# 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。

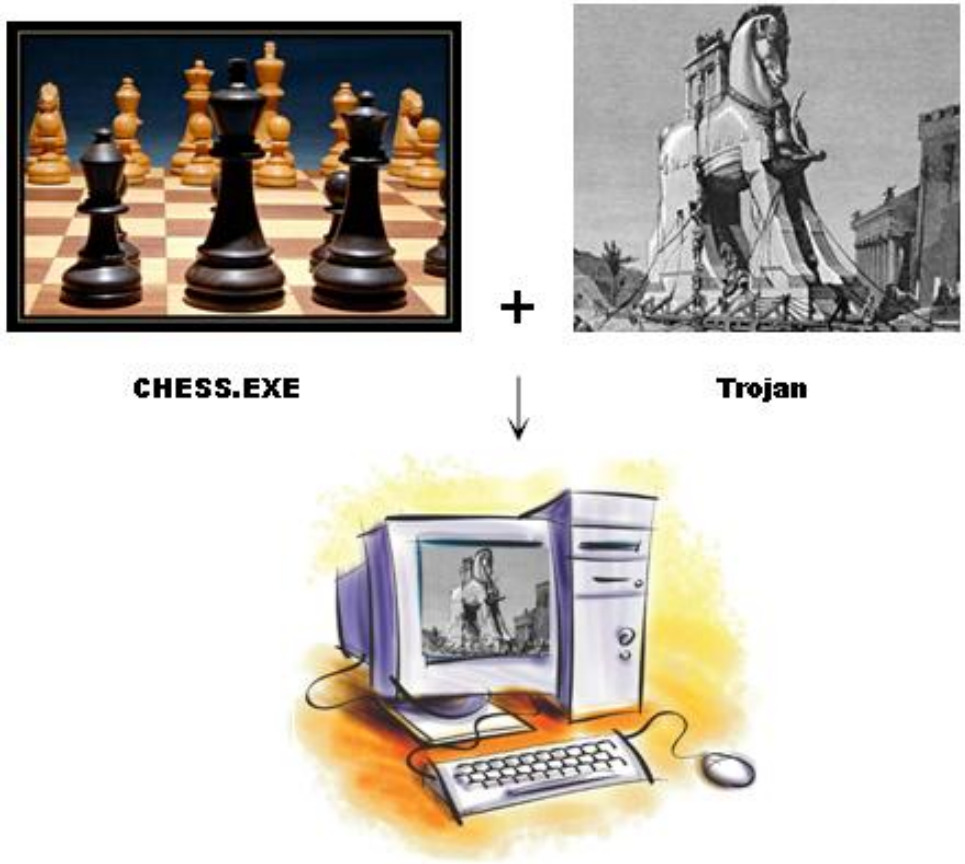
# 常見的木馬程式

| 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



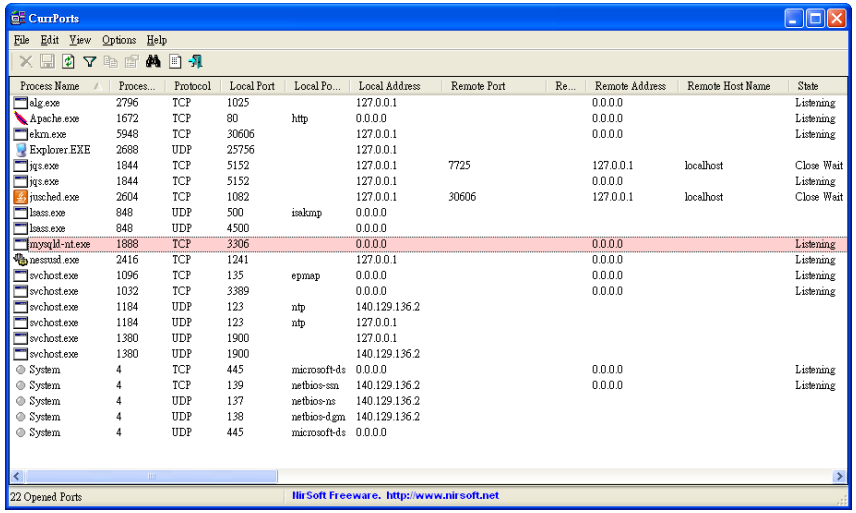
# 對策

- 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**

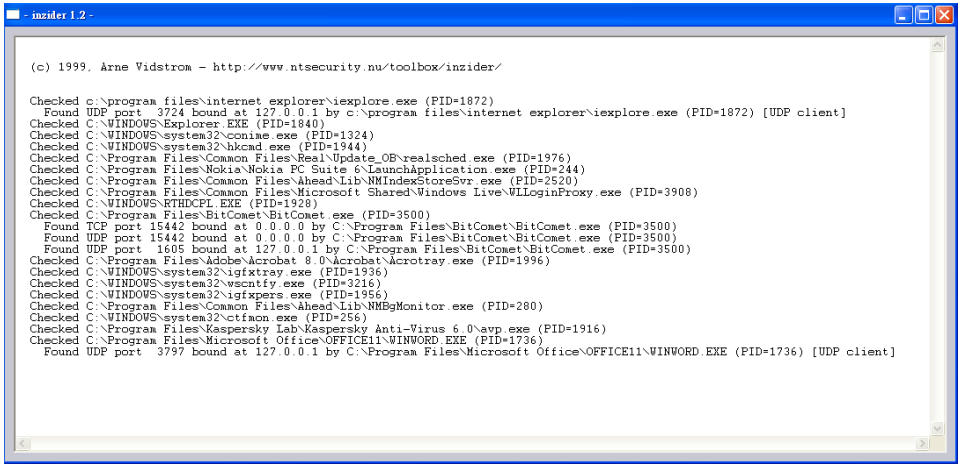
- 可以即時的顯示出電腦上的使用狀況，例如程式位置、連接埠、IP 位址...等資料。如果發現異常的連線，還可以將異常連線中斷。



# 工具程式

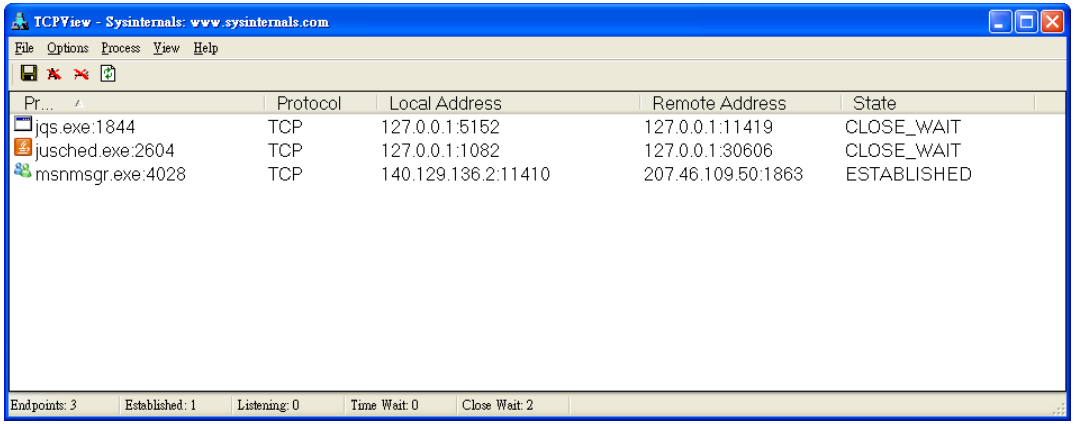
- **Inzider**

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



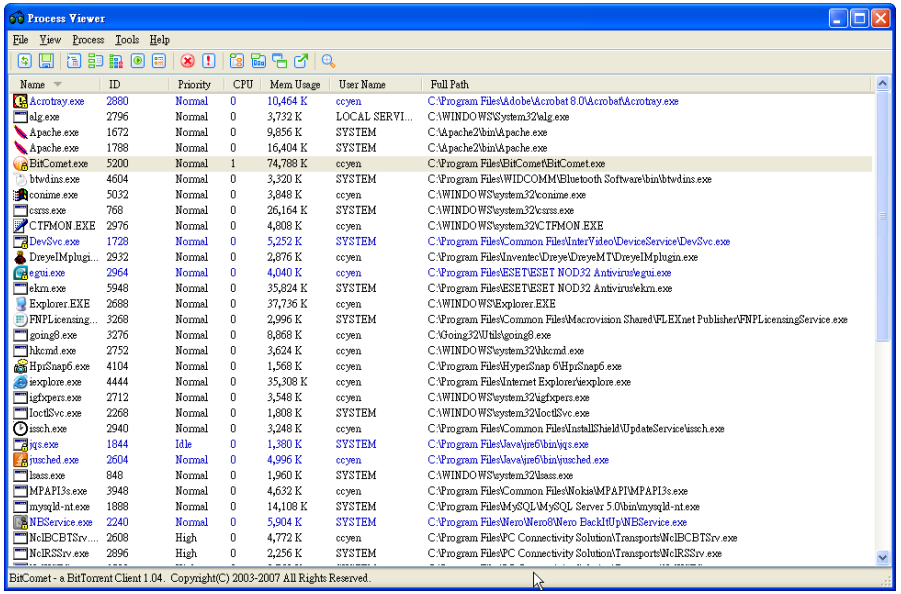
# TCPView

- 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。



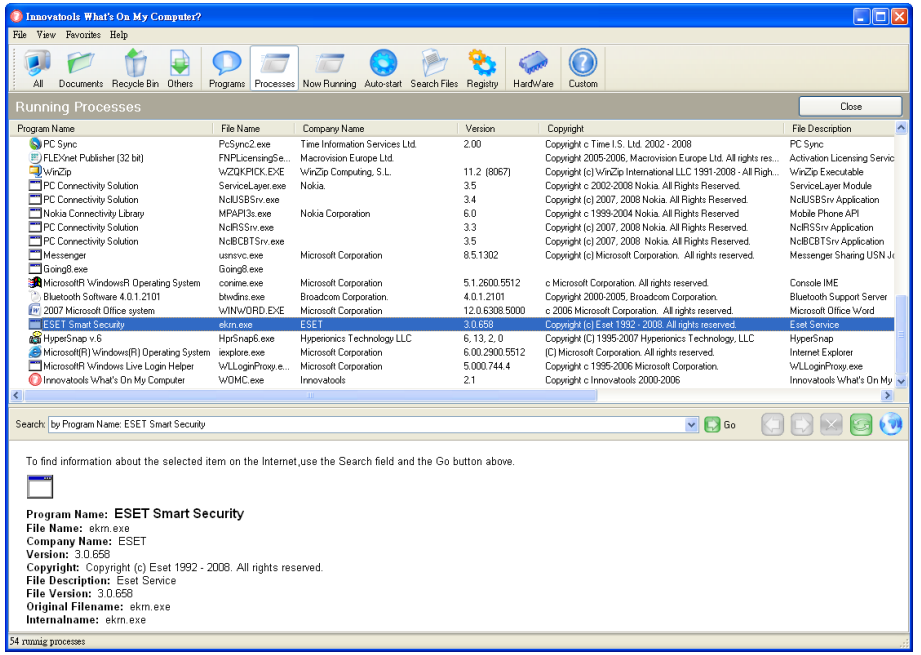
# Process Viewer

- 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。



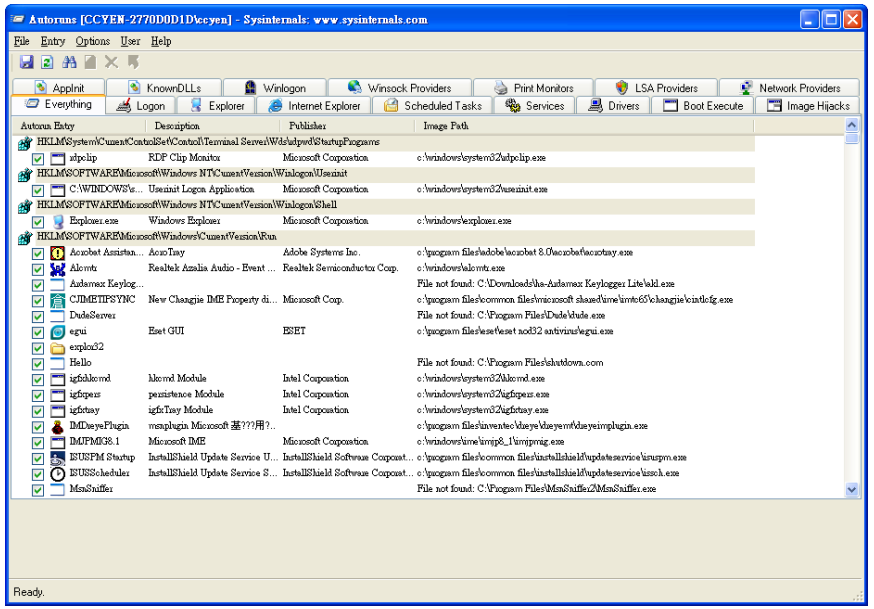
# What on my computer

- 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。



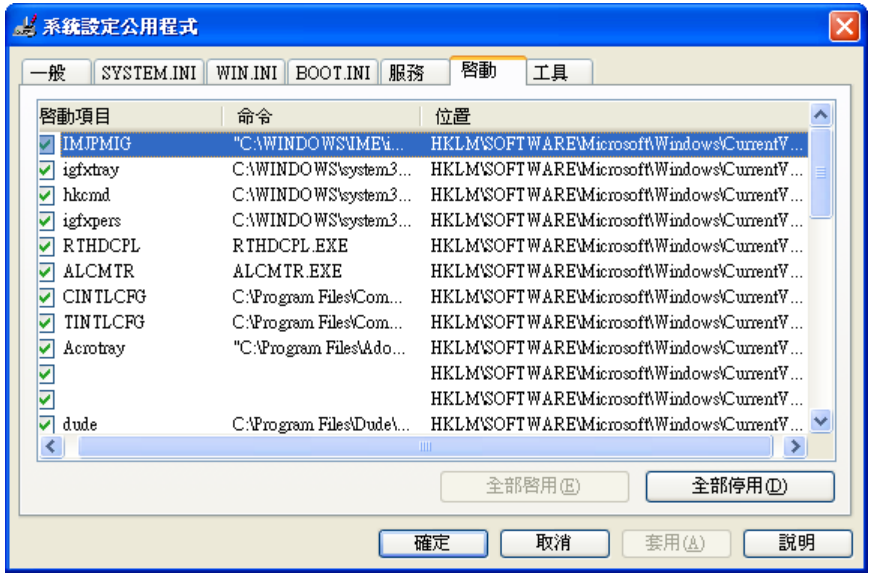
# AutoRuns

- 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。



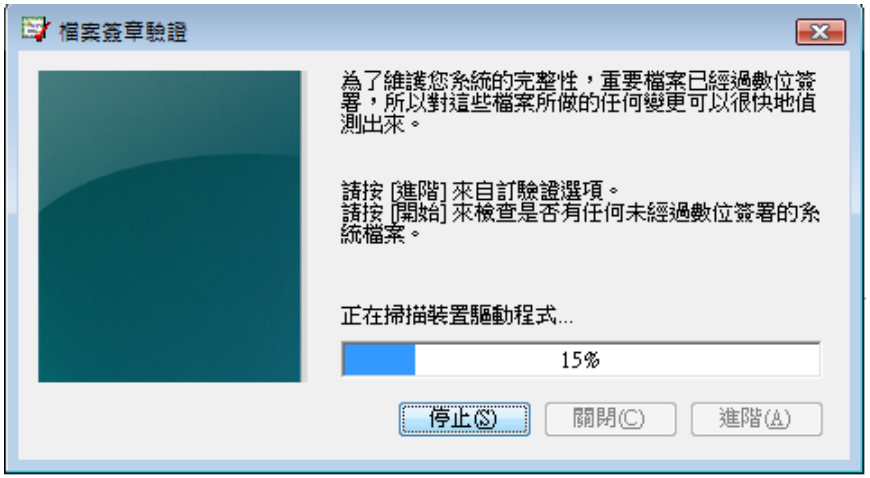
# MSConfig

- 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 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。

# 工具程式

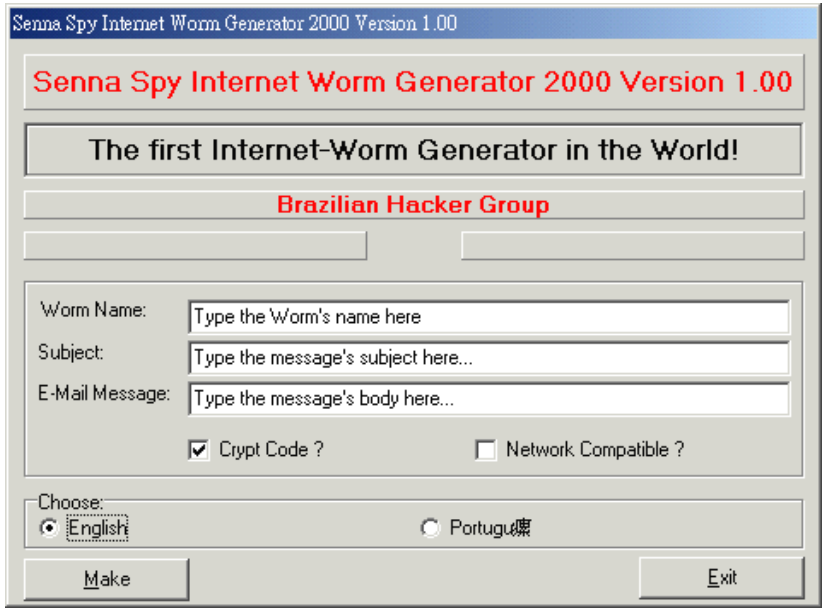
- **MegaSecurity.org**


No Downloads

| Files 2000 | Files 2001 | Files 2002 | Files 2003 | Files 2004 | Files 2005 | Files 2006 | Files 2007 | Files 2008 |
|---|---|---|---|---|---|---|---|---|
| N/A | January | January | January | January | January | January | January | January |
| N/A | February | February | February | February | February | February | February | February |
| March | March | March | March | March | March | March | March | March |
| April | April | April | April | April | April | April | April | April |
| May | May | May | May | May | May | May | May | May |
| June | June | June | June | June | June | June | June | June |
| July | July | July | July | July | July | July | July | July |
| August | August | August | August | August | August | August | August | August |
| September | September | September | September | September | September | September | September | September |
| October | October | October | October | October | October | October | October | N/A |
| November | November | November | November | November | November | November | November | N/A |
| December | December | December | December | December | December | December | December | N/A |

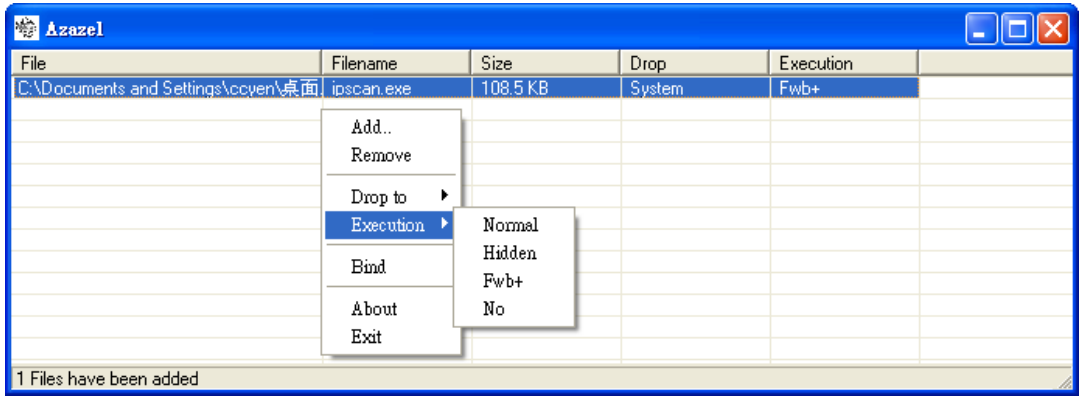
# Senna Spy

- 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。



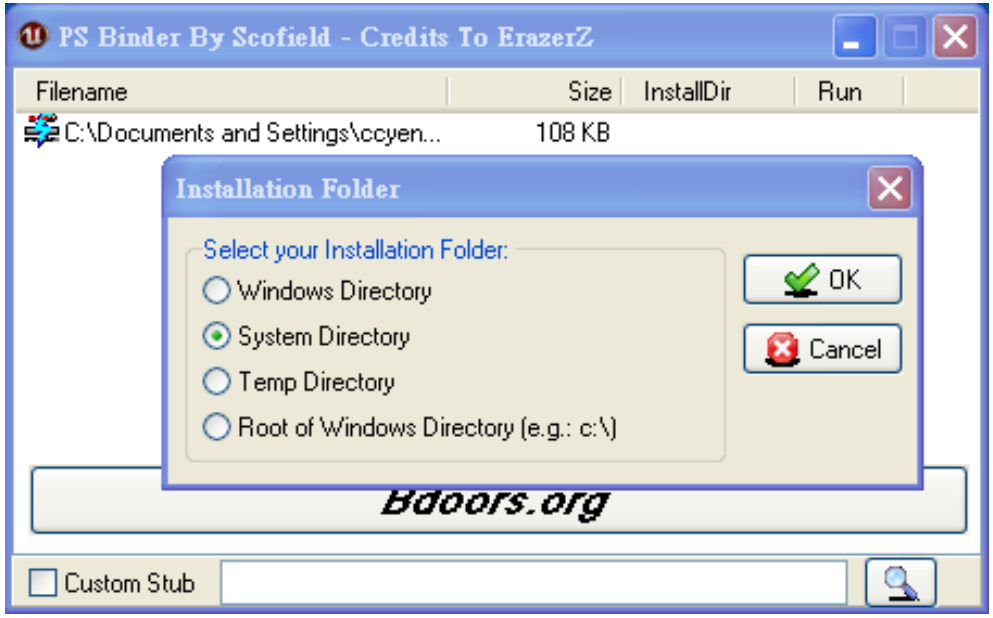
# Azazel

- 檔案包裹程式，可以包裹無限個檔案並放在指定的路徑下，並能夠自動隱藏執行。

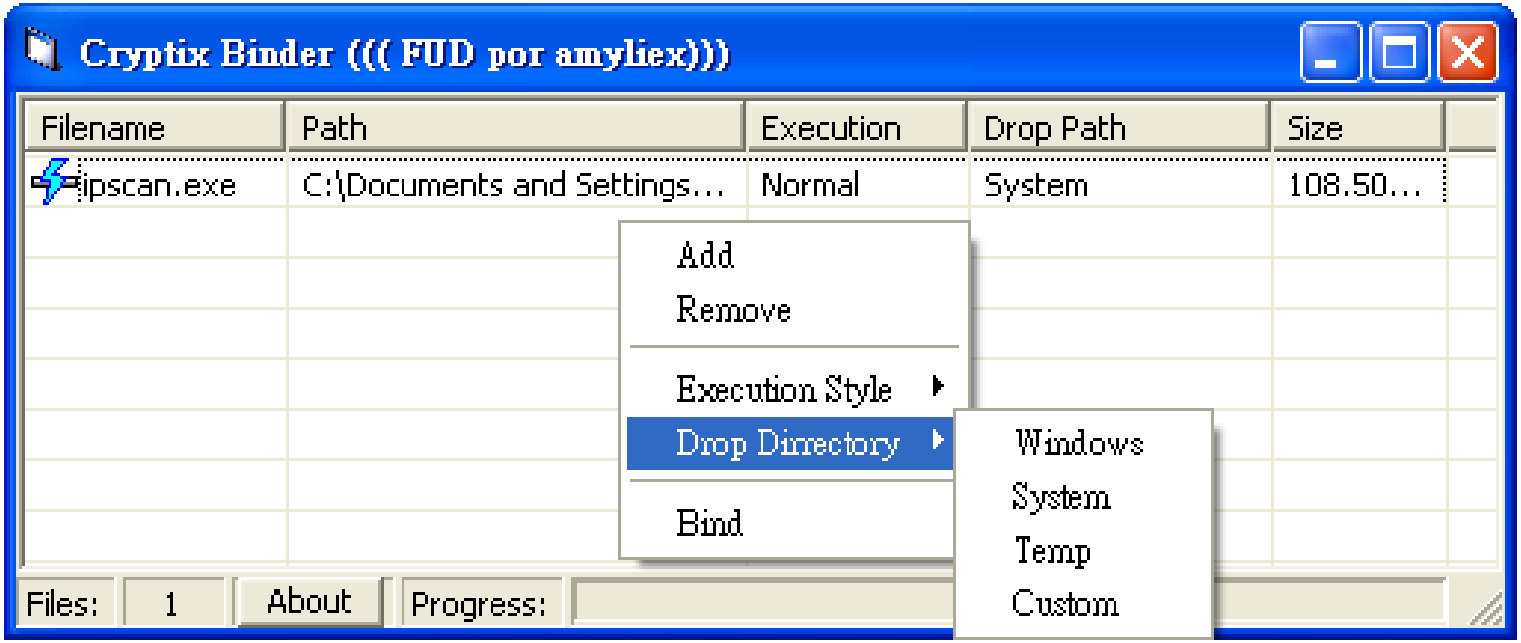


# PSBinder

- 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。

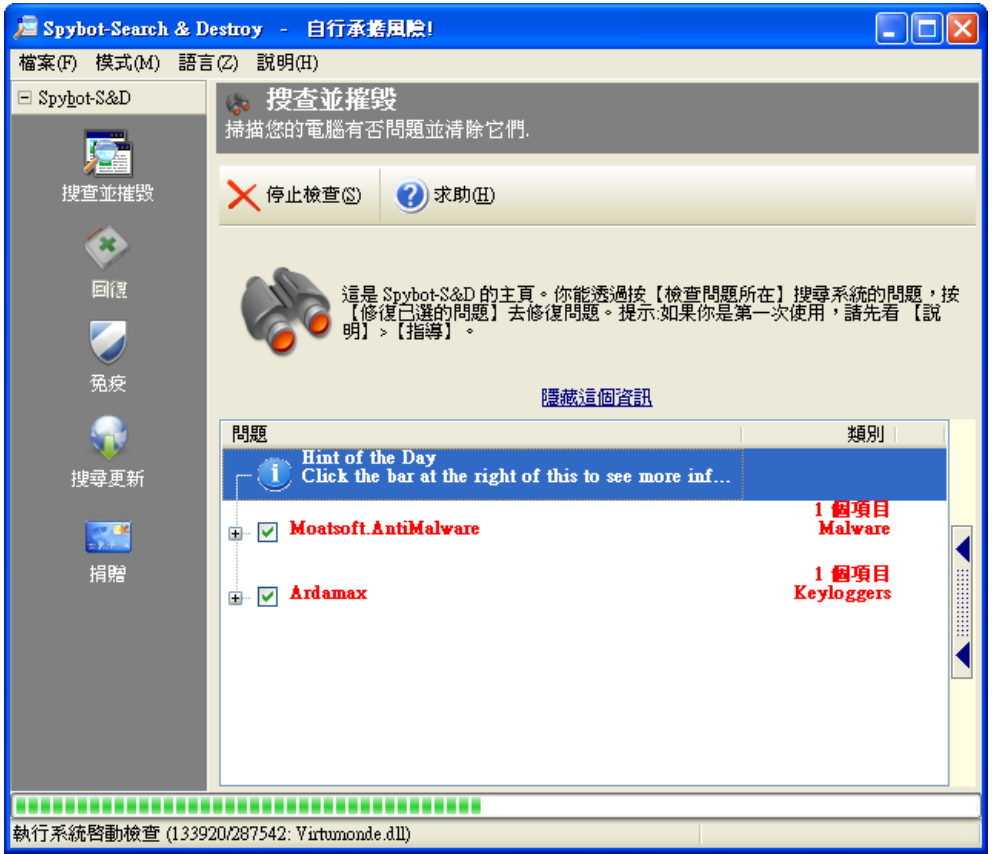


# Cryptix Binder



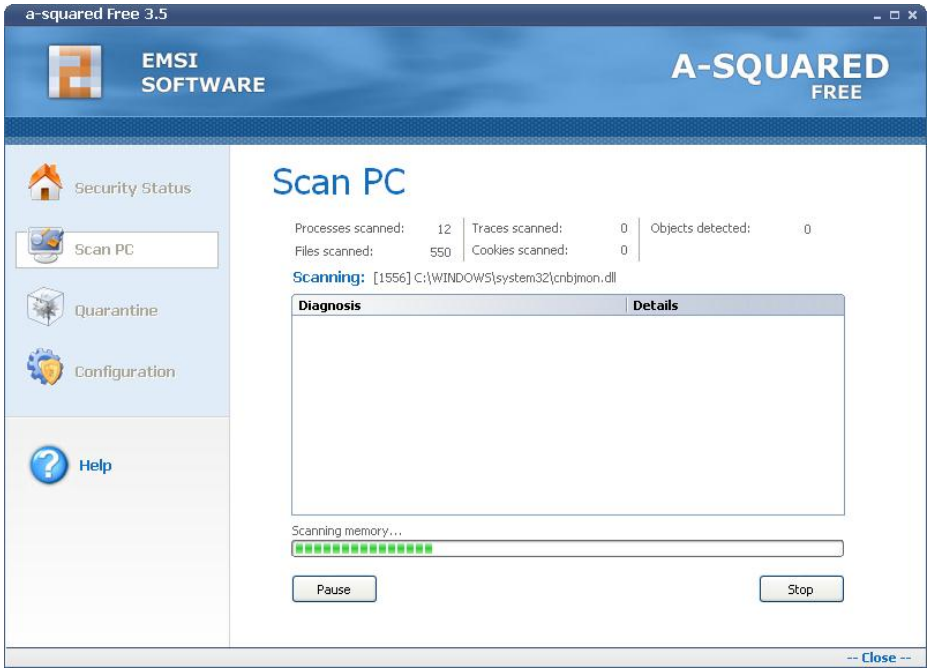
# SpyBot Search & Destroy

- 掃瞄及清除木馬的軟體。

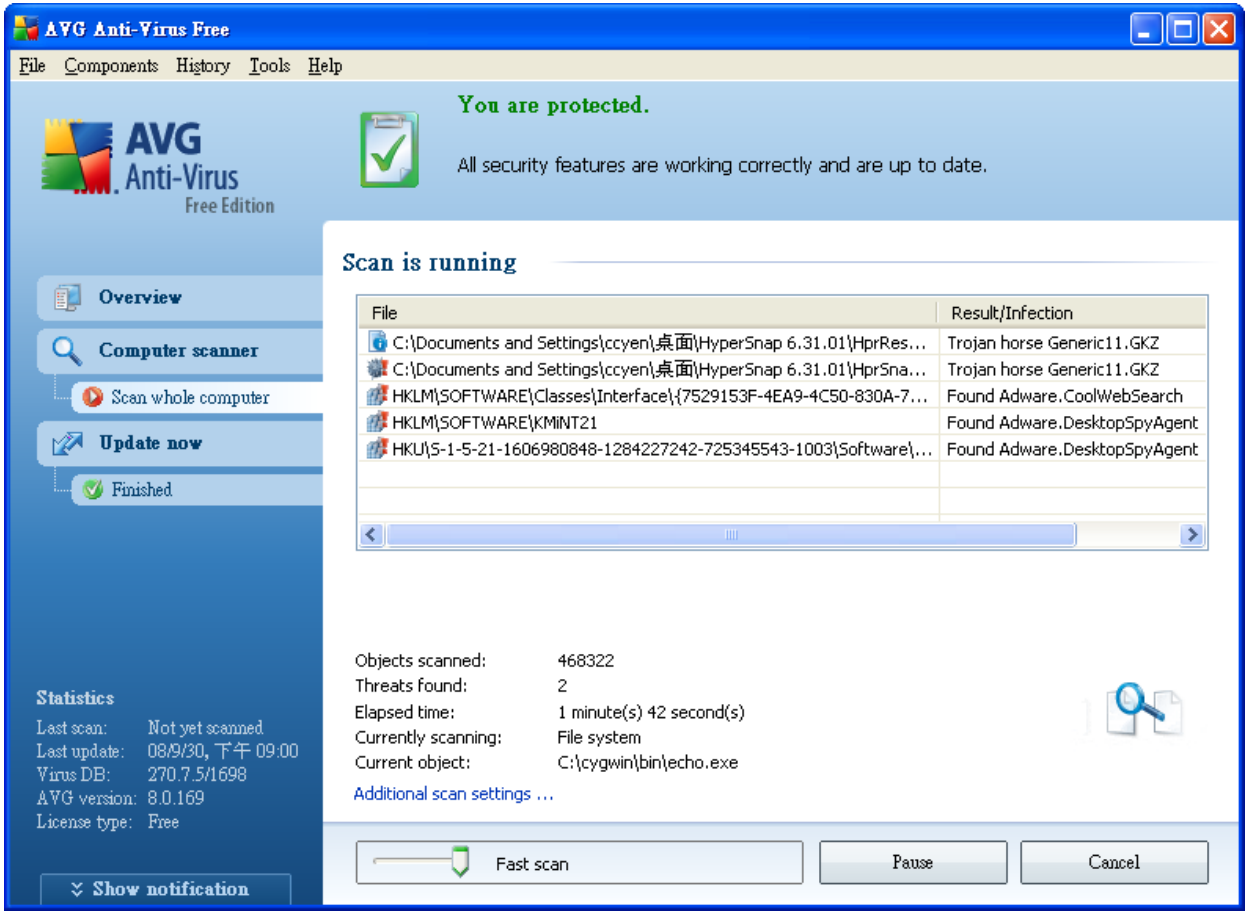


# A-Squared Free

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



# AVG Free Edition



# AD-Aware 2008 Free

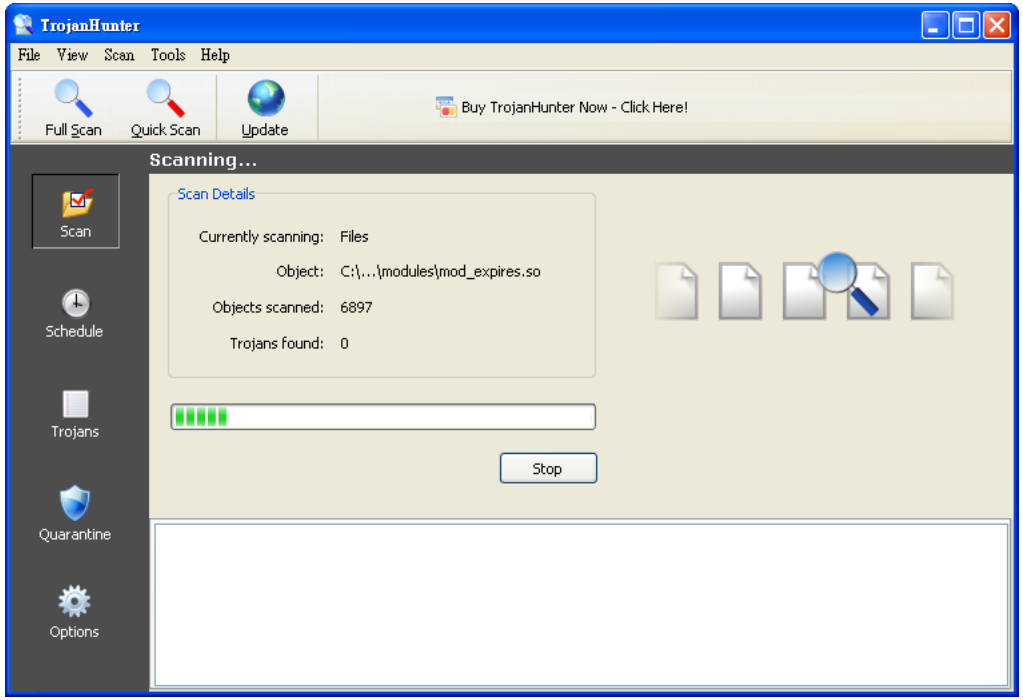
- Ad-Aware SE Personal 結合了後門程式掃瞄與個人隱私記錄、反追蹤移除等功能的免費軟體，可以線上更新掃瞄檔。

# 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。

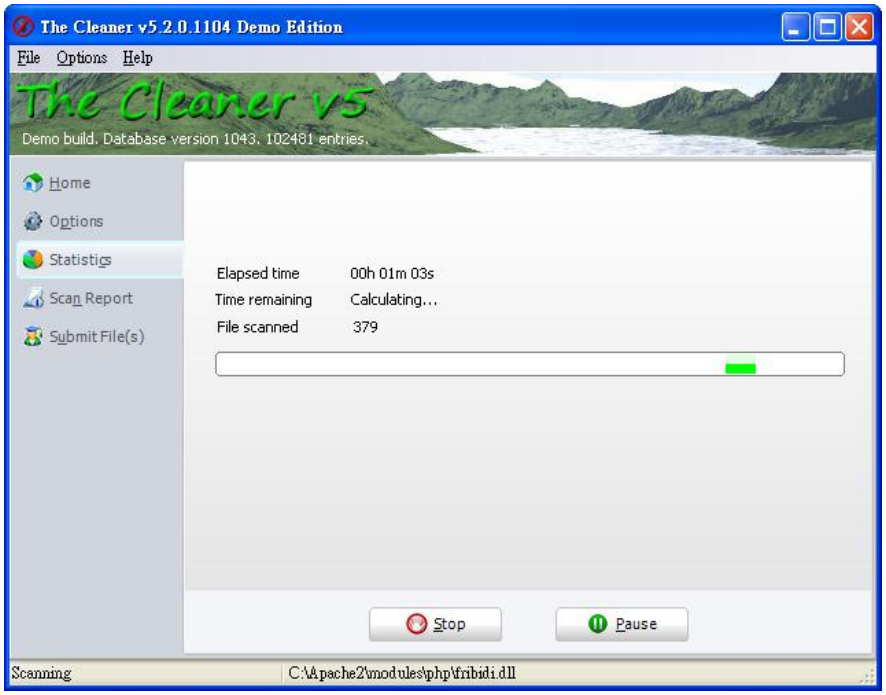
# Trojan Hunter

- 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)
- 使用兩種以上的掃瞄及清除木馬的軟體並更新，檢查掃瞄以後看看是否有發現被植入後門。