

第十四章

木馬與後門程式

木馬與後門

- 木馬程式(trojan)及後門程式(backdoor)是攻擊者獲得目標系統存取權限的兩個方法，他們的樣貌多變，但是都有一個共同的特徵，就是必須藉由其他的程式或者是以欺騙的手法安裝到目標系統上。

後門程式

- 後門是指一種繞過安全性控制，以獲取對程式或系統訪問權的方法。
- 在軟體的開發階段，程式師常會在軟體內創建後門以便可以修改程式中的缺陷。
- 這裡敘述的後門，則是指駭客入侵系統後，預留將來的進入通道。

後門程式

- 後門程式必須是作業系統中正在服務的程式，因此通常都會偽裝成一個熟知的服務名稱，或者是一個沒有啟動的服務，讓一般使用者不容易發現有異常的程序在運作中。

木馬程式

- 特洛伊木馬程式或簡稱木馬程式，是一個小的電腦程式，偽裝成某種有用的或有趣的程式，吸引受害者去下載及安裝使用，但是實際上卻包藏禍心，暗地裡做壞事。
- 特洛伊木馬不會自我複製，也不會主動散播到別的電腦裡面。

木馬程式傳播方式

(1)立即訊息的附件。

(2)IRC(Internet Relay Chat)。

(3)電子郵件附加檔案。

(4)網路芳鄰檔案分享。

木馬家族

- 遠端管理木馬(Remote Administration Trojans)
- 資料傳送木馬(Data-Sending Trojans)
- 破壞木馬(Destructive Trojans)
- 阻斷服務攻擊木馬(DoS Attack Trojans)
- 代理木馬(Proxy Trojans)
- 檔案傳輸木馬(FTP Trojans)
- 關閉安全軟體木馬(Security Software Disablers)

木馬屠城的管道

- ICQ。
- IRC。
- 附件。
- 實體的存取。
- 瀏覽器或郵寄軟體的臭蟲(Bug)。
- NetBIOS (檔案分享)。
- 冒牌(Fake)程式。
- 不可信任的網站及免費軟體(例如：Foxy)。
- 從網際網路的網站下載檔案、遊戲、螢幕保護。
- 來自於不滿員工的壓縮(shrink-wrapped)軟體包。

木馬入侵的徵兆

- 光碟托盤(drawer)自動打開或關閉。
- 電腦畫面上下翻轉或反白。
- 壁紙(Wallpaper) 或背景設定自動改變。
- 印表機自動列印文件或訊息。
- 瀏覽器自動前往奇怪或未知的網頁。
- Windows 視窗顏色自動改變。
- 螢幕保護設定自動改變。

木馬入侵的徵兆

- 滑鼠左右鍵功能自動對調。
- 滑鼠指標消失。
- 滑鼠指標自己移動。
- Windows Start 按鈕消失。
- 奇怪的聊天視窗出現，並且強迫與陌生人交談。
- ISP 指控受害者電腦在做 IP 掃描。
- 某人對受害者了解太多關於其電腦的個人資料。

木馬入侵的徵兆

- 電腦自己關機。
- 工作列(Taskbar) 消失。
- 帳號密碼被改變。
- 信用卡購買結帳單出現奇怪的項目。
- 電腦螢幕自動開關。
- 數據機自動撥號及連接到網際網路。
- Ctrl+Alt+Del 無法工作。
- 當要重新開機，作業系統卻有訊息顯示有其他使用者仍然連線中。

常見的木馬程式

木馬程式	協定	Ports
Back Orifice	UDP	31337 或 31338
Deep Throat	UDP	2140 及 3150
NetBus	TCP	12345 及 12346
Whack-a-mole	TCP	12361 及 12362
NetBus 2 Pro	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423 及 40426

包裹程式

- 攻擊者怎麼讓受害者的電腦安裝任何的木馬程式？
- 其中的一種方法就是使用包裹程式 (wrappers) ，包裹程式又稱捆綁程式 (Binders) 。
- 一個包裹程式可以將一個指定的應用軟體執行檔 (EXE) ，與木馬程式打包成一個單一的執行檔。通常這個執行檔會是令人忍不住執行的。

包裹程式



CHESSEX

+



Trojan



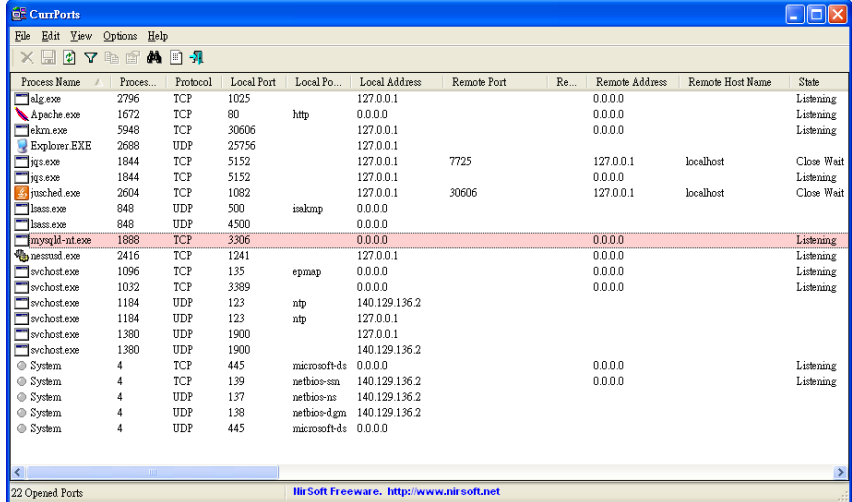
對策

- 使用工具掃描及檢查開啟的可疑 port 。
- 使用工具掃描執行中的程序。
- 使用工具檢查可疑機碼項目。
- 使用工具掃描可疑的網路活動。
- 安裝防木馬軟體。
- 系統檔案核對。
- 避執行木馬程式。

工具程式

■ Currport

- 可以即時的顯示出電腦上的使用狀況，例如程式位置、連接埠、IP 位址...等資料。
 - 如果發現異常的連線，還可以將異常連線中斷。



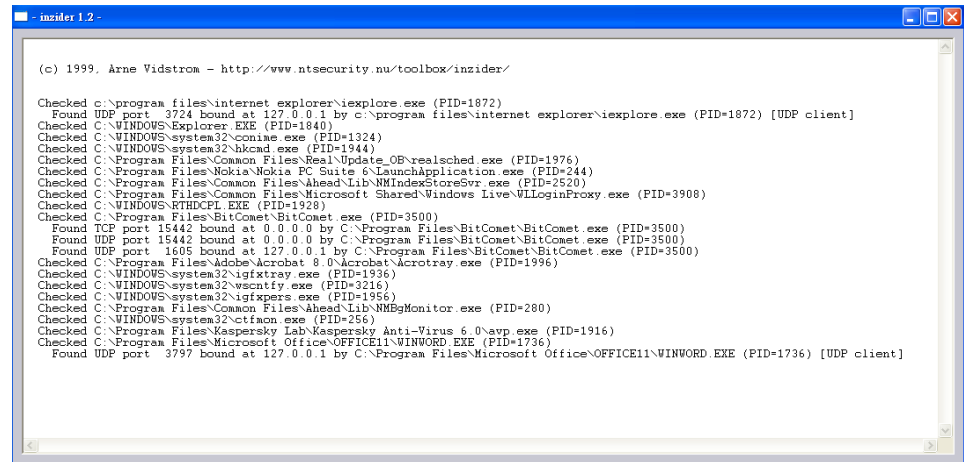
The screenshot shows the CurrPorts application window with a table of open ports. The table has columns for Process Name, Process ID, Protocol, Local Port, Local Port Name, Local Address, Remote Port, Remote Address, Remote Host Name, and State. The status bar at the bottom indicates '22 Opened Ports' and provides a website link: 'NirSoft Freeware, <http://www.nirsoft.net>'.

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Address	Remote Host Name	State
alg.exe	2796	TCP	1025		127.0.0.1		0.0.0.0		Listening
Apache.exe	1672	TCP	80	http	0.0.0.0		0.0.0.0		Listening
ekm.exe	5948	TCP	30606		127.0.0.1		0.0.0.0		Listening
Explorer.EXE	2688	UDP	25756		127.0.0.1				
igmp.exe	1844	TCP	5152		127.0.0.1	7725	127.0.0.1	localhost	Close Wait
igmp.exe	1844	TCP	5152		127.0.0.1		0.0.0.0		Listening
msched.exe	2604	TCP	1082		127.0.0.1	30606	127.0.0.1	localhost	Close Wait
lsass.exe	848	UDP	500	isakmp	0.0.0.0				
lsass.exe	848	UDP	4500		0.0.0.0				
mysql-nt.exe	1888	TCP	3306		0.0.0.0		0.0.0.0		Listening
netssnd.exe	2416	TCP	1241		127.0.0.1		0.0.0.0		Listening
svchost.exe	1096	TCP	135	epmap	0.0.0.0		0.0.0.0		Listening
svchost.exe	1032	TCP	3389		0.0.0.0		0.0.0.0		Listening
svchost.exe	1184	UDP	123	ntp	140.129.136.2				
svchost.exe	1184	UDP	123	ntp	127.0.0.1				
svchost.exe	1380	UDP	1900		127.0.0.1				
svchost.exe	1380	UDP	1900		140.129.136.2				
System	4	TCP	445	microsoft-ds	0.0.0.0		0.0.0.0		Listening
System	4	TCP	139	netbios-ssn	140.129.136.2				
System	4	UDP	137	netbios-ns	140.129.136.2				
System	4	UDP	138	netbios-dgm	140.129.136.2				
System	4	UDP	445	microsoft-ds	0.0.0.0				

工具程式

■ Inzider

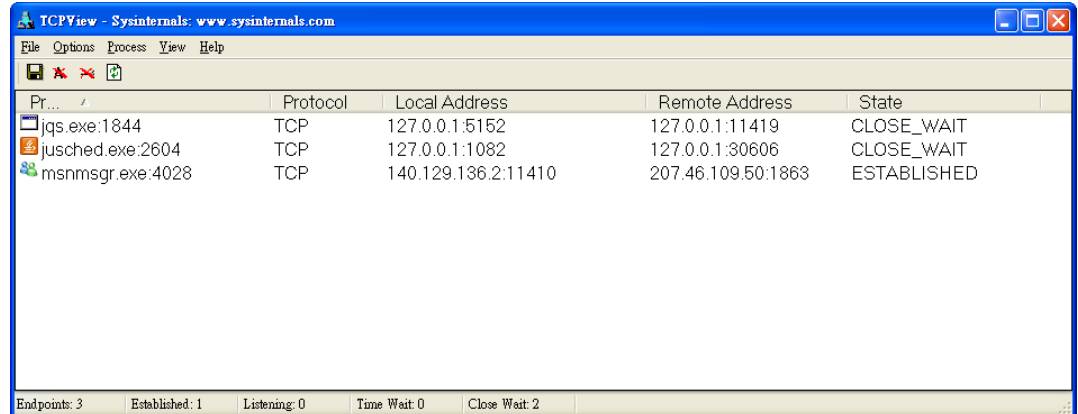
- 能列出並追蹤程序及 Port，支援 Windows 95 / 98 / ME / NT 4.0 / 2000 / XP / 2003。



```
- inzider 1.2 -  
  
(c) 1999. Arne Vidstrom - http://www.ntsecurity.nu/toolbox/inzider/  
  
Checked c:\program files\internet explorer\iexplore.exe (PID=1872)  
  Found UDP port 3724 bound at 127.0.0.1 by c:\program files\internet explorer\iexplore.exe (PID=1872) [UDP client]  
Checked C:\WINDOWS\Explorer.EXE (PID=1840)  
Checked C:\WINDOWS\system32\conime.exe (PID=1324)  
Checked C:\WINDOWS\system32\hccad.exe (PID=1944)  
Checked C:\Program Files\Common Files\Real\Update_OB\realsched.exe (PID=1976)  
Checked C:\Program Files\Nokia\Nokia PC Suite 6\LaunchApplication.exe (PID=244)  
Checked C:\Program Files\Common Files\Ahead\Lib\NMIndexStoreSvr.exe (PID=2520)  
Checked C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLLoginProxy.exe (PID=3908)  
Checked C:\WINDOWS\RTHDPL.EXE (PID=1928)  
Checked C:\Program Files\BitComet\BitComet.exe (PID=3500)  
  Found TCP port 15442 bound at 0.0.0.0 by C:\Program Files\BitComet\BitComet.exe (PID=3500)  
  Found UDP port 15442 bound at 0.0.0.0 by C:\Program Files\BitComet\BitComet.exe (PID=3500)  
  Found UDP port 1605 bound at 127.0.0.1 by C:\Program Files\BitComet\BitComet.exe (PID=3500)  
Checked C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrotray.exe (PID=1996)  
Checked C:\WINDOWS\system32\igfxtray.exe (PID=1936)  
Checked C:\WINDOWS\system32\wscntfy.exe (PID=2916)  
Checked C:\WINDOWS\system32\igfxpers.exe (PID=1956)  
Checked C:\Program Files\Common Files\Ahead\Lib\NMBgMonitor.exe (PID=280)  
Checked C:\WINDOWS\system32\ctfaon.exe (PID=256)  
Checked C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0\avp.exe (PID=1916)  
Checked C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE (PID=1736)  
  Found UDP port 3797 bound at 127.0.0.1 by C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE (PID=1736) [UDP client]
```

TCPView

- 此軟體本為 sysinternals 網站所有，但已被微軟買走。TCPView 可即時的檢查及觀看 TCP 及 UDP 的流量狀態，也包含了本地或遠端的 TCP 連線之位址，同時還可以檢視目前正在電腦上執行的程序以及擁有者。



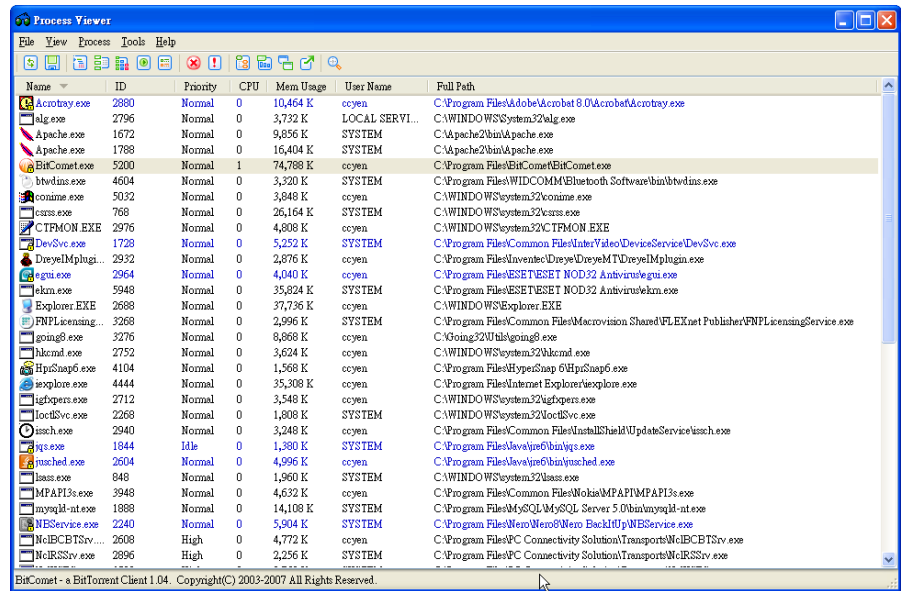
The screenshot shows the TCPView application window with the following data:

Pr...	Protocol	Local Address	Remote Address	State
iqs.exe:1844	TCP	127.0.0.1:5152	127.0.0.1:11419	CLOSE_WAIT
jusched.exe:2604	TCP	127.0.0.1:1082	127.0.0.1:30606	CLOSE_WAIT
msnmsgr.exe:4028	TCP	140.129.136.2:11410	207.46.109.50:1863	ESTABLISHED

At the bottom of the window, the status bar shows: Endpoints: 3 | Established: 1 | Listening: 0 | Time Wait: 0 | Close Wait: 2

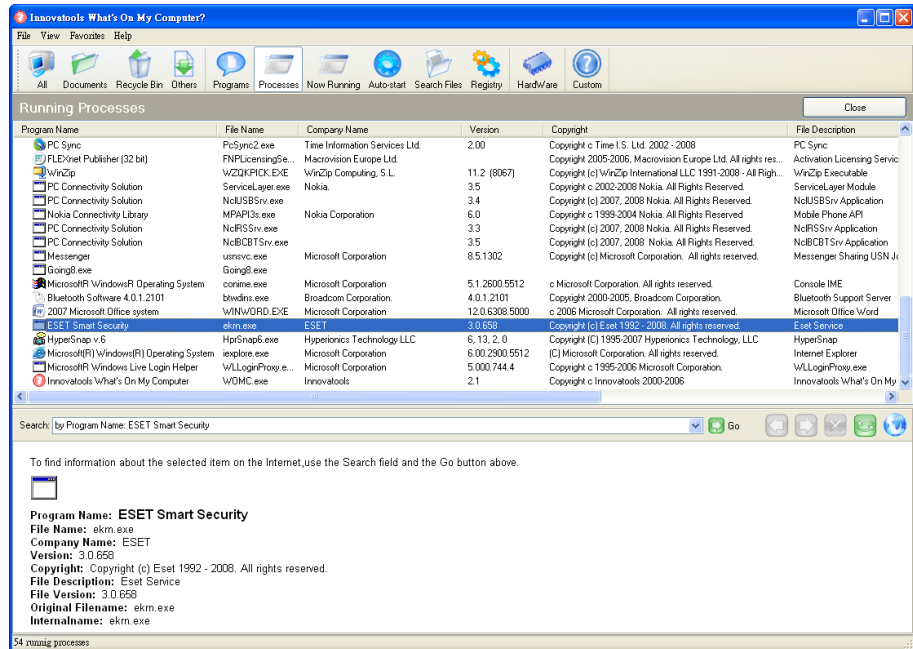
Process Viewer

- Process Viewer 是一個程序檢視工具，顯示處理程序的詳細路徑與版本資訊及顯示使用的記憶體...等資訊，此外也允許結束程序或設定程序的優先權。



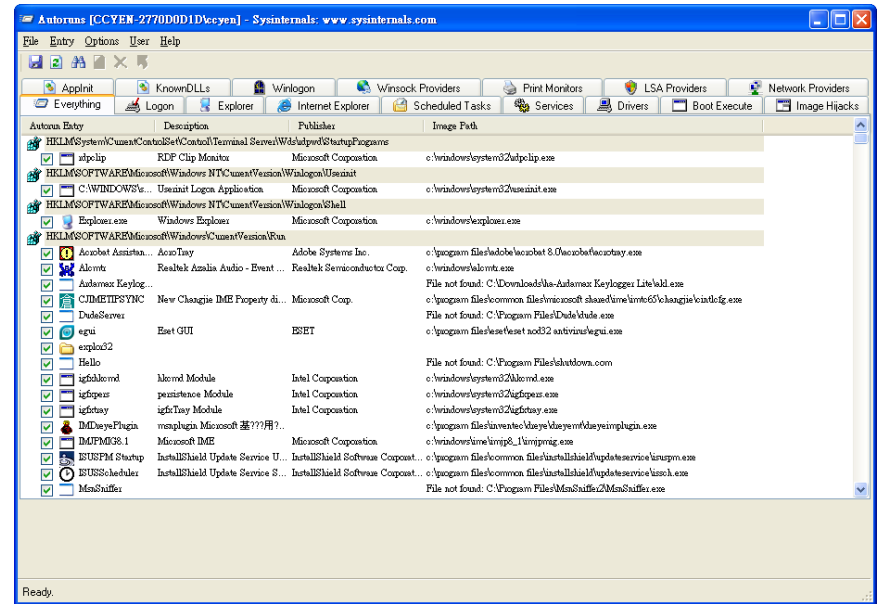
What on my computer

- 對系統中所安裝的程式、檔案，都可以顯示出來，且會自動連上網路蒐集相關的訊息。



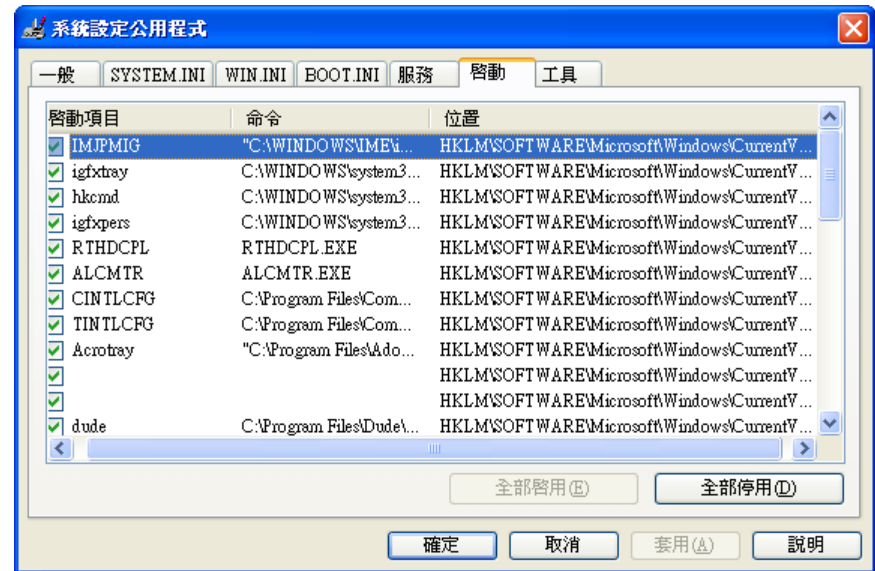
AutoRuns

- 此公用程式顯示設定在系統開機或登入期間所執行的程式，這些程式包含啟動資料夾、Run、RunOnce和其他登錄機碼中的程式。



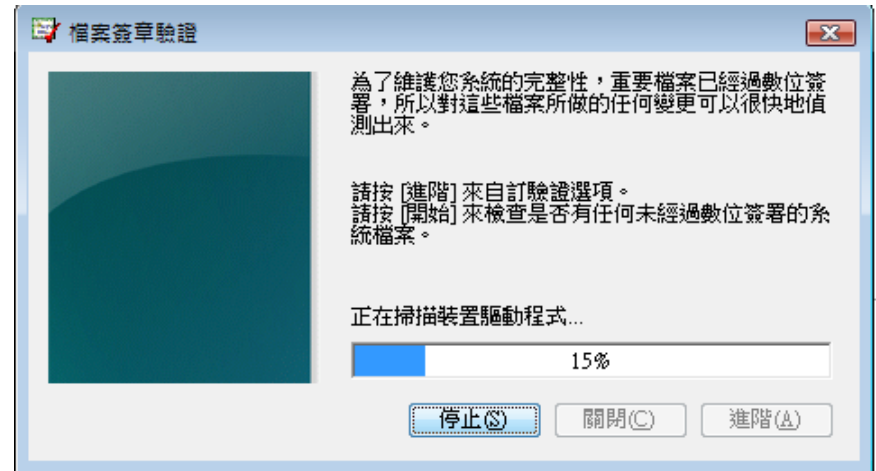
MSConfig

- 可以用以下方式開啟隱藏的功能，選擇「開啟」→「執行」→輸入「msconfig」→「確定」→選擇「啟動」頁籤，這裡可看到系統啟動時會自動執行的機碼。



簽署檔

- 所謂「簽署檔」，就是被授予以 Microsoft 數位簽署的檔。該簽署可證明該檔案是與原始檔一模一樣的副本。
- 通過 Microsoft 簽字驗證工具，我們可在電腦上找出已簽署和未簽署的檔案，也可查看簽署檔的身份驗證，以確認該檔還沒有被篡改。

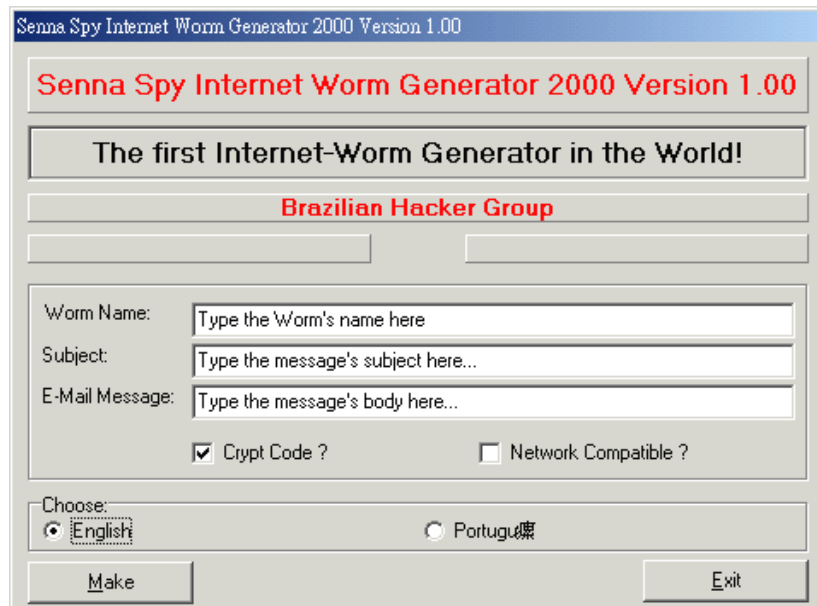


新的木馬程式

- 木馬功能會越來越強，體積也越來越小，佔用的記憶體也很像一般的process，同時會取個名稱像是kernel32.exe的名字讓管理者困惑。木馬程式會複製執行檔到系統目錄或是特定目錄下，以增加下次開機存活機會。
- 木馬程式開啟的port會使用後面的port (接近65536)，因為若要檢測全部的port要花很長的時間，這樣木馬程式就可以規避偵測。新的木馬client與server的連線彼此採取加密的措施，確保連線過程的資料不被竊取。
- 新的木馬會隱藏在DLL檔裡面，擺脫了傳統木馬開啟port監聽的技術，而採用改寫DLL(動態連結函式庫)或驅動程序的方式，這樣一來系統既沒有產生新的文件，一切的服務也照常運作，更沒有多的port開啟。

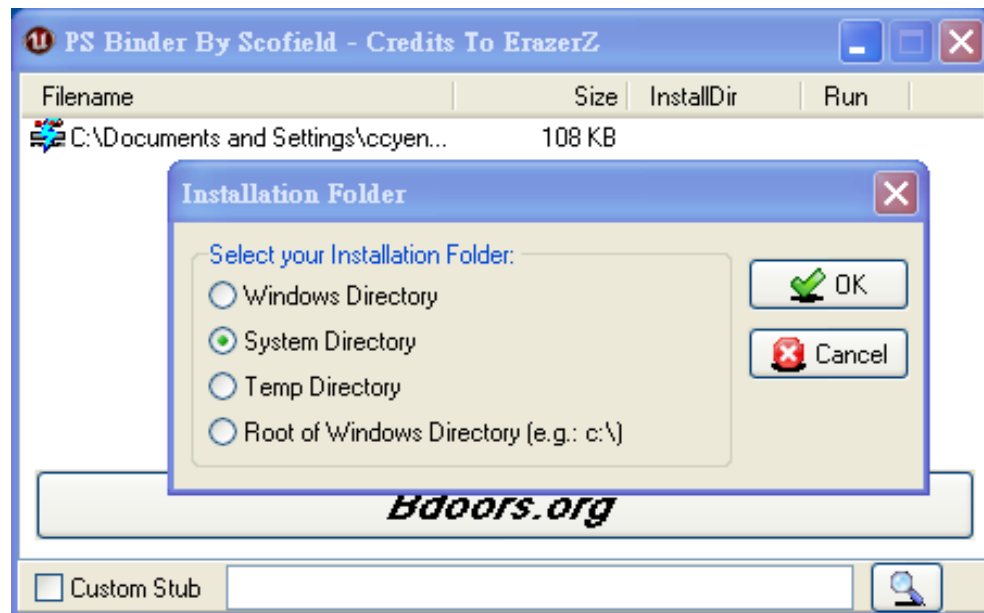
Senna Spy

- 是木馬產生器，可以產生具有新功能的 Visual Basic 木馬程式原始碼，所以任何人都可以修改其程式碼。

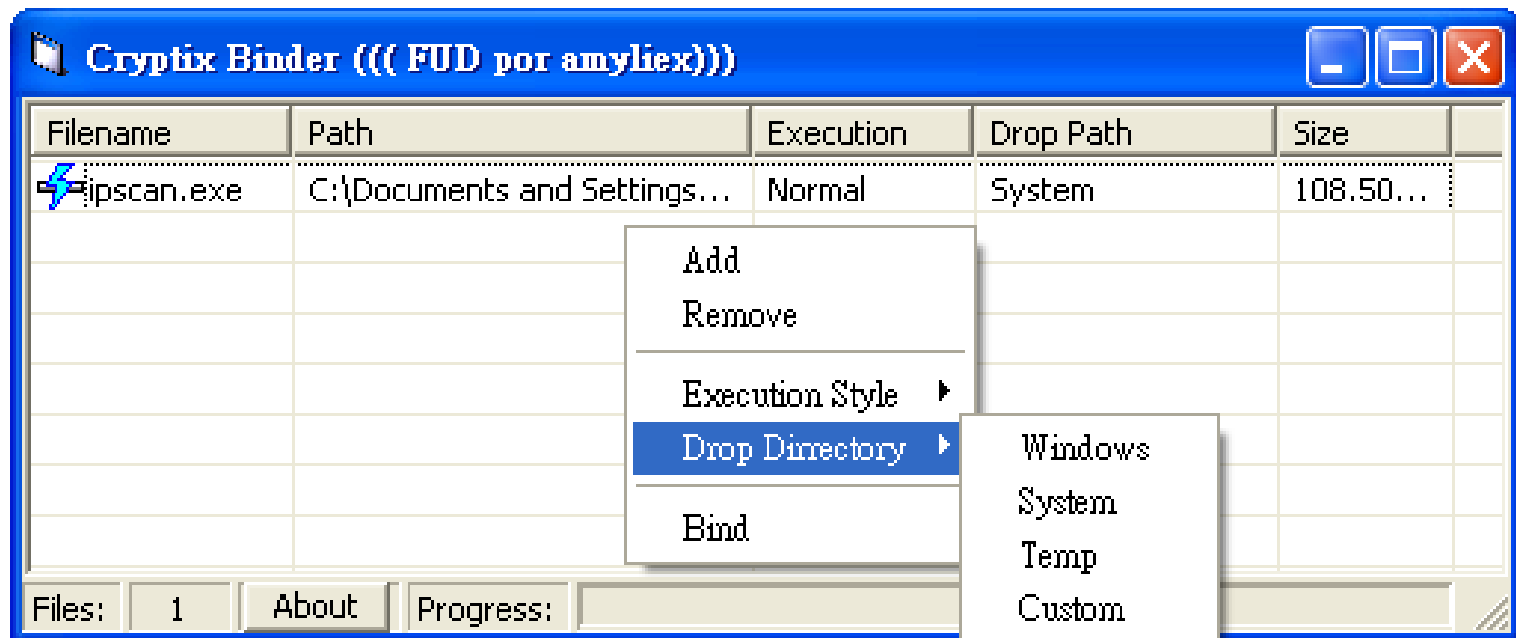


PSBinder

- 可包裹檔案並放在指定的路徑下，並能夠自動執行指定的程式。

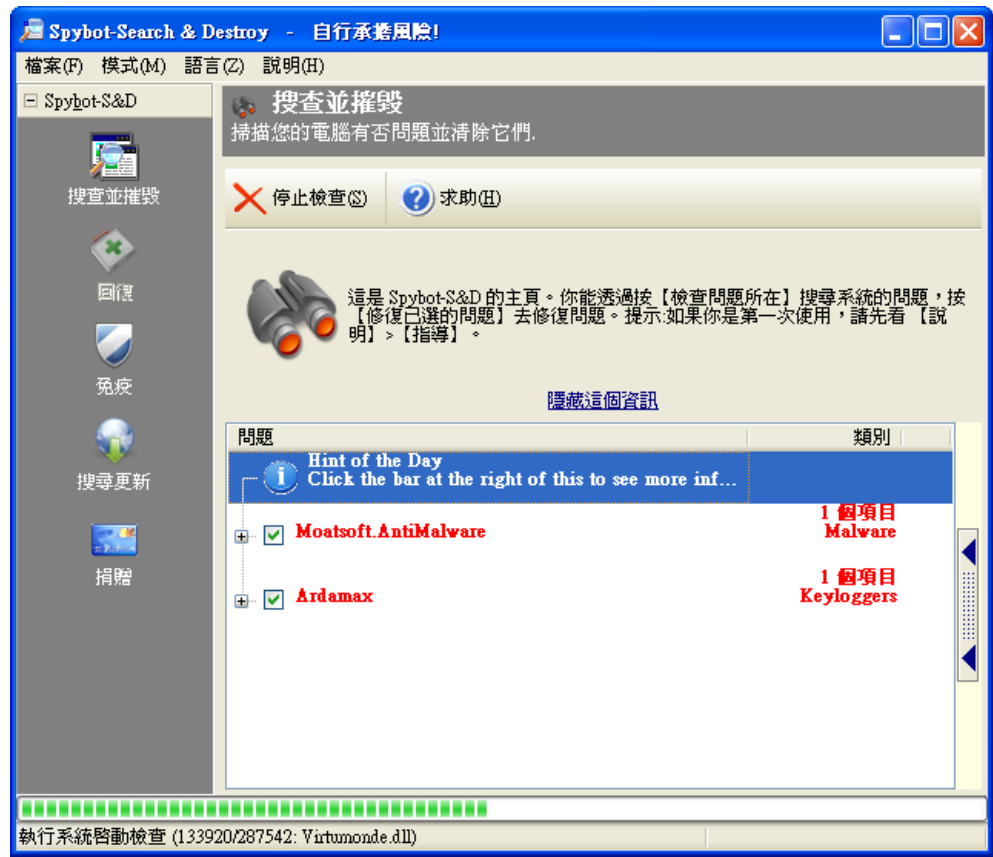


Cryptix Binder



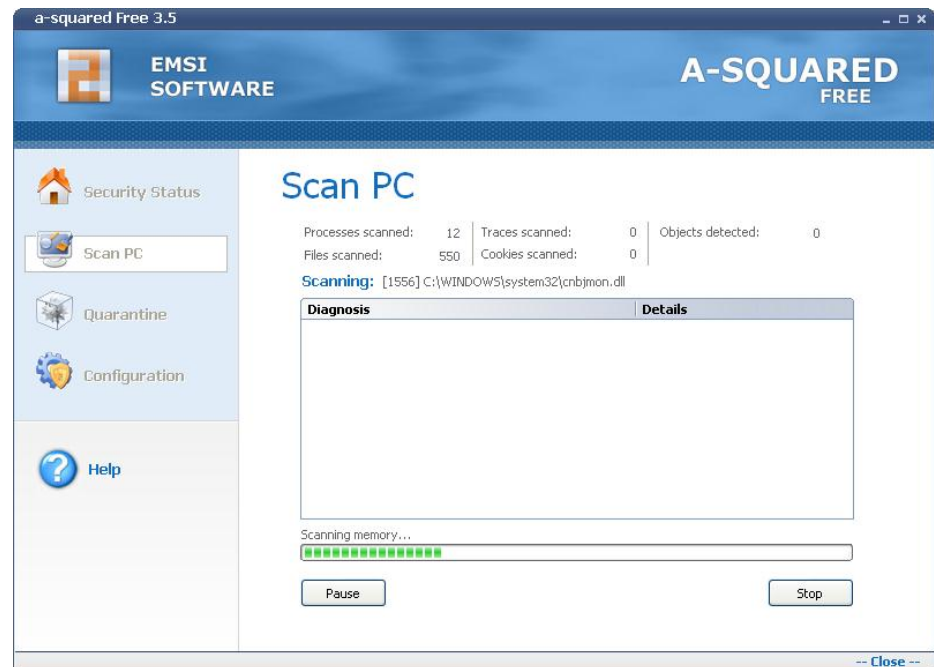
SpyBot Search & Destroy

- 掃瞄及清除木馬的軟體。



A-Squared Free

- a-squared Free 是一個專門掃描木馬程式、後門軟體的免費軟體，不具有常駐、及時掃描的功能，所以非常省資源。可對單檔案進行掃描。



AVG Free Edition

AVG Anti-Virus Free Edition

File Components History Tools Help

You are protected.
All security features are working correctly and are up to date.

Scan is running

File	Result/Infection
C:\Documents and Settings\ccyen\桌面\HyperSnap 6.31.01\HprRes...	Trojan horse Generic11.GKZ
C:\Documents and Settings\ccyen\桌面\HyperSnap 6.31.01\HprSna...	Trojan horse Generic11.GKZ
HKLM\SOFTWARE\Classes\Interface\{7529153F-4EA9-4C50-830A-7...	Found Adware.CoolWebSearch
HKLM\SOFTWARE\KMINT21	Found Adware.DesktopSpyAgent
HKU\5-1-5-21-1606980848-1284227242-725345543-1003\Software\...	Found Adware.DesktopSpyAgent

Objects scanned: 468322
Threats found: 2
Elapsed time: 1 minute(s) 42 second(s)
Currently scanning: File system
Current object: C:\cygwin\bin\echo.exe

Additional scan settings ...

Fast scan | Pause | Cancel

Statistics
Last scan: Not yet scanned
Last update: 08/9/30, 下午 09:00
Virus DB: 270.7.5/1698
AVG version: 8.0.169
License type: Free

Show notification

AD-Aware 2008 Free

- Ad-Aware SE Personal 結合了後門程式掃描與個人隱私記錄、反追蹤移除等功能的免費軟體，可以線上更新掃描檔。



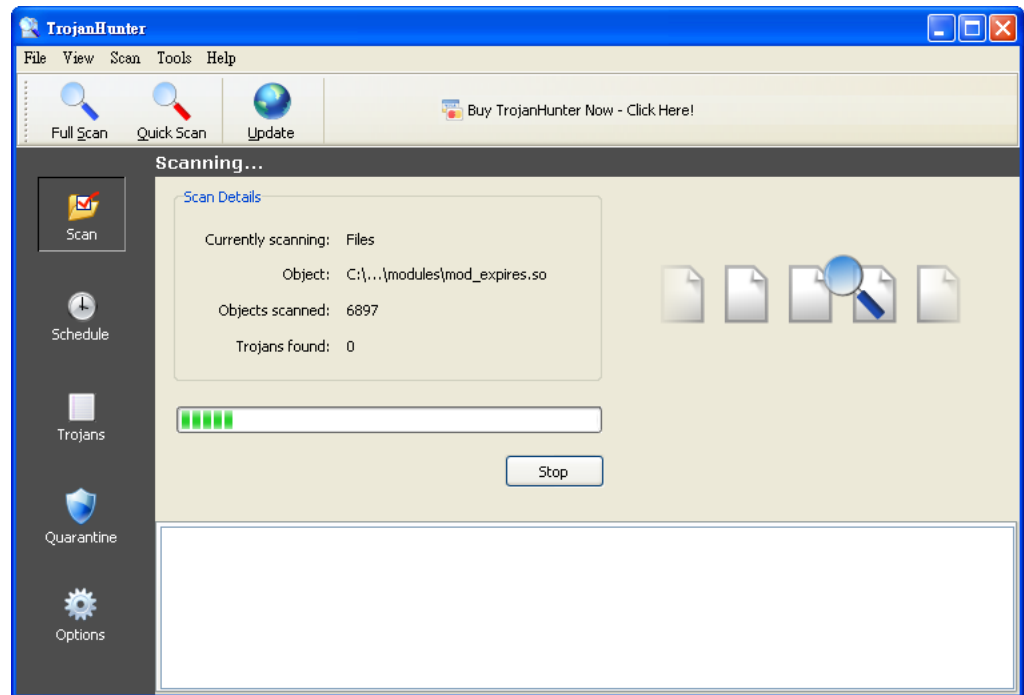
Spy Emergency

- 提供了反間諜軟體、反惡意軟體的解決方案，提供了即時防護及特徵碼更新功能，具中文操作畫面。



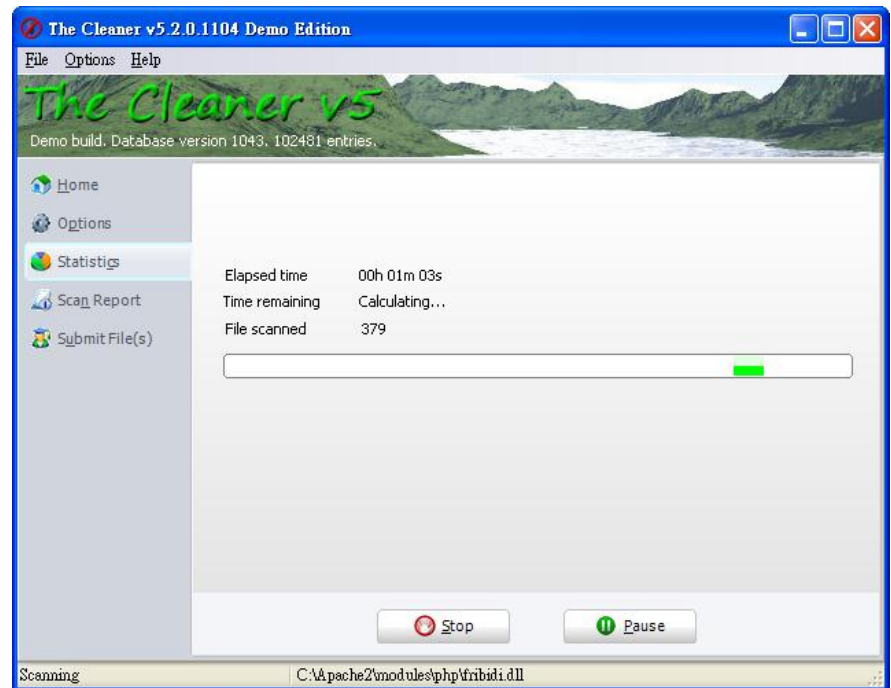
Trojan Hunter

- 可掃描及移除電腦系統中的特洛伊木馬程式，並可以自訂偵測規則。



Cleaner

- Cleaner 的功能很強大，清除的特洛伊木馬種類很多，可多達上千種。



練習

- 使用 Currport 檢查 Port 的使用狀況。
- 使用 TCPView 檢查自己使用的電腦，看看是否有異常的連線，能否解釋每一個連線。(關閉 MSN 或即時通，有助於連線的減少)
- 使用兩種以上的掃描及清除木馬的軟體並更新，檢查掃描以後看看是否有發現被植入後門。