教你如何百毒不侵

大仁科技大學
數位學習中心
韋俊丞

病毒

- 一段電腦程式碼，會將自身附加到程式或檔案，在電腦之間散佈
- 每種病毒有自己的擴散方式，例如寄生在檔案或程式上再經由使用者下載、拷貝後感染。
- 病毒可能會損壞軟體、硬體和檔案。

蠕蟲

- 病毒需要寄居體，而蠕蟲則相當獨立：它可以自行存在、自行複製、自行擴散。因此蠕蟲可以在短時間內快速擴散，形成全球性事件。
  - 網路服務蠕蟲 (network service worms) 利用網路服務中有弱點的作業系統或應用程式進佔主機；再繼續掃描其它相同弱點的主機，作爲攻擊目標。由於蠕蟲擴散不需要人的參與，所以擴散極快。
  - 大量郵件蠕蟲 (mass mailing worms) 與郵件病毒相仿，只是蠕蟲不需要寄居在其它檔案上。郵件蠕蟲感染一台電腦後，繼續使用受害者的通訊錄將自己再大量的寄出。

特洛伊木馬

- 木馬程式可以自行存在，但不以複製或擴散爲目的。它看似好的程式，卻暗藏惡意。
- 偵測木馬程式有時並不容易，因爲它執行起來像是一個正常的應用程式。此外，較新的木馬程式也會使用躲避監視的手法。
- 不同於病毒或蠕蟲只會產生破壞，木馬程式可能爲攻擊者帶來利益，因此木馬攻擊似有凌駕前兩者的趨勢。

惡意行動碼

- 網路時代開始後，大家開始撰寫跨平台行動碼 (mobile code)，在不同的作業系統、不同的瀏覽器及電子郵件閱讀器上都能順利執行。
- 行動碼可以從遠端系統傳來在本地執行的軟體，通常行動碼的下載不需要使用者的允許。
- 雖然行動碼大多是善意的，但惡意行動碼可以攻擊系統，並傳送病毒、蠕蟲及木馬。
- 惡意行動碼與病毒及蠕蟲等頗有不同，它不感染檔案或企圖擴散，也不利用特定的弱點。惡意行動碼是靠本地主機所授予行動碼的權限。
- 行動碼最常使用的語言是 Java, ActiveX, Java Script, VB Script 等。

追蹤 Cookies

- Cookie 是特定網站在客戶端建立的一個小資料檔
  - 會談 cookie 是暫時的，只在一次網站拜訪中有效；
  - 長期 cookie 則長期存在客戶端電腦中，在每次拜訪該網站時，讓網站得以識別該使用者。網站可以藉以記錄使用者的喜好。
- 然而長期 cookie 可被利用做爲間諜程式，在使用者不知情下，追蹤他的瀏覽器活動。

攻擊工具 (I)

- 攻擊工具 (attacker tools) 主要是幫助攻擊者不經授權地存取被感染的系統。攻擊工具可以藉由蠕蟲或木馬等惡意程式送進系統；再被用來進行下一步的攻擊。
- 後門程式 (backdoor) 通常包含客戶端與伺服器兩個部分，前者在入侵者的遠端電腦上，後者在受感染的系統內。兩者連線後，入侵者就可以存取受感染系統的檔案或下指令。
  - 殭屍程式 (zombie) 是一種後門程式，植在一個系統內讓它去攻擊別的系統。DDoS 攻擊就是利用許多的殭屍系統同時對一個受害者發動攻擊。

攻擊工具 (II)

- 鍵盤側錄 (keylogger) 監視並記錄鍵盤的使用，可能包括受害者鍵入的密碼、郵件、信用卡帳號等私密訊息。
- Rootkit 是一個或一組的惡意程式可以幫助入侵者控制系統並躲避偵測，成功地植入 rootkits 可以讓入侵者擁有管理員的權限。
- 瀏覽器嵌入軟體 (web browser plug-in) 可被用做間諜程式；一旦嵌入後，可以監視使用者的瀏覽器活動，包括上過的網站與瀏覽的網頁。
- 攻擊者工具包 (attacker toolkits) 可以一次植入各種工具到受害者的電腦裡面，讓攻擊者立即或日後監控受害者。

綜合比較

- 病毒、蠕蟲和木馬程式三者也常被彼此誤用。下圖顯示三者間的差異。
- 惡意行動碼與追蹤 cookies 主要是在網站瀏覽過程中入侵。
- 攻擊工具是指後門程式、rootkits 與鍵盤側錄等，本身不造成損害，而是植入後可供駭客使用的工具。

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			

混合攻擊

- 混合攻擊 (blended attack) 是一個惡意程式使用多種感染與傳輸方法，Nimda 惡意程式就使用了四種擴散方式：
  - 電子郵件：當一個主機有弱點的使用者打開了被感染的電子郵件附件，Nimda 感染主機，並找出郵件通訊錄將自己大量的寄出。
  - 視窗的資源分享：Nimda 掃描設定不當檔案分享的主機，利用 NetBIOS 傳輸來感染主機上的檔案。當使用者執行被感染的檔案，就會啓動 Nimda。
  - 網站伺服器：Nimda 掃描網站伺服器，尋找微軟 IIS 的已知弱點 (同一弱點在 2001 年稍早被 Code Red 蠕蟲利用，造成全球三十餘萬台電腦被感染)，若找到弱點，就感染該伺服器及其檔案。
  - 網站客戶端：如果一台有弱點的網站客戶端瀏覽了被 Nimda 感染的網站伺服器，則客戶端主機也被感染。
- 除了以上方法，混合攻擊也可以利用 IM (即時通)或 P2P 做爲擴散管道。

非關技術-社交工程

- 最難防禦的資訊安全攻擊是人對人的欺騙，稱之爲社交工程 (social engineering)。
- 社交工程是攻擊者藉由社交手法取得系統或網路的資訊，例如 ID, password 等。接觸管道包括電話、電子郵件、或面對面的與組織成員對話。
- 除了傳統管道外，即時通訊 (instant massaging, IM) 是較新的社交工程管道。以組織的角度來看，IM 像是一個個的後門，隨時會有機密資訊外洩的可能。
- 網路釣魚也是社交工程的一種。
- 防制社交工程的唯一方法是經由資訊安全的教育訓練。

網路釣魚

- 網路釣魚 (phishing) 是一種欺騙攻擊，它可能是一個看似有公信力的惡意網站，或是冒名的電子郵件要受害者連結到惡意網站。
  - 左圖爲釣魚信件

From: "Web服務" <shih@thu.edu.tw>
To: undisclosed-recipients:;
Sent: Thu, 17 Feb 2011 15:14:49 +0800 (CST)
Subject: 確認您的電子郵件身份

親愛的mail.tajen.edu.tw電子郵件帳戶擁有者，
此消息是從 mail.tajen.edu.tw信息中心所有mail.tajen.edu.tw
電子郵件帳戶的所有者。目前，我們正在提升我們的數據庫和電子郵箱
帳戶中心。我們正在刪除所有未使用的電子郵件帳戶 mail.tajen.edu.tw
創造更多空間的新帳戶。為了防止您的賬戶關閉
你將有更新在下面，讓我們將知道它的一份禮物
使用的帳戶。
確認您的電子郵件身份下列
電子郵件用戶名：
郵箱密碼：
出生日期：
國家或地區：
警告！帳戶所有者拒絕更新他或她的帳戶內
七天收到此警告將失去他或她的帳戶
永久。
謝謝您mail.tajen.edu.tw！
警告代碼：VX2G99AAJ
謝謝，
mail.tajen.edu.tw隊
mail.tajen.edu.tw有限公司在線測試版

安全政策

- 如果沒有制定惡意程式防禦的相關政策，組織就不會貫徹執行防禦措施。以下爲常見的安全政策：
  - 外部進入組織的任何儲存媒體都要通過惡意程式掃描後才能使用。
  - 所有電子郵件附件都要先存入本地磁碟並通過掃描後才能開啓。
  - 禁止以電子郵件送出或接收某些種類的檔案，如 .exe 檔。
  - 限制或禁止使用可能傳輸惡意程式的軟體，例如 P2P 或沒有公信力的 IM。
  - 一般使用者不該有管理員的權限。
  - 要求系統與應用軟體更新並安裝修補程式。
  - 限制使用可移除的儲存媒體，如 USB 碟；尤其在公共區域或安全區域。
  - 指明各系統應該安裝的防禦軟體，並指導軟體的設定方式。
  - 規定只能使用組織認可的方法與其它網路通訊。

教育訓練

- 組織的資訊安全教育訓練中，應該加強惡意程式防禦的認知，以下是部分宣導重點：
  - 不開啓可疑之郵件或附件，即使熟識寄件者。
  - 不開啓某些種類的檔案 (如 .exe 與 .com 等)。
  - 不回應要求提供財務或個人資料的電子郵件。
  - 不點選可疑網站的彈出視窗。
  - 不瀏覽任何可能含惡意內容的網站。
  - 不任意關閉安全防禦機制，如防毒軟體與個人防火牆等。
  - 不下載來路不明的程式。
  - 任何疑問請撥校內分機 1930－1935 (共五線)詢問

弱點補強

修補管理

- 安裝修補程式是作業系統與應用程式最常用的弱點補強方式。
- 新的弱點被公布而修補程式未安裝前，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。

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。

防毒軟體

- 掃描系統最重要的部分，像是啓動檔。
- 注意系統上可疑的活動，例如當系統接收或傳送電子郵件時掃描附件。
- 監視應用程式的行爲，例如郵件軟體、瀏覽器和 IM 等。在應用程式執行有風險的動作前 (例如下載行動碼)，防毒軟體應提醒使用者。
- 掃描檔案檢查已知病毒。應該設定防毒軟體固定時間掃描整個硬碟，同時也要掃描其它儲存媒體。
- 識別惡意程式的種類，像是病毒、蠕蟲、木馬、行動碼、鍵盤側錄等。

防毒偵測的準確性

- 防毒軟體對惡意程式的偵測方式仍是以比對特徵 (signatures) 爲主；這種方法對識別已知惡意程式相當有效，對已知病毒的變形、變種也有很好的偵測效果。
- 特徵比對乃針對已知的威脅；要偵測全新的惡意程式則使用探索方式 (heuristic method)，包括在程式裡搜尋可疑的邏輯順序，或是先在虛擬機器 (virtual machine) 上執行程式來檢查可疑活動。
- 偵測新威脅的探索方式容易造成誤殺 (false positive)，也就是把好的檔案誤判爲惡意程式。因此，商用防毒軟體通常會讓使用者自己調節偵測的敏感度，在安全性和方便性之間做取捨。
- 主要的防毒軟體廠商通常在重要攻擊事件發生幾小時內，就要完成惡意程式分析、編寫攻擊特徵、測試之後連同說明文件下載給用戶。

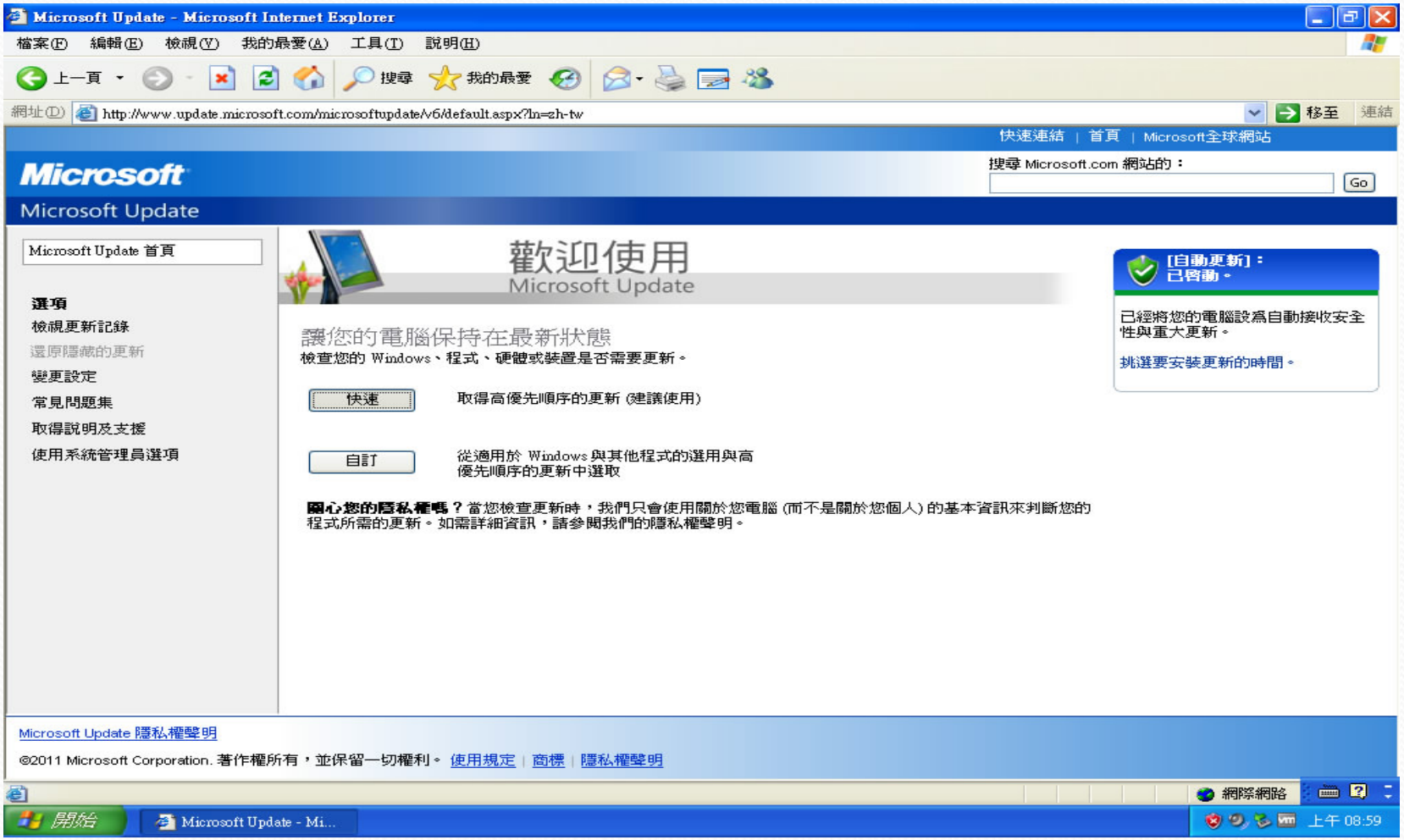
間諜程式的偵測與移除

- 防毒軟體主要在處理惡意程式；而間諜程式偵測與移除工具則同時針對惡意程式及非惡意程式形態的間諜程式。它常見的功能包括：
  - 監視最有可能帶進間諜程式的應用程式，像是瀏覽器與電子郵件軟體等。
  - 經常性的掃描檔案、記憶體與設定檔，尋找已知間諜程式。
  - 識別幾種間諜程式類別，包括惡意行動碼、木馬程式與追蹤 cookies 等。
  - 防止幾種間諜程式的下載方法，包括網站的彈出視窗、追蹤 cookies、瀏覽器嵌入等。
  - 監視網路及作業系統的核心，以及啓動程式。
  - 隔離或刪除間諜程式。

微軟資訊安全入口網站


Microsoft 資訊安全首頁 - Windows Internet Explorer
http://www.microsoft.com/taiwan/security/default.mspx
Google
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
Search Web
Video
我的最愛
建議的網站
取得更多附加元件
自訂連結
美女地圖
新光證券富貴角7號
Microsoft 資訊安全首頁
網頁(P)
安全性(S)
工具(O)
請按一下此處安裝 Silverlight
Taiwan 變更 | 所有的 Microsoft 網站
Microsoft
搜尋 Microsoft.com
bing
Web
高可信度電腦運算：資訊安全
資訊安全首頁
資訊安全公告
最近發生的事件
經銷商
資訊適用於
家庭使用者
IT 專業人員 (TechNet)
開發人員 (MSDN)
商務人員
全球資訊安全網站
資訊安全相關文章
擺脫不想要的軟體
間諜軟體：如何處理間諜軟體和其他有害軟體。
惡意程式碼：掃描並移除您電腦中的惡意程式碼軟體
完成
網際網路 | 受保護模式: 啟動
100%

微軟更新


Microsoft Update - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D) http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=zh-tw
移至 連結
快速連結 | 首頁 | Microsoft全球網站
Microsoft
搜尋 Microsoft.com 網站的：
Go
Microsoft Update
Microsoft Update 首頁
選項
檢視更新記錄
還原隱藏的更新
變更設定
常見問題集
取得說明及支援
使用系統管理員選項
歡迎使用
Microsoft Update
讓您的電腦保持在最新狀態
檢查您的 Windows、程式、硬體或裝置是否需要更新。
快速
取得高優先順序的更新 (建議使用)
自訂
從適用於 Windows 與其他程式的選用與高優先順序的更新中選取
[自動更新]：已啟動。
已經將您的電腦設為自動接收安全性與重大更新。
挑選要安裝更新的時間。
關心您的隱私權嗎？當您檢查更新時，我們只會使用關於您電腦 (而不是關於您個人) 的基本資訊來判斷您的程式所需的更新。如需詳細資訊，請參閱我們的隱私權聲明。
Microsoft Update 隱私權聲明
©2011 Microsoft Corporation. 著作權所有，並保留一切權利。 使用規定 | 商標 | 隱私權聲明
網際網路
開始
Microsoft Update - Mi...
上午 08:59

免費防毒

- 微軟 Security Essentials
  - 大仁校園使用
  - 原版作業系統即可擁有
- 小紅傘 Avira Antivir Personal Free
  - 僅限個人及非商業用途
  - 最多人使用免費防毒軟體
- AVG
  - 僅限個人及非商業用途
  - 掃描速度快，偵測率高
  - 跟其他免費版的防毒軟體比起來，AVG的防護還算是頗齊全的。
- 雲端防毒軟體-Immunet Protect
  - 第二套防毒軟體
  - 結合網路即時病毒資訊通報

微軟 Security Essentials

- 下載網址：http://www.microsoft.com/security_essentials/default.aspx
- 與作業系統結合度高
- 可搭配Windows Defender 間諜軟體防護使用(Vista與Windows 7)
- 大仁校園主要防毒軟體

小紅傘 Avira Antivir Personal Free

- 下載網址：http://row.avira.com/zh-tw/pages/index.php
- 最多人使用的免費防毒軟體
- 可使用救援光碟
- 有廣告畫面

AVG

- 下載網址：http://www.avgtaiwan.com/
- 無廣告畫面
- 功能不因免費而有所縮減
- 救援光碟可使用

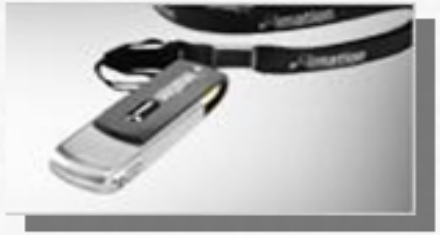
雲端防毒軟體-Immunet Protect

- 下載網址：
  http://www.immunet.com/free/index.html
- 第二套防毒軟體
  - 和其它防毒軟體一起安裝
- 雲端防毒
  - 用戶端不下載任何病毒碼資料庫，一切防護都是即時雲端同步完成
- 好友社群即時通報機制
- 基本上不需設定的設定
- 極度輕省快速的效能

間諜軟體偵測工具-Spybot

- 下載位址：http://www.safer-networking.org/ct/home/index.html
- 可有效偵測間諜軟體
- 具有免疫功能
- 資源耗費較大，不建議太老舊電腦安裝

硬體支援-Imation 高速防寫碟王



Imation高倍速隨身碟 磁碟分割 密碼保護　讓您擁有國安等級的防護

Imation USB 2.0 Swivel隨身碟具備有強大的應用功能，防寫設計、密碼保護、磁碟分割及格式化等超強功能一應俱全。您可將您的隨身碟分割成任意2個容量的區塊，其中一區由密碼保護，保存機密資料不外流。消費者不論在任何場合使用電腦，都可安心地保存專屬於自己的資料！為檔案攜帶及交流，公司簡報，照片，影音儲存的最佳選擇。

Imation USB 2.0 Swivel隨身碟，為一款可隨插即用的USB2.0高速傳輸隨身碟。記憶體採用SLC封裝技術，可重覆寫入資料10萬次，遠超過低價MLC 1萬次的寫入次數。最高容量4GB，適合儲存高解析度影音檔與圖檔；另外在美學設計上也有重大突破，機體輕盈小巧，即插即用，並且附贈USB延長線及頸帶方便隨身攜帶，永不掉蓋設計讓您不會遺失USB蓋，使用超方便。

全球資料儲存媒體的領導廠商Imation，除了在光碟燒錄上擁有相當大的市佔率，現更推出記憶卡及隨身碟等儲存產品，以滿足消費者在儲存管理重要資產上的更多選擇。

救援光碟

- 救援光碟是一套 Linux 架構的應用程式
- 可讓使用者存取已經無法開機的電腦
- 透過此系統修復受損的系統、拯救其中的資料或是掃描系統中的病毒感染項目
- 電腦須設定爲由光碟機開機才可進入救援模式