symantec™

Confidence in a connected world.

資訊安全講座
淺談資訊安全與網路安全威脅

藍允澤 / Danny Lan

上奇科技

電腦網路已深入每一個人的生活當中

- 政府機關
  - 個人身份資料、稅務資料、戶政資料 …
- 公共設施
  - 電力供給、瓦斯供給 …
- 金融機構
  - 股市交易、信用卡、存款 …
- 醫療機構
  - 病歷管理、維生系統、藥物管理 …
- 交通運輸
  - 交通控制中心、機場、車站 …
  - 飛機、高鐵、捷運 …
  - 自動導航、汽車電腦 …
- 通訊系統
  - 智慧型手機、交換機系統 …
- …

試想 …

- 當電腦網路出了差錯時?
  - 個人隱私外洩
  - 重要資料的遺失
  - 重要公共設施癱瘓
  - 金融交易無法進行造成的損失
  - 醫療安全問題
  - 交通安全受到影響
  - 通訊系統的癱瘓
  - …

駭客能做些什麼?


Music and Moonlight
Love and Romance
THERE MAY BE
TROUBLE AHEAD
HACKED

symantec™

Confidence in a connected world.

網路安全威脅的發展重點及未來發展趨勢

上奇科技

2008 年網路威脅重點趨勢

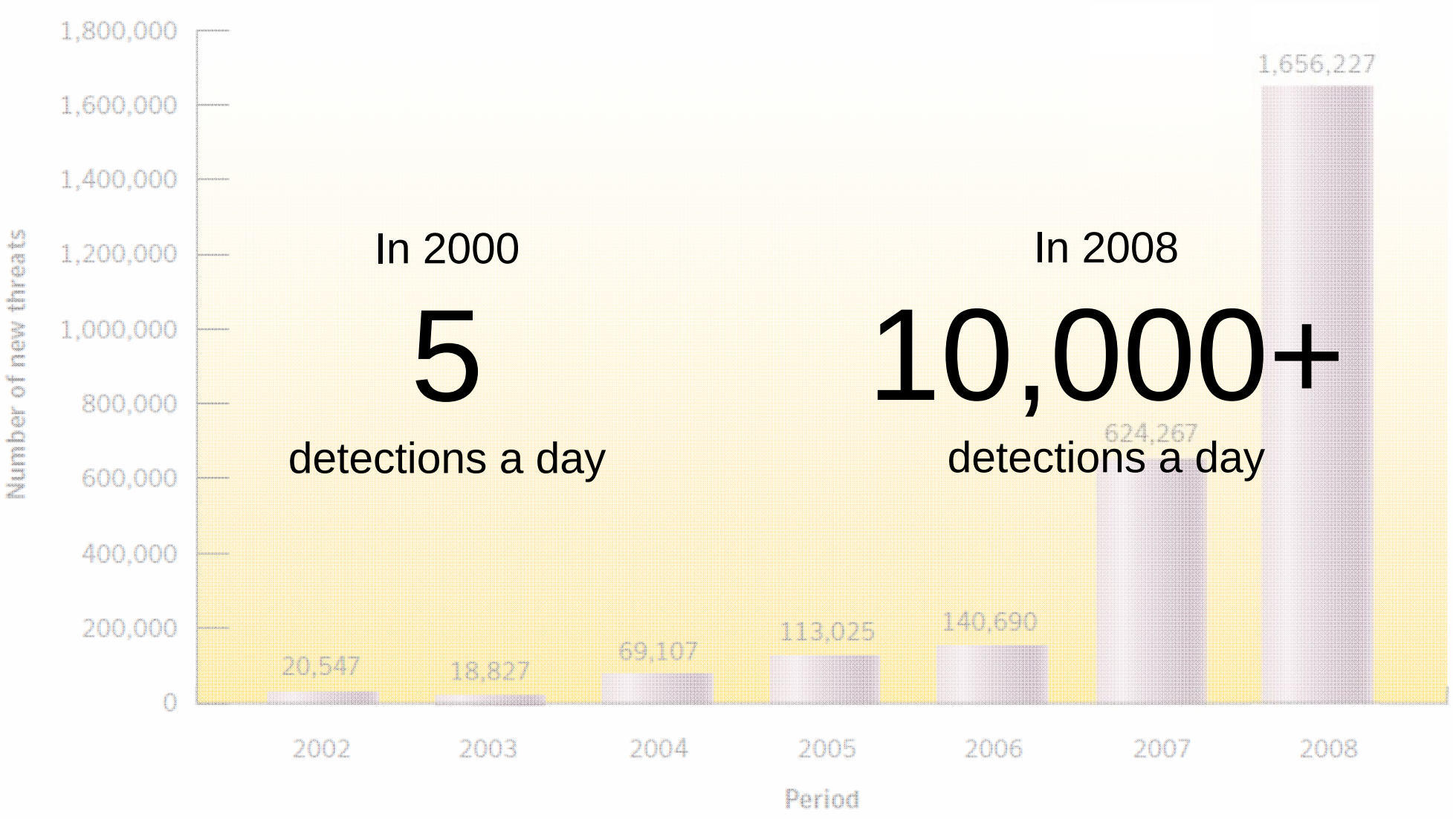
隨著特定國家的網際網路與寬頻成長起飛，其網路上惡意活動亦隨之提高

網頁式攻擊 **(web-based attack)** 爲目前惡意活動在網際網路上主要的攻擊媒介

攻擊者比起過去更注重在欺騙一般使用者，目的在於竊取個資以獲取金錢利益

即使面臨全球經濟景氣不振，地下經濟卻仍持續蓬勃發展

真的有那麼多的病毒嗎?



In 2000

5

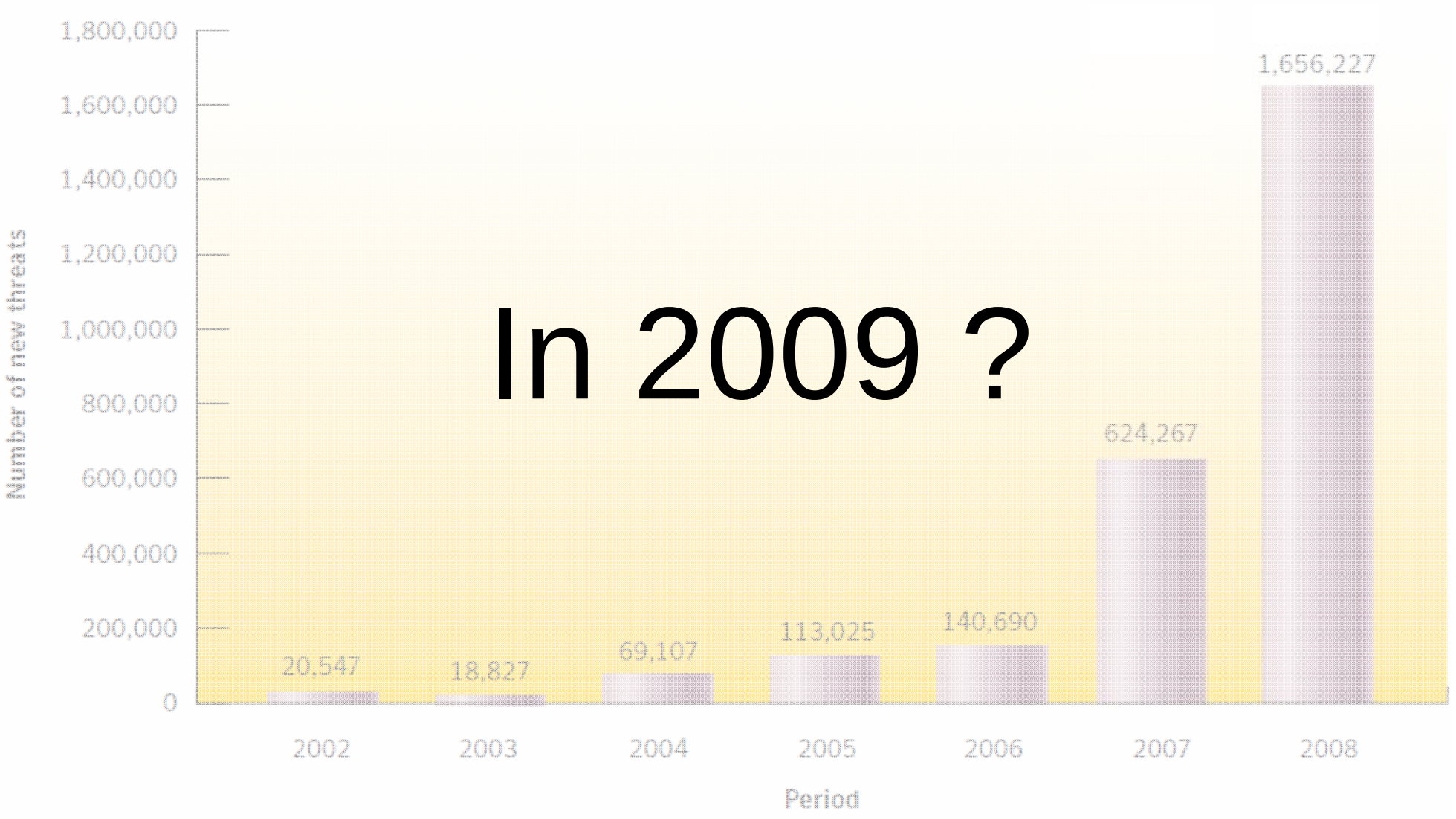
detections a day

In 2008

10,000+

detections a day

真的有那麼多的病毒嗎?


In 2009 ?
Number of new threats
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
20,547
18,827
69,107
113,025
140,690
624,267
1,656,227
2002
2003
2004
2005
2006
2007
2008
Period

2009 資安新聞回顧

- 蠕蟲竊金融個資 **900**萬電腦受駭 (2009/01/18 中時電子報)
- 駭客也搭歐巴馬熱　小心別中毒 (2009/01/21 法新社)
- 卡巴斯基美國網站遇駭 否認客戶資料外洩 (2009/02/10 ZDnet)
- **Adobe**遇駭 別開不明**PDF**檔 (2009/02/25 中時電子報)
- 駭客入侵網路相簿 正妹裸照外流 (2009/03/12 自由時報)
- 小心！ 假強風特報 真電腦病毒 (2009/03/18 中時電子報)
- 大陸鬼網竊機密　台灣受駭居第一 (2009/03/30 TVBS)
- 當心盜版蘋果軟體首支**Mac**殭屍網路程式出現 (2009/04/17 中廣新聞網)
- 麥可死訊熱門　**MSN** 機器人病毒手腳快　已大量散播 (2009/06/29 NOWnews)
- 駭客利用微軟漏洞攻擊逾千網站受害 (2009/07/07 中廣新聞網)

symantec™

Confidence in a connected world.

常見的網路安全威脅及入侵手法

上奇科技

常見的網路安全威脅

- 系統入侵 **(System Hacking)**
  - 利用各種技術手段或系統弱點，進入目的系統中取得存取權限並存取資料
- 惡意程式碼 **(Malicious Code)**
  - 利用程式感染檔案系統，以達到特定的攻擊目的
- 監聽 **(Sniffing)**
  - Sniffer - 利用技術監聽網路中的通訊內容
  - Keylogger - 利用技術紀錄主機上的所有輸入內容
- 服務阻斷 **(Denial of Service)**
  - 利用大量訊息攻擊主機，使主機無法正常運作
- 垃圾訊息 **(Spamming)**
  - 散播使用者不需要的訊息，達到廣告或攻擊的目的
- 網路釣魚 **(Phishing)**
  - 利用詐騙手法，騙取使用者的敏感性資料
- 社交工程 **(Social Engineering)**
  - 使用言語取得對方信任，以得到特定的資訊

symantec™ 上奇科技

網頁植入惡意程式碼嚴重威脅使用者

近一年國內資安危機 1866網站被駭

383網站遭植入惡意程式

記者王珮華／專題報導

瀏覽網站有多危險？根據資安之眼網站統計，過去一年內，被植入惡意程式的國內網站達383個，純粹遭入侵的網站則高達1,483個。其中發生資安危機次數最多的，爲台灣電子地圖服務網站，遭植入惡意連結；而公務機構如投資人保護中心，也曾遭植入惡意連結，對我國網路使用安全造成莫大威脅。

根據資安之眼網站（http://www.itis.tw/）統計，過去一年被駭客植入惡意程式最頻繁的網站包括：台灣電子地圖服務網、亞太固網寬頻、台安醫院、投資人保護中心、ESPN STAR體育台網站、Hinet理財網。而去年被入侵竄改網頁次數最多的網站，則有聲寶家電、台北市公寓大廈暨社區服務協會社區網、中央圖書館台灣分館與上閣屋餐飲集團首頁。

資安之眼站長BLUE表示，被駭客入侵所造成的損害，分爲幾個層次，輕則網頁被置換，宣示駭客實力；若進一步植入惡意程式，如木馬或間諜程式，只要使用者進入該網頁，就會在不知不覺中被植入惡意程式，或轉址到有惡意程式的網站。使用者被植入惡意程式後，日後在網路上的活動將被駭客一覽無遺，電腦被控制，帳號密碼很可能流出，個人資料也有曝光危險。

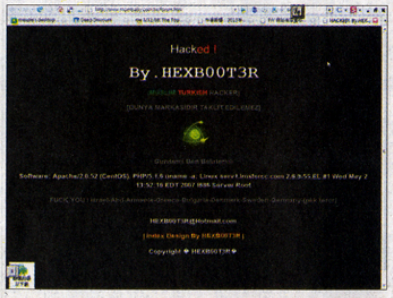
不過BLUE也提醒，資安之眼表列有資安威脅的網站，不代表使用者去瀏覽過一定有風險，其一是因網站獲知被入侵將會儘快修復；其次部分網站漏洞，是透過瀏覽器進行多樣的攻擊行爲，危害等級可大可小，因此建議使用者應作好電腦作業系統與防毒軟體的更新才能自保。

不幸名列第一的台灣電子地圖服務網站，表示確曾被植入惡意連結，但是去年6月的事情，現在早已修復完畢。該公司指出，去年年中有一波台灣網站被駭，全國最大電信業者Hinet也難倖免，爲此該公司建置入侵偵測系統，希望第一時間就化解駭客攻擊。

聲寶公司則表示，該公司官網在今年1月確實遭植入非官方網頁，但官網有防護措施，網友在瀏覽過程中並不會因此啓動該惡意網頁，也不會因此造成網友電腦被入侵。目前該惡意網頁已經移除，並加強防護措施。

資安之眼爲國內知名資訊安全資訊網站，其所提供的「TW網站淪陷資料庫」，主要資訊來源包括國際駭客組織網站Zone-h、Turk-h、搜尋引擎Google，以及專門通報資安事件的部落格「大砲開講」等國內外共九個資訊來源，站長本身也會自行偵測。

阿碼科技資安顧問邱銘泉表示，該站引述的資料來源均爲資安人員經常關注的網站，有一定的可信度。



國內網站遭駭客入侵頻傳，資訊安全問題備受重視。圖為國內知名婦幼雜誌討論區，日前遭駭客入侵置換首頁。（記者王珮華攝）

常上的網站 2成躲著木馬

【記者黃玉芳/台北報導】

網路詐騙猖獗，東森購物、奇摩拍賣、誠品網路書店陸續傳出個人資料外洩，「資安人雜誌」

防詐騙「三不二戒」

三不：

1.不想讓別人看到的資料盡量不要上網或存在電腦中。

台灣為亞太區第三大惡意程式碼攻擊國家

數位生活

文／商常發 圖／HP

台灣已進入高資訊化的社會，上網查詢資料、MSN連線、手機傳簡訊是一般大眾每日必須之作業。相對的資訊安全之防毒、防駭也是大眾最關心的議題。

賽門鐵克最新一期全球網路安全威脅研究報告，台灣為亞太區第三大惡意程式碼攻擊國家，同時也是本區中擁有第二多被傀儡程式所感染的電腦數，較上一期成長一倍以上，目前佔全地區約15%。

這份報告指出，2007年下半年網路威脅數量較上期飆漲468%，網頁應用程式攻擊已成為新的主流攻擊方式，而且社交網站已成為駭客攻擊最常利用的平台。台灣在亞太區擁有釣魚網站主機數量排名第五，金融性質網站為最常被利用。

業者表示，相對於網路攻擊行為，網頁應用程式已經成為主要的攻擊活動管道，越來越多的線上使用者僅因為造訪常去的網站而遭到感染。亞太區前10大新惡意程式碼樣本家族中，前三名都是針對網頁設定或瀏覽器首頁進行修改。

社交網站已成為最常被釣魚網站利用的靶子，在全球前4大釣魚網站國家中，最主要被利用的網站都是社交工程類。台灣排名第一的惡意程式碼是竊取線上遊戲帳號的Gamepass.Trojan木馬程式，台灣是回報這隻木馬程式頻率第二多的國家，僅次於中國大陸。

此外，利用網路工作、進行線上交易、收發電子郵件、上網購物血拼、找資料或玩Game，但一般使用者對網路安全還是缺乏深度認知，反而卻有許多令人發噱的想法，讓自己暴露在危險之下。

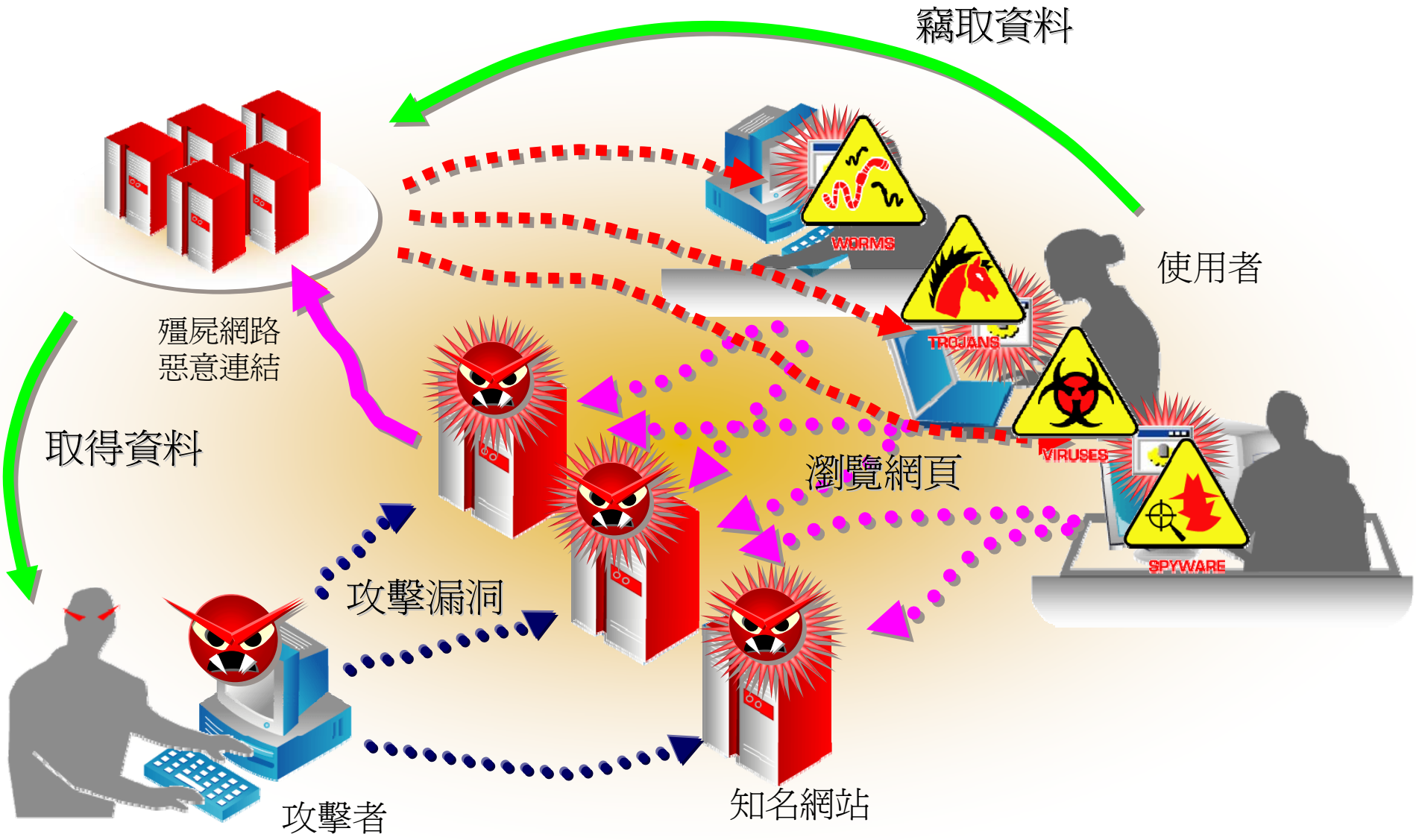
例如：「我有裝安全軟體就夠了！」錯！網路就是病毒散播的大本營，除了挑選有口碑、通過病毒公報（Virus Bulletin）最新發佈的VB 100%病毒偵測安全軟體外，安裝的軟體也要能夠對抗各式新興線上威脅，來保護IE瀏覽器或是FireFox瀏覽器，最好還能檢查家中無線網路的安全性等功能。

又如：「安全軟體裝兩套，一加一防護加倍？」這又錯了，如果同時安裝兩套安全軟體，反而可能會讓電腦產生強烈副作用，讓軟體或電腦無法正常運作，非但不能做出有效防護，反而營養過剩造成系統負擔，裝多不如裝好。

許多人以為「病毒數抓的多就是好的安全軟體？」這可不一定。由於每家防毒軟體定義病毒的標準不同，現代病毒變種多，同一隻病毒可以有眾多花名，所以選擇安全軟體的標準不再是看抓毒數量，而是要選擇全方位功能的安全軟體。

資料來源: 2008/3/26聯合晚報,2008/4/16中國時報,2008/4/25自由時報

駭客藉由網站散播惡意程式的手法(網頁掛馬)



什麼是隨身碟病毒?

- 什麼是隨身碟病毒?
  - 隨身碟病毒又稱 Autorun 病毒，是一種透過 autorun.inf 檔案以及作業系統的特性，經由 USB 隨身碟或外接式硬碟傳遞的惡意程式
- 隨身碟病毒的興起
  - 隨著 USB 隨身碟、外接式硬碟、儲存卡等移動式儲存裝置的普及，移動式儲存裝置已逐漸取代傳統的磁碟片，成爲最主要的檔案傳遞媒介
  - 自 Microsoft 推出 Windows XP 後，開始利用 autorun.inf 讓使用者可以在使用外接式裝置時，自動執行指定的指令以方便使用者
- 已知的隨身碟病毒
  - W32.Gammima.AG (KAVO)
  - W32.Downadup.B (Conficker、Kido)
  - …

隨身碟病毒的運作原理

- 隨身碟病毒的運作原理
  - 當使用者使用隨身碟時，作業系統會立刻尋找隨身碟中的 autorun.inf 檔案，並且根據 autorun.inf 裡的內容，執行相對應的程式或指令

隨身碟病毒的行爲解析

- 惡意程式透過網頁或其他管道進入使用者的電腦
- 使用者插入USB 隨身碟時
  - 惡意程式將 Autorun.inf 及惡意執行檔寫入 USB 隨身碟裝置
  - 當使用者將 USB 隨身碟插入其他電腦時
    - 系統讀取 Autorun.inf 中的指令執行指定的惡意執行檔
    - 產生惡意執行檔至指定的系統資料夾
    - 修改系統登錄檔使電腦於開機時自動執行
    - 修改系統登錄檔不允許檔案總管顯示隱藏檔案

隨身碟病毒的安全性影響

- 最令人感到困擾的傳播途徑
  - 結合社交工程手法
  - 由相互認識的人傳遞，警戒心會降低
  - 利用使用者要求使用便利的目的
  - 藉由作業系統的自動執行功能
- 任何病毒都可以利用隨身碟傳遞

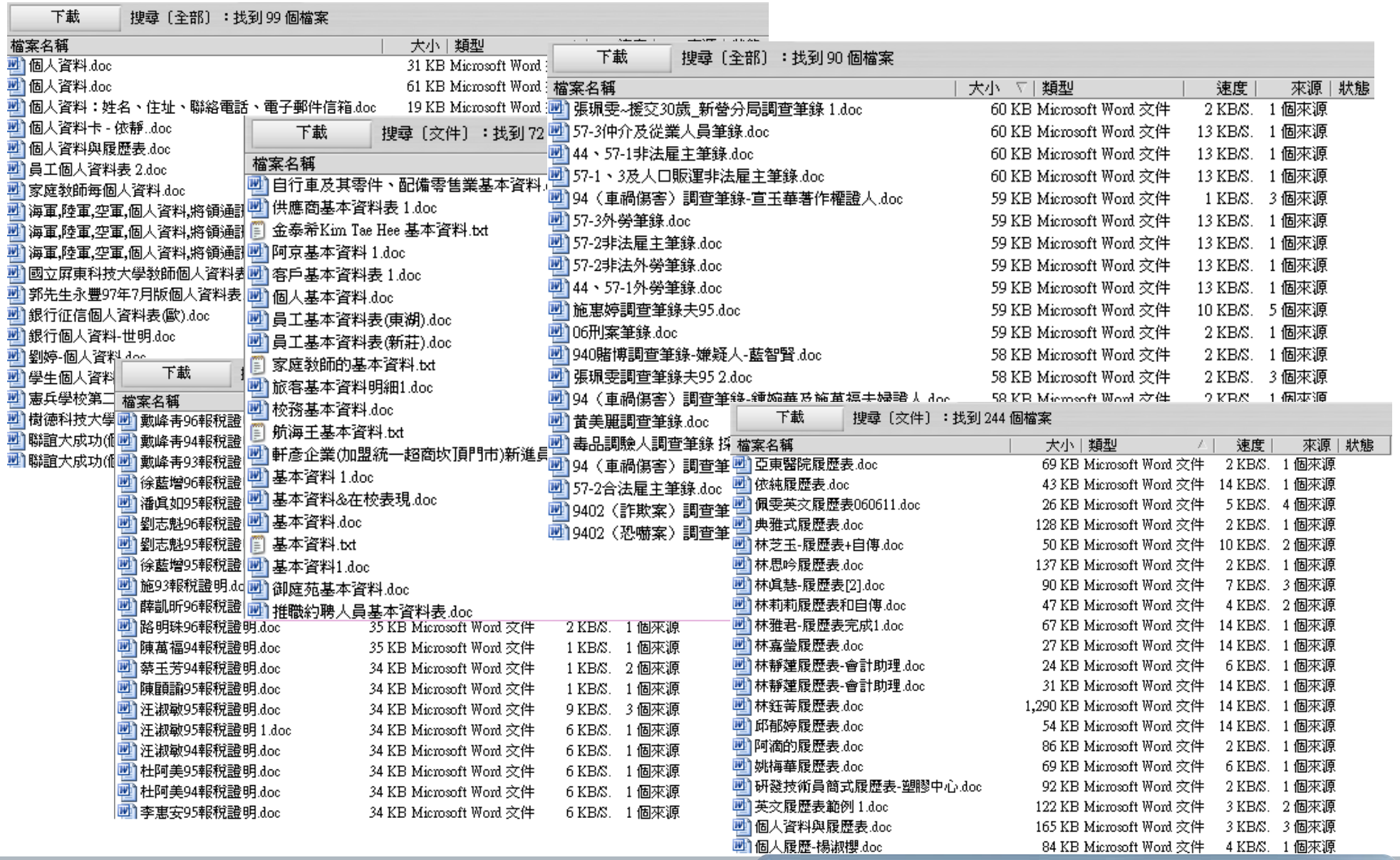
symantec™

Confidence in a connected world.

個人資料外洩與保護

上奇科技

電腦的使用不當造成資料外洩

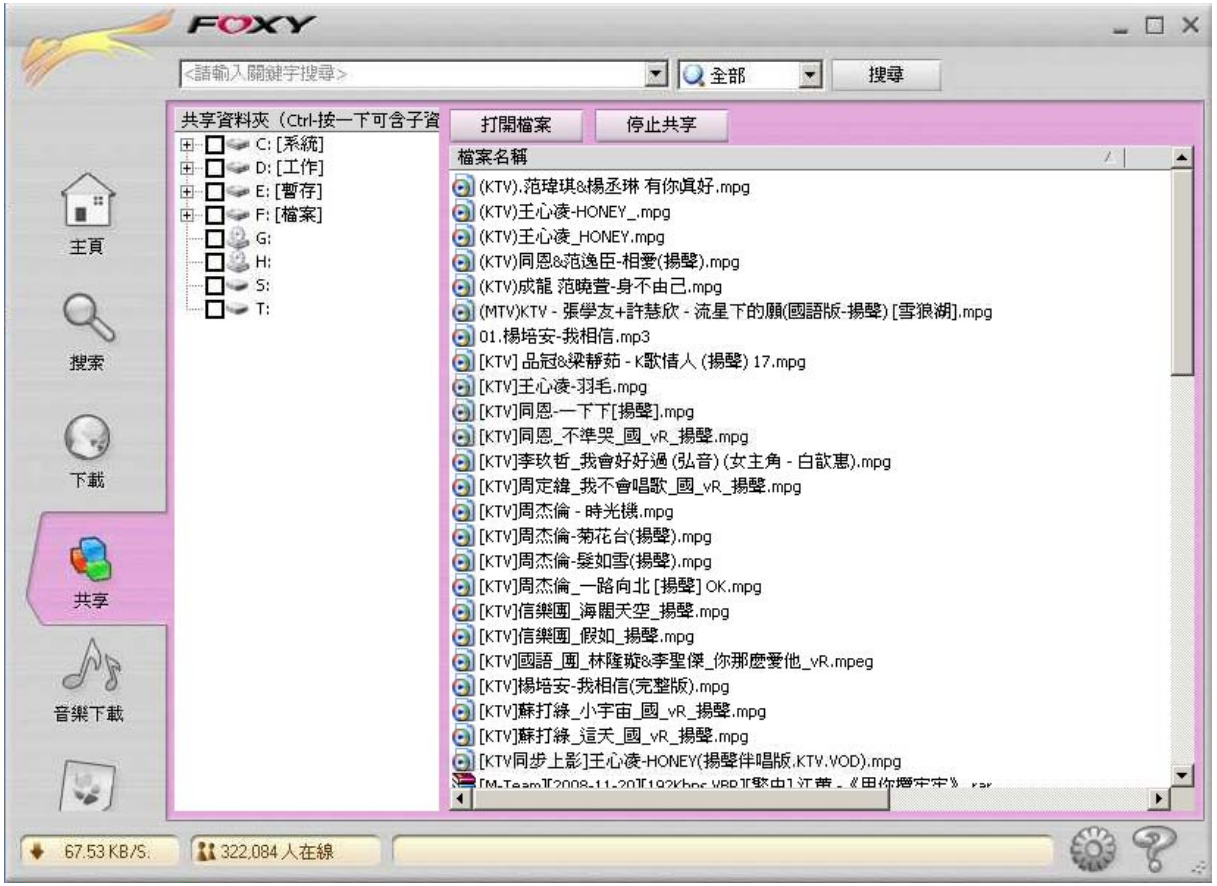


網路上什麼都有

- 您知道您的資料已經上網了嗎?
- 網路上可以找得到的東西比您想像中還要多

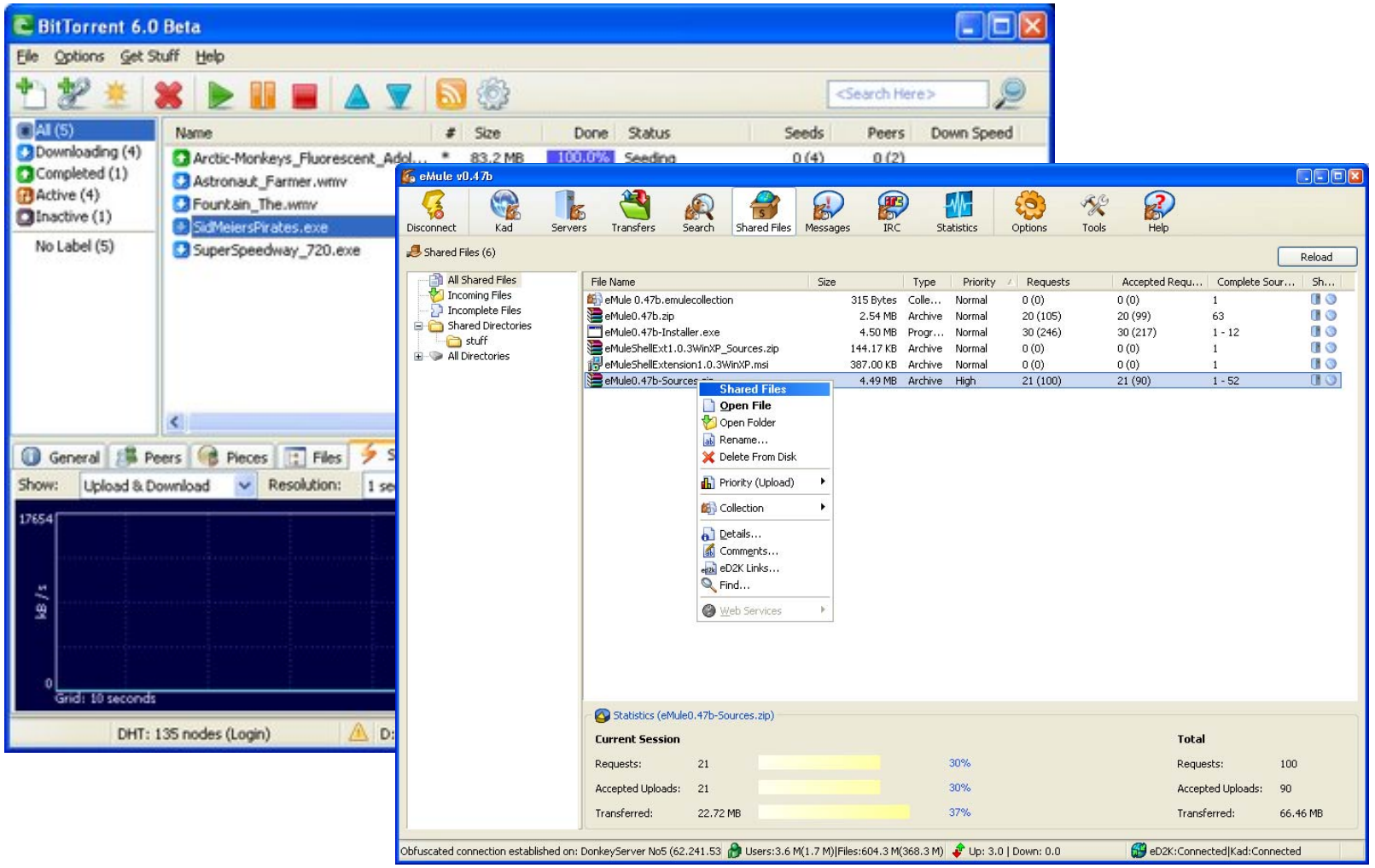
P2P 檔案共享軟體的秘密

- 什麼是 P2P 檔案共享軟體?
  - P2P 是 Peer-to-Peer 的簡寫，意思就是參與其中的所有角色都是平等互惠的，由所有的使用者直接互相分享。
- 使用檔案共享軟體的風險
  - 會共享預設資料夾中的檔案
  - 會無限制的使用頻寬
  - 無法過濾下載的檔案來源
- 如何安全使用檔案共享軟體
  - 不常駐
  - 使用頻寬控管軟體
  - 不任意下載來路不明的檔案



常見的 P2P 檔案共享軟體

- BitTorrent
- eMule
- FOXY



symantec™

Confidence in a connected world.

如何加強個人的網路安全防護降低風險

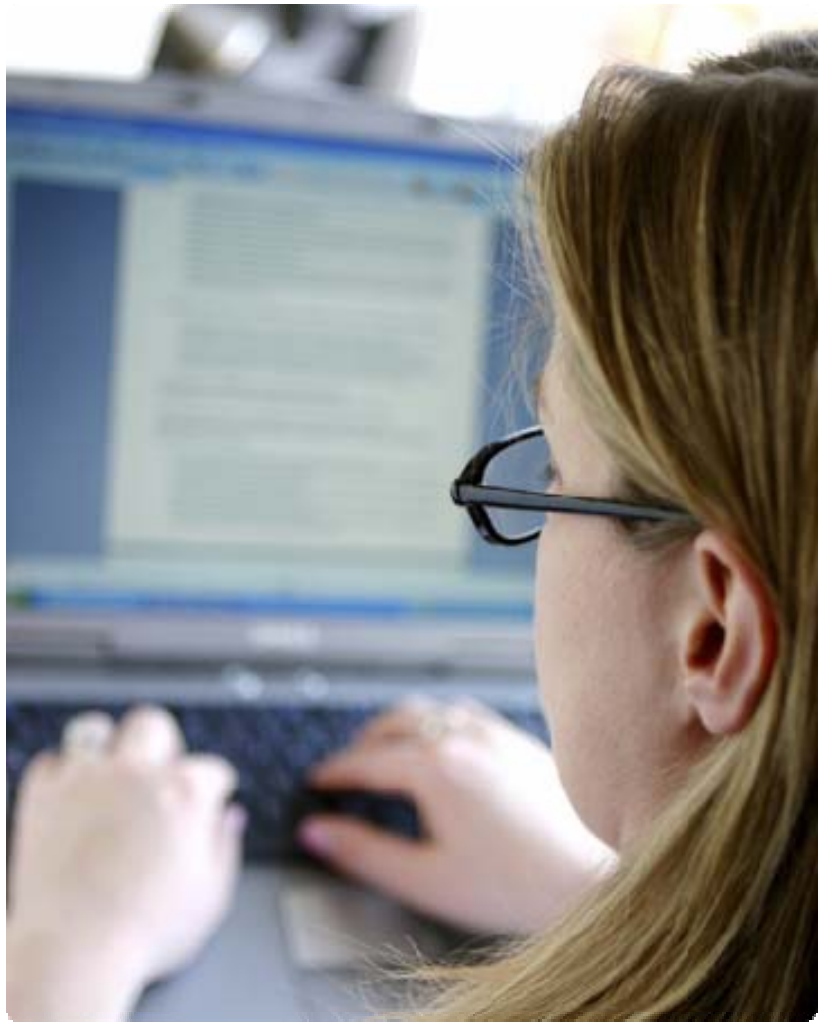
上奇科技

爲什麼會中毒?

- 使用者沒有建立良好的使用習慣
  - 未確認就開啓來路不明的檔案或網路連結
  - 使用來路不明或未合法授權的程式
  - 瀏覽高風險的網站
  - 沒有設定密碼或使用容易猜測的密碼
  - 下載來路不明的檔案
- 未修補系統所存在的弱點
  - Service Pack
  - Security Patch
- 沒有使用個人防火牆
  - 系統中開啓了不必要的通訊埠
- 沒有安裝防毒軟體
  - 未更新病毒定義檔
  - 使用過舊的防毒軟體

輕鬆對抗電腦病毒及惡意軟體

- 建立良好的使用習慣
- 隨時保持系統軟體在最新狀態
  - Windows Update
  - Service Pack
- 使用個人防火牆
  - Windows XP SP2
  - Windows Vista
  - 含有個人防火牆的防毒軟體
- 使用最新的防毒軟體
  - 定期更新病毒定義檔
  - 定期掃描



良好的使用習慣

- 不開啓來路不明的電子郵件
- 不瀏覽風險較高的網站
- 再三確認網址，避免使用超連結
  - 超連結的真面目
    - <A HREF="http://www.symantec.com.tw">http://www.symantec.com.tw</A>
  - 駭客喜歡玩的文字遊戲
    - www.citibank.com.tw 與 www.citybank.com.tw
    - www.paypal.com 、 www.paypal.com 與 www.paypa1.com
- 絕不下載或開啓來路不明的檔案
  - 圖片、影片、MP3
  - 壓縮檔
  - Word、Excel
- 不使用來路不明的軟體
  - 有趣的小遊戲
  - 免費軟體或共享軟體
  - 盜版軟體、好用的工具

強化系統的防護能力

- 使用個人防火牆
  - 防止惡意連結透過未使用到的通訊埠連線
  - 使用IP分享器或建立DMZ區域
    - 隔離內部系統與網路，使外界不容易找到內部的系統
- 隨時保持系統軟體在最新狀態
  - Service Pack
  - Security Patch
- 移除或停用沒有用到的軟體
- 使用最新的防毒軟體
  - 定期更新病毒定義檔
  - 定期掃描
- 使用複雜度及強度高的密碼
- 定時備份重要資料

您的密碼安全嗎?

/ Run \ Report \

Domain	User Name	LM Password	<8	Password	Audit Time	Method	Password Age (days)
WINXPPRO	Administrator	PASSWORD		password	0d 0h 0m 1s	Dictionary	0
WINXPPRO	dannylan	X06MP3YK6		x06mp3yk6	0d 19h 1m 14s	Brute Force	0
WINXPPRO	Emma	5057	x	5057	0d 0h 2m 48s	Brute Force	0
WINXPPRO	Frank	Q1W@E3	x	q1W@e3	0d 0h 28m 56s	Brute Force	0
WINXPPRO	GrandTech	GRANDTECH		GrandTech	0d 0h 0m 0s	User Info	0
WINXPPRO	Guest	*empty*	x	*empty*			0
WINXPPRO	Symantec	SYMANTEC@123		Symantec@123	0d 0h 3m 19s	Brute Force	0

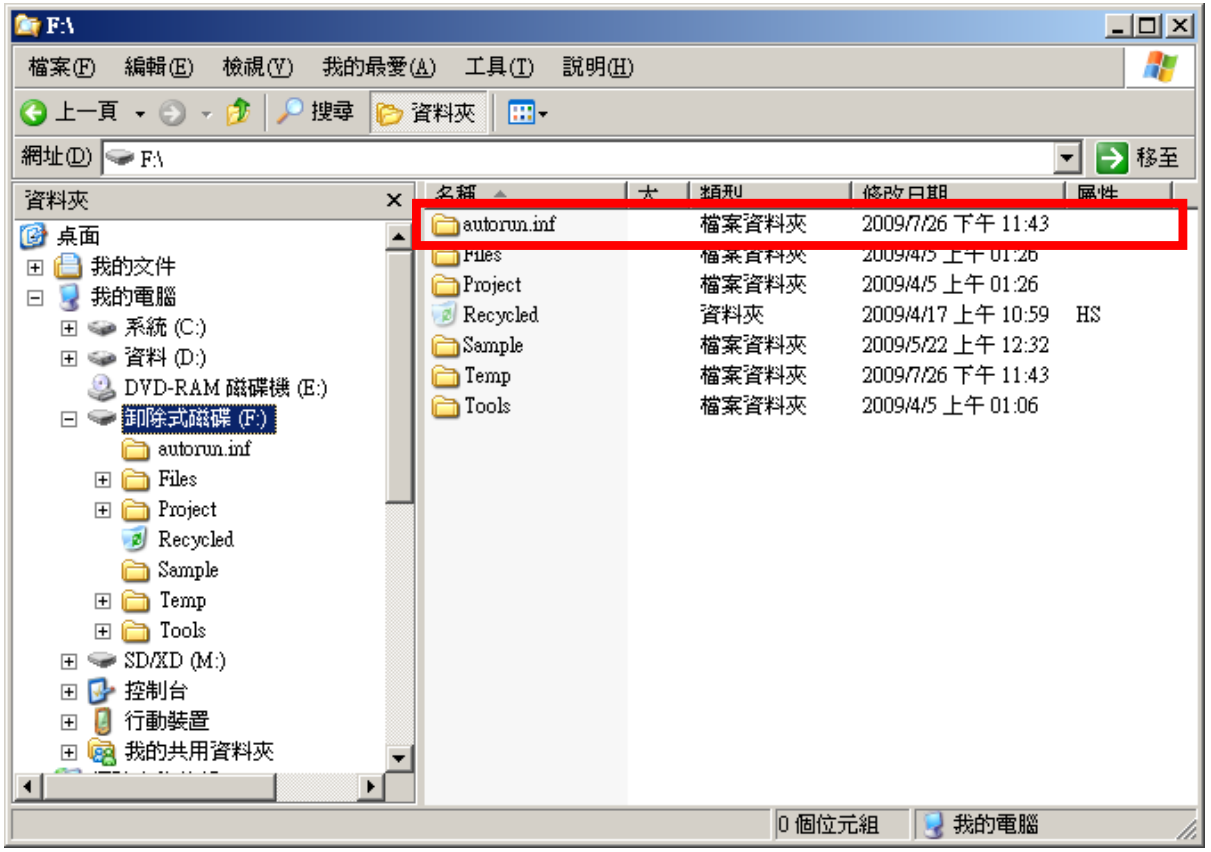
- 安全性低的密碼只需要數分鐘就能輕易破解
- 駭客或病毒會先從 Administrator 帳號進行密碼猜測
  - 通常一般使用者都沒有設定此帳號的密碼或密碼過於簡單
- 字典檔已內建上萬組的密碼組合，其中包含一般人經常設定的密碼組合
  - 0000、123456、password ...

使用安全性高的密碼

- 必須包含英文字母、數字與特殊字元，英文字母須含大小寫
  - 特殊字元爲：!@#$%^&*...等符號
  - 英文字母不可爲有意義的單字，例如名字或是單位名稱
- 密碼長度建議在 8 位數以上
- 需注意經常性的替換密碼 (約莫90天換一次)
- 如何設定一個複雜度及強度高，又容易記住的密碼
  - 善用中文輸入法的優勢

如何防治隨身碟病毒

- 避免系統被植入隨身碟病毒
  - 關閉自動執行或自動播放功能
- 避免隨身碟或外接式硬碟被植入病毒
  - 在隨身碟或外接式磁碟中建立一個名爲 autorun.inf 的資料夾



symantec™

Confidence in a connected world.

我中毒了嗎?

上奇科技

我的電腦中毒了嗎?

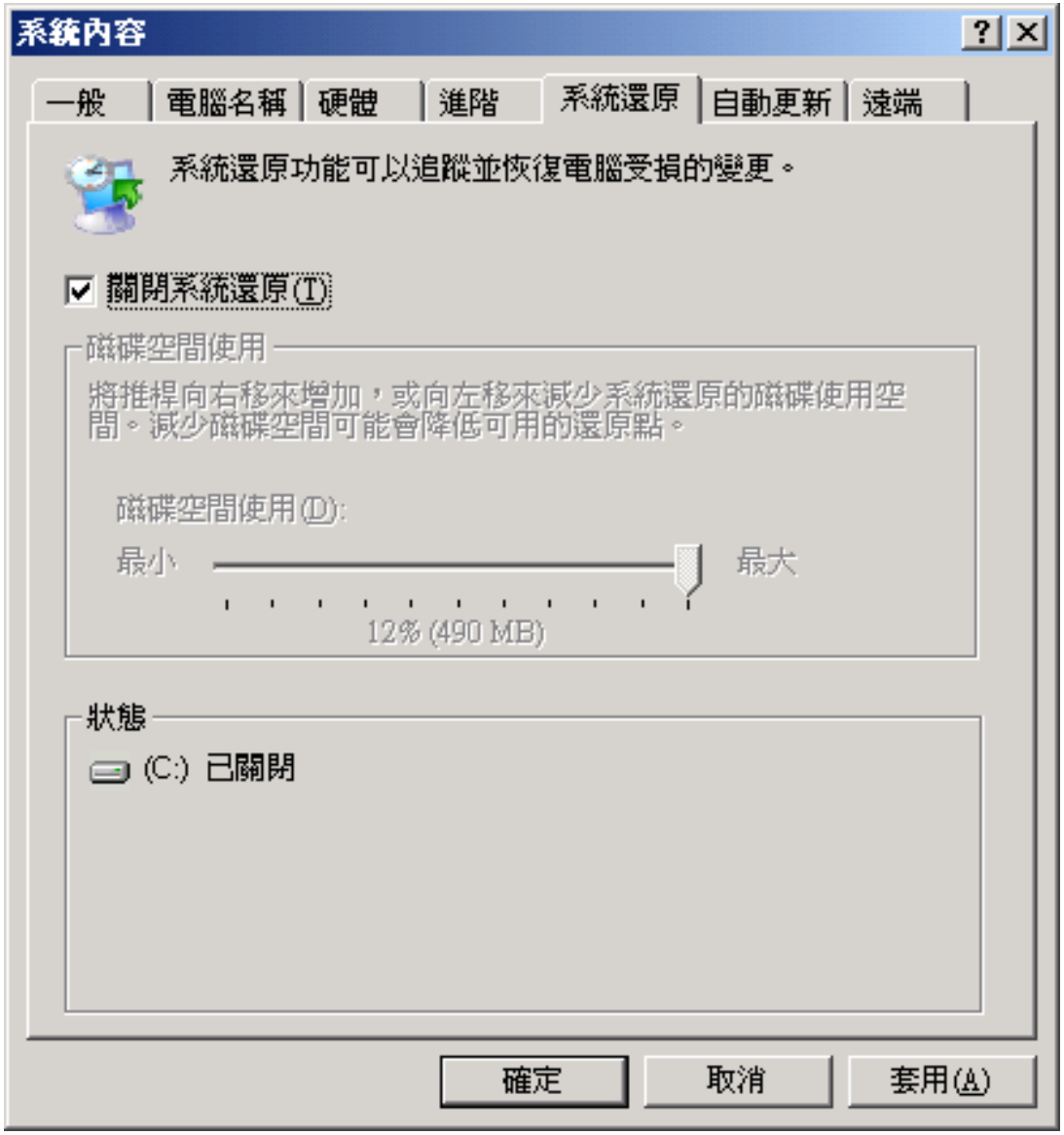
- 即使是防毒專家也無法告訴您正確的答案
- 這些都有可能是中毒也都有可能不是
  - 無法開機?
  - 電腦或網路變慢了?
  - 一直跳出奇怪的錯誤訊息?
  - 硬碟裡多了一堆奇怪的檔案?
  - 程式或防毒軟體無法正常執行?
  - 系統設定被更改而且無法恢復原來的設定?
  - 系統中被安裝了來路不明的程式?
  - …

防毒軟體告訴我發現病毒了怎麼辦?

- 大多數的環境下，防毒軟體會在偵測到已知的可疑威脅時跳出訊息通知使用者。您可以依據訊息中的資訊了解：病毒名稱、檔案位置、發現時間、採取動作
- 所以我中毒了嗎??
  - 跳出訊息表示已偵測到可疑的惡意活動
  - 在正常情況下，防毒軟體會直接攔截病毒的活動
- 我該怎麼做?
  - 通常只需要持續觀察
  - 如果持續跳出訊息或有疑似中毒症狀
    - 可能有未知的病毒存在
    - 通報管理人員協助處理

不小心中毒了怎麼辦?

- 立即拔除網路線避免感染其他電腦
- 關閉系統還原功能
- 使用乾淨的開機環境開機
  - 使用開機磁片或光碟
  - 進入安全模式(SAVE MODE)
  - 將硬碟安裝到其他乾淨的主機
- 使用防毒軟體掃毒
  - 線上掃毒
    - http://security.symantec.com
- 請專業人員協助處理
  - 系統維護廠商
  - 防毒軟體廠商



防毒軟體的迷思：防毒軟體真的有效嗎?

- 防毒軟體真的有效嗎?
  - 單然有，但是效果很有限
  - 以目前病毒推陳出新的速度，沒有單一公司能做到完全保護
- 防毒軟體的困境
  - 永遠都有新的威脅，且病毒的變種速度與種類不斷增加
    - 病毒使用加殼壓縮及隱匿技術逃避偵測，舊的技術無法處理新一代的病毒
  - 防毒軟體必須仰賴病毒定義檔才能發揮作用
    - 先發現病毒才會病毒定義檔，且目標式攻擊的病毒樣本收集不易
  - 無法有效清除已被感染病毒的系統
  - 防毒軟體無法防禦網路攻擊行爲
  - 防毒軟體可能會誤判
    - 有抓到病毒的防毒軟體不一定就是好的防毒軟體
      - Windows Explorer 被防毒軟體誤判爲惡意程式 (2007-12)
      - Windows 重要元件(lsasrv.dll)被誤判爲惡意程式導致系統當機 (2007-06)
  - 防毒軟體也有可能成爲被攻擊的目標

面對未來的網路安全威脅應該有的認知

- 「世界上沒有永遠安全的系統」 --- Kevin D. Mitnick
  - 要設計出完美無缺的系統是不可能的
  - 任何系統或軟體都有被攻擊的機會
  - 單單依靠防毒軟體以及閘道端的防護，已不足以應付今日的威脅
    - W32.Blaster.Worm (2003.08.11) – 個人防火牆及入侵偵測系統
    - W32.Gammima.AG (2007.08.27) – 應用程式控管及裝置控管
- 資訊安全是現代每一個人都必須關心的議題
  - 大多數的使用者還存在「不會這麼倒楣」的心態
  - 駭客對於攻擊目標的價值與我們所想的不同
  - 個人的不在意可能會造成不可收拾的後果
- 如何做到真正的安全?
  - 良好的習慣
  - 適當的防護
  - 定時的更新

symantec™

Confidence in a connected world.

Thank you!

dannylan@pixnet.net
http://security.magicworks.net

上奇科技