/7/30 上午 1	DAT 植紫	0 KB	
		Folder		ProcessExplorer.zip	2011/9/28 上午 0	WinRAR ZIP 整個權	1,803 KB	
dme.txt	21,413	7,349 Text Document		smsniff (1).zip	2011/10/13下午	WinRAR ZIP 聖婦權	84 KB	
uniff.chm	19,310	11,346 Compiled HTML .	10 10 00 00 00 00 00 00 00 00 00 00 00 0	smeniff (2) zip	2011/10/13 下午	WinRAR ZIP 聖頭標	84 KB	
oniff.exe	72,192	66,471 Application		(smsniff.zip)	2011/10/13 下午	WinRAR ZIP 整线相	84 K8	
			P THEFT (C)	SOP_Ver0.6.docx	2011/10/13 下午	Microsoft Word	2,919 KB	
				TANet要買IPq_Day_09-22-2011-00-03	2011/9/24 下半 0	Adobe Acrobat	14 KB	
				TANet要同IPq_Day_09-24-2011-00-03	2011/9/24 上半 1	Adobe Acrobat	14 KB	
			ge prostasor snare ((/192.108.1.103) (2	en topdump.doc	2011/8/16 下午 0	Microsoft Word	47 88	
				Tcpvcon.exe	2010/7/28 下午 0	原用程式	195 KB	
		更新保定。 ● 解型論 ● 解型論 ● 雇更新 夜站秋次 ● 夜寫約	並 教行相葉(G)	E				
		 不用確 	記載覆寫(W) 由 I DVD RW 磁碟	料構 (圧)				
網共 112,91	5 位元組, 共計 3 個檔案	0 9980	総存在的編集(5) ● 抽取式段研 (5) ● 抽取式段研 (5)	F) we 0492168110				
	X	X	1 Star 10 10					
	Han Han	HEAL HEAL	albert					
1965 (2019) oppet 6906/1979 kadalari zancipila (797	SEALER NUMBER B		電車至于習料天(L) Automas Matematican					
1921. (1) das 1921 (2) (1)	1998. 1	1989年1月1日 日本国家	Mactee (P管職示編案(X) 田一 Mactee					
	a) 🛎 🗎	w)	(第年設定(V) / 「」」					
IC MUSEC MUSIC, MEETING GROUPER Annapple lage	400 - 4/10/2020 H	Electron + s	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	na Ng				
9+0528/2541. (10940)								

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

💐 Smar	tSniff							_ 0	×
<u>Eile E</u> di	t <u>V</u> iew <u>O</u> pti	ons <u>H</u> elp							
	17 🔺 🛙) 🖬 Þa 😭	-71						
I 🛆	Protocol	Local Address	Remote Address	Local Port	Remot	Service Name	Packets	Data Size	
@ 24	TCP	192.168.0.5	66.218.71.233	1084	80	http	44	36,592 Byt	:е
0 25	TCP	192.168.0.5	212.199.29.6	1085	80	http	26	11,532 Byt	:е
@ 26	TCP	192.168.0.5	212.199.29.13	1086	80	http	4	1,221 Byte	s
0 27	TCP	192.168.0.5	212.199.29.6	1087	80	http	10	7,257 Byte	is 🔤
28	TCP	192.168.0.5	216.136.131.30	1088	80	http	6	826 Bytes	Ţ
•								•	
GET /p	a?q=nirs	oft&s=27666	79 HTTP/1.1						
Accept Refere Accept User-A Host: Connec HTTP/1 Date: P3P: n	GET /pa?q=nirsoft&s=2766679 HTTP/1.1 Accept: */* Referer: http://search.yahoo.com/search?p=nirsoft&ei=UTF-8&fr=fp-tab-web-t&cop= Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: pa.yahoo.com Connection: Keep-Alive HTTP/1.0 200 OK Date: Wed, 30 Jun 2004 08:37:19 GMT								
Parts p	Contucle	= nccp://p3	p.yanuo.com/	мас∕рзр.	хш⊥~, СР	.= CHO D26	CON COR	HUM DEV	الح
28 TCP/IP	conversations	s, 1 Selected							

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
ξ擊來源IP	au 124 37 131	攻擊來源 PORT 63230
目標IP	180.20 114.0	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

🐯 SmartSniff	24	1311	THE REAL	1 The 100			23
<u>File Edit View Options Help</u>	2						
🕨 = 🗉 💙 🛓 🗋 🖬 🗈	🕆 📲						
Index Pr Local Address	Remote Address	Local Port	Remot / Local Host	Remote Host	Service Name	Packets	-
@ 17 TCP 192.168.1.100	64.233.183.100	21346	80		http	29	
@ 19 TCP 192.168.1.100	64.233.183.120	21348	80		http	9	
@ 20 TCP 192.168.1.100	64.233.183.120	21349	80		http	9	
© 21 TCP 192.168.1.100	64.233.183.120	21350	80		http	58	
36 TCP 192.168.1.100	72.14.203.138	21351	80		http	12	
@ 37 TCP 192.168.1.100	64.233.183.101	21352	80		http	16	
@ 38 TCP 192.168.1.100	64.233.183.100	21353	80		http	17	
③ 39 TCP 192.168.1.100	64.233.183.101	21354	80		http	13	
@ 40 TCP 192.168.1.100	64.233.183.101	21355	80		http	12	-
•	III						
GET /news/ton/yr/dL023ns Host: nt2.ggpht.com Connection: keep-alive User-Agent: Mozilla/5.0 (Accept: */* Referer: http://news.goog	(Windows NT 6.1; WOW64 gle.com.tw/nwshp?hl=zh) AppleWebKit/5 -TW&tab=wn	35.1 (KHTML, like Gecko) Chrome/14.	<mark>0.835.202</mark> Safa	r <mark>i/535.1</mark>	- m
Accept-Encoding: gzip,de	Flate,sdch						
Accept-Language: zh-TW,zl	n;q=0.8,en-US;q=0.6,en	;q=0.4					
Accept-Charset: Big5,utf-	-8;q=0.7,*;q=0.3						
GET /news/tbn/qkVHYrbagil	oZWM/2.jpg HTTP/1.1						+
4376 TCP/IP conversations, 1 Select	ed						

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

Sma	rtSniff	f						
-	it)	√iew <u>O</u> ptions <u>H</u> elp						
		V 🛦 🗋 🖬 🗗 🖪						
dex	Pr	Local Address	Remote Address	Local Port	Remot / Local Host	Remote Host	Service Name	Packets
1	TCP	192.168.1.100	66.220.151.86	26480	80		http	1
2	TCP	192.168.1.100	66.220.151.86	26966	80		http	1
3	TCP	192.168.1.100	66.220.151.86	26992	80		http	1
4	TCP	192.168.1.100	69.171.229.13	26092	80		http	3
_			m					
_								

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

apture Filter		-	23
Type one or more filter strin examples for filter strings:	ngs, separated by sp	aces or enter keys. H	ere's some
include:remote:tcp:80 include:both:udp:53-139 exclude:both:tcpudp:192.1	68.0.1-192.168.0.10	00	
include:remote:tcp:63230			
			-

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

File E	dit	View Options Help					
> =	-	7 🔺 🗋 🖬 🖬	7 - 71				
Index	Pr	Local Address	Remote	e Address	Local Port	Remote P	ort
01	TCP	192 168 1 100	66.220	151.86	26480	80	
© 2							
<u>ې</u> 3							
≥ 4	TCP		69.171	229.13	26092	80	
5			38	HTML Report	rt - TCP/IP Streams		
9	TCP	192.168.1.100	38	Expon TCP/I	P Streams	Cui+E	
10	TCP	192.168.1.100	20	Save Packet	Summaries		
© 11	TCP	192.168.1.100	20	IRNIetInfo		Ctrl+I	
12	TCP	192.168.1.100	72				
13	TCP	192.168.1.100	38	Choose Colu	umns		
© 14	ТСР	192.168.1.100	72	Auto Size Co	olumns	Ctrl+Plus	
<		III		Select All		Ctrl+A	+
				Deselect All		Ctrl+D	
				Сору		Ctrl+C	I .
				Move Next		F8	1
				Move Previo	ous	F7	

合管理 ▼ 新博客	料本				8== •	6
	× ∠≅ ^	修改日期	5百开)	大 山		
(我的最愛		INF WALLEY FILS	28.00			
🗼 下載	🍌 cycgame	2011/9/12下午 0	檔案資料夾			
三 桌面	HP LJ4200-4300 Series PCL5 Driver	2011/7/21下午 0	福富資料夾			
🔠 最近的位置	🗉 🍶 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			
媒體櫃	Program Files (x86)	2011/8/12 上午 1	福宾资料夾			
2 文件	📕 🔒 TeamViewerPortable	2011/7/7 上午 07	福案資料夾			
♪ 音楽	🎍 Windows	2011/8/25下午 0	檔案資料夾			
副規範	🍶 使用者	2011/6/28 上午 1	福宾資料夾			
	🍶 新増資料夾	2011/7/29下午1	檔案資料夾			
電腦						
本機磁碟 (C:)						
cycgame						
檔案名稱(N): pa	cket					
存檔類型(T): Tex	d Files (*.txt)					

🥘 packet.txt - 記事本		×
檔案(F) 編輯(E) 格式(O)	檢視(V) 說明(H)	
Index : Protocol : Local Address : Remote Address : Remote Port : Local Port : Local Fort : Local Host : Service Name : Packets : Data Size : Total Size : Data Size : Capture Time : Local MAC Address : Local MAC Address : Remote MAC Address : Cacal IP Country : Remote IP Country :	1 TCP 192.168.1.100 66.220.151.86 26480 80 http 14 8.878 Bytes 10.651 Bytes 0.0 KB/Sec 2011/10/14 上午 02:51:01:625 2011/10/14 上午 02:54:46:504 00:03:44.878	
Index : Protocol : Local Address : Remote Address : Local Port : Local Host : Remote Host : Service Name : Packets : Data Size : Data Size : Data Size : Last Packet Time : Local MAC Address : Remote MAC Address : Local IP Country :	2 TCP 192.168.1.100 66.220.151.86 26966 80 http 14 8,862 Bytes 10,633 Bytes 0.0 KB/Sec 2011/10/14 上午 02:51:01:626 2011/10/14 上午 02:54:46:504 00:03:44.877	*

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」。

VT Community Sign in	•			Languages
	VIRUS FOTAL	Virusto files a of virus detect	otal is a service tha and URLs and facili ses, worms, trojans, ed by antivirus engin	at analyzes suspicious tates the quick detection and all kinds of malware nes. More information
Analysis	Search Stats	Advanced	VT Community	FAQ About VT
Upload a file	Submit a URL	-		
l f yo) 選擇檔 bu wish, you can also (2 素選擇檔案 Send it ove Send files via er Maximum file s	r SSL 0 le e e e e e e e e e e e e e e e e e e	Service load

VirusTotal © Hispasec Sistemas - Delog - F Twitter - Contact: info@virustotal.com - TOS & Privacy Policy

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

VT Community Sign in V

Languages V



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. <u>More information...</u>

File name: op0722.ra Submission date: 2011-10-1 Current status: analysing	r 4 01:27:37 (UTC) 檔案分析		not reviewed Safety score: - 分析結果
Antivirus	Version	Last Update	Result
AhnLab-V3 分	2011.10.13.00	2011.10.13	
DrWeb 析	5.0.2.03300	2011.10.12	-
Emsisoft 的	5.1.0.11	2011.10.13	
3Data 病	22	2011.10.13	-
IcAfee -	5.400.0.1158	2011.10.13	
AcAfee-GW-Edition 5	2010.1D	2011.10.13	-
SUPERAntiSpyware 🕸	4.40.0.1006	2011.10.13	
7BA32	3.12.16.4	2011.10.13	-
Additional information			Show a

SHA256: 6b7ef27c446f01db0a0714f64f5e95e38892fb0b256dfa6c9325cfc3fb35726f

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。



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 us Community user(s	ser(s) with a total of 0 reputation credit(s) say(s) this) with a total of 0 reputation credit(s) say(s) this sam	sample is goodware. 0 VT ple is malware.	VT Community
File name: Submission date: Current status: Result:	op0722.rar 2011-10-14 01:27:37 (UTC) finished 0/ 37 (0.0%) 47個病毒掃描 沒有任何1個弓	引 擎掃 描的結果 擎判斷該檔案有問	not reviewed Safety score: -
P Compact			Print results
Antivirus	Version	Last Update	Result
AhnLab-V3	2011.10.13.00	2011.10.13	a
AntiVir	7.11.15.252	2011.10.13	-
Antiy-AVL	2.0.3.7	2011.10.13	a .
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	15-11
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	5
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。



Clean site

Websense ThreatSeeker