惡意軟體

- 病毒
  - 傳統
    - 自我複製的可執行程式
    - 破壞硬碟資料 or 格式化硬碟
    - 佔據系統記憶體空間
  - 現代
    - 利用 JAVA 或 Active X 的特性撰寫病毒
    - JAVA 病毒會強迫 windows 不斷開啟新視窗吃光資源
    - 對使用者造成不便的不懷好意的程式碼，均被歸類為病毒

惡意軟體 (Cont.)

- 感染病毒的徵兆
  - 突然出現音樂
  - 偶而出現亂碼
  - 無法開機
  - 畫面出現硬碟格式化警告訊息
  - 系統執行速度變慢
  - 不斷重開機
  - 檔案大小異常變大
  - ...

惡意軟體 (Cont.)

- 病毒種類
  - 巨集病毒 : Word, Excel
    - Ex. Taiwan No. 1 巨集病毒
  - 開機型病毒 :
    - 藏匿在開機磁區
    - 控制 DOS 的各種 『中斷』
  - 檔案型病毒
    - 可執行檔 : Ex. .com or .exe
    - 常駐型 : 躲在記憶體 , 須以冷開機處理
    - 非常駐型 : 中毒檔案一旦被執行會感染更多檔案

惡意軟體 (Cont.)

- 複合型
  - 兼具開機型及檔案型病特性
    - Ex: Hammer (大榔頭), Flip
- 隱形飛機式病毒
  - 又稱中斷截取者
  - 控制 DOS 的中斷向量，讓 DOS 及防毒軟體認為系統是乾淨的
- 千面人病毒
  - 中毒的檔案所含病毒碼均不相同
  - Ex: Whale, Flip

惡意軟體 (Cont.)

- 病毒擴散方式
  - 複製到掃瞄電腦目前連線的其他電腦
  - 自行複製病毒碼傳給通訊錄中的人
    - Ex: Outlook (容易撰寫程式)
- 防毒原則
  - 使用防毒軟體 : Ex. McAffee, Trend, 賽門鐵克
  - 不要開啟有問題的附件
  - 不要相信任何寄送給你的『安全警告』

惡意軟體 (Cont.)

- 病毒躲避監視的方法
  - 千面人 (polymorphism)：病毒藉著與不同的金鑰加密來改變外形
  - 變體 (metamorphism)：病毒不是靠變形來躲避監視，而是實質地改變自己的內容 例如在原始碼中加入多餘的程式或調整程式順序
  - 隱藏 (stealth)：例如有的隱藏病毒可以修改作業系統顯示的檔案大小，讓人無法察覺被寄生檔案的改變
  - 加殼 (armoring)：病毒使用特殊的程式碼保護自己，使防毒軟體或清毒專家更難偵測、分解與瞭解病毒碼
  - 通道 (tunneling)：病毒建立通道來攔截低階的作業系統呼叫與中斷，以削弱防毒軟體的偵測功能

特洛依木馬

- 一種看起來友善，實際上卻有惡意的程式
- 例：螢幕保護程式或登入的對話盒可能隱含不良動作，如：下載具傷害性的軟體、安裝鍵盤側錄程式、開啟後門 (Backdoor) 供駭客使用
- 會執行非預期或未授權 (惡意) 之動作的程式
- 不會感染其他寄宿檔案
- 直接刪除受感染程式清除

特洛依木馬 (Cont.)

- 根據維基百科上面的說法，感染彩虹橋木馬的電腦可以控制：
  1. 控制「工作管理員」，可關閉運作中的程式或啟用軟體
  2. 控制「檔案總管」，可瀏覽、上傳、偷取或刪除特定檔案
  3. 控制視窗大小，關閉、放大縮小視窗，或重新命名視窗名稱
  4. 取得系統資訊 ...
  5. 提取電腦中的帳號、密碼
  6. 側錄鍵盤輸入的文字、帳號、密碼
  7. 擷取電腦螢幕畫面
  8. 擷取 Webcam 拍到的畫面
  9. 登出電腦、重開機或關閉電腦
  10. 編輯系統登錄檔
  11. 遠端指令控制系統

特洛依木馬 (Cont.)

2008-12-1 字型：+ - | 看推薦 | 發言 | 列印 | 轉寄

駭客入侵拍女子裸照 PO她部落格嗆聲

〔記者黃良傑／屏東報導〕還在連線的電腦不要亂放，並時常留意鏡頭有無不正常開機，因為駭客就在你身邊，小心全裸被偷拍還不自知！

男大學生扮駭客炫耀

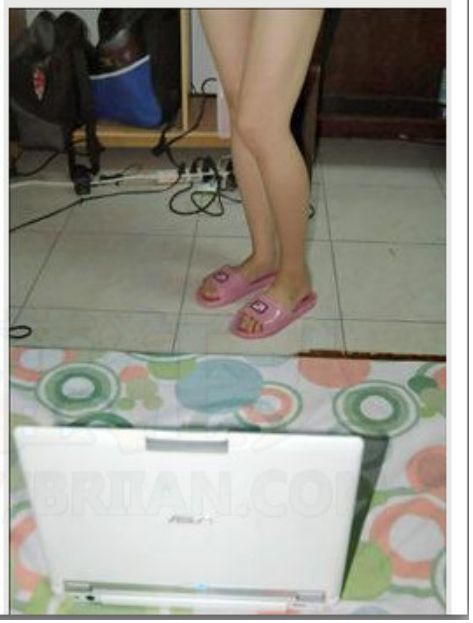
新竹縣21歲曾姓男大學生扮駭客，侵入屏東縣一名陳姓女子的電腦，植入可自動開啟、恢復、傳輸的「彩虹橋木馬程式」，再透過網路遠端遙控，開啟女子電腦上的攝影機，恰巧陳女把仍連線中的筆電放在床上，又未留意電腦遭人侵入並啟動攝影機，從浴室洗完澡全裸出浴，全被曾某窺見拍下，另錄下被害女子和男友在房內的私密談話與活動。

曾姓大學生只為證實自己可炒熱別人部落格的能力，竟惡作劇地把陳女全裸影像，PO到陳女自己的部落格上，供不特定人進入瀏覽，4月13日晚，陳女進入雅虎奇摩網站自己的部落格，驚見自己出浴的裸體畫面，嚇得花容失色。

對方行徑囂張，還在部落格上留言「反正妳本來就在賺，多一點客人有何不好？」、「要妳不要再賣了，不懂自愛誰愛妳！」等不堪入目的言詞，涉及詆毀被害人，陳女報警處理。

屏東縣警局科技犯罪小組循IP位址，找

彩虹木馬程式入侵圖解



緩衝區溢位攻擊

- 嘗試將超過緩衝區大小的資料寫入緩衝區的攻擊
- 超出緩衝區的資料會被載入主記憶體
- 正確的資料可能會被覆蓋
- 可以讓任意程式（可能是有惡意的）被執行
- 讓系統當機
- Sasser病毒
  - 利用Windows 已知的缺陷進行擴散
  - 副作用：機器因不明因素不斷重開機

制作Sasser病毒嫌犯落網 年僅18歲

【大紀元5月9日訊】〔自由時報羅彥傑綜合八日外電報導〕德國警方八日表示，他們已逮捕一名涉嫌創作新型電腦病毒「殺手」（Sasser）的嫌犯，是一名年僅十八歲的高中生。「殺手」病毒上週開始肆虐全球，利用微軟視窗作業系統的瑕疵進行破壞，造成一千八百萬台電腦重複關機又開機。

德國下薩克森邦警署發言人費德勞說，這名嫌犯於七日被捕，而且坦承設計「殺手」病毒，但警方尚不確定這名青年是否設計出「殺手」的所有變種病蟲。費德勞說：「他已坦承不諱，而且微軟公司的專家現在也證實他就是這隻病毒的始作俑者。」

德國警方不願透露這名嫌犯的身分，不過「明鏡週刊」指出，此人的姓名是史文（Sven J.），是一所高中的畢業生，但尚未取得畢業證書。

德國警方與檢察官七日搜索嫌犯父母位於北部瓦芬森鎮的寓所，查扣其所有的電腦。「明鏡週刊」在未引述消息來源的情況下報導，美國中央情報局與聯邦調查局也參與搜捕嫌犯的行動，但嫌犯犯罪的動機目前尚不明朗。

網路防毒專家對這起案件能迅速破案感到訝異，認爲這可能是在打擊病毒設計集團犯罪方面，截至目前收穫最豐的一次逮捕行動。費德勞說，這名和父母同住的嫌犯和黑社會沒有任何關係，但目前尚不能證實他與其他撰寫病毒程式者有無關聯。

專門設計電腦病毒與病蟲的不法集團，一直讓執法人員很傷腦筋。芬蘭網路安全業者F-Secure防毒研究部主任海波南說：「真希望這次逮捕行動可以讓他們收斂一點。如果我們能開始抓到這些傢伙，就一定可以對目前撰寫病毒程式的那些人施加多一些壓力。」

「殺手」病毒自一開始就讓網路防毒專家摸不著頭緒。與大多數最近出現的病毒不同，「殺手」在設計上僅是用來擴散與癱瘓電腦網路，而不是控制電腦或竊取裡面的資訊。目前流行的說法是，撰寫「殺手」的作者和兩個月前流行的「網路天空」（Netsky）病毒作者是同一票人。

包括歐洲、北美和亞洲的企業與個人電腦用戶都傳出遭到「殺手」病毒的侵入，台灣也有三分之一的郵局支局傳出災情。「殺手」也造成英航劃位櫃檯作業紊亂，四日有二十架班次爲此延誤十分鐘。

間諜軟體

- 需要更高深的技術知識
- 間諜軟體的形式
  - 網站上的 cookies
  - 鍵盤側錄程式
- 記錄敲擊鍵盤記錄
- 定期擷取電腦畫面
- 持續暗中監視你在特定電腦上活動的軟體

其他形式的惡意軟體

- Rootkit
  - 一組駭客入侵的工具組合，可以
    - 監視訊務以及鍵盤敲擊記錄
    - 建立後門
    - 修改日誌檔與現有的系統工具以避免被偵測出來
    - 攻擊網路上的其它機器

惡意的網頁程式碼

- 網頁可移動式程式碼
  - 可以在所有作業系統或平台上運作的程式碼
  - 貿然使用多媒體技術（例如 Java 與 ActiveX）可能會導致某些具有錯誤或不可信任的程式
  - 透過網站可以快速地擴散

整理

特徵	病毒	蠕蟲	木馬	惡意行動碼	追蹤cookie	攻擊工具
可否自行存在？	否	是	是	否	是	是
可否自行複製？	是	是	否	否	否	否
擴散方法爲何？	使用者互動	自行擴散	使用者不知情的網路下載、電子郵件附檔、或由惡意者植入			

偵測並移除病毒與間諜軟體

- 防毒軟體的兩種運作方式：
  - 掃描病毒特徵
    - 必須持續更新病毒特徵
  - 檢視電腦上執行程式的行為
    - 嘗試存取系統電子郵件程式中的通訊錄
    - 嘗試改變 Windows 裡的註冊檔設定

偵測並移除病毒與間諜軟體 (Cont.)

安全政策

- 安全政策應說明惡意程式之防禦責任，做為建置各項防禦措施之基礎。

教育訓練

- 建立並維持所有人對惡意程式的認知，並加強資訊人員對惡意程式防禦的教育訓練，可以有效降低人為錯誤所造成的資訊安全事件。

弱點補強

- 補強系統及網路的弱點可以降低惡意程式的攻擊動力。

威脅防禦

- 建置多重的威脅防禦措施 (如防火牆與防毒軟體) 可以避免惡意程式成功的攻擊系統或網路。

偵測並移除病毒與間諜軟體 (Cont.)

補丁管理

- 安裝補丁是作業系統與應用程式最通用的弱點補強方法。
- 新的弱點被公布而補丁還未完成安裝前，是系統最脆弱的時候。

最小權限

- 最小權限原則是在不影響工作的情況下，只提供最小的使用權限給使用者、程式和主機。由於惡意程式經常需要取得管理員權限，因此最小權限原則是一個有效的防禦手段。

強化主機

- 主要的原則還是關掉或移除不需要的服務、排除不安全的檔案共享、建置身分認證機制並勤於更換夠強的密碼。

參考資料

- 趨勢科技
  http://www.trend.com.tw/corporate/security/virusprimer_1.htm
- 電腦病毒
  http://www.ntp.ks.edu.tw/computerknowledge/copedu/%B9q%B8
-