



Confidence in a connected world.



淺談網路威脅發展新趨勢 個人如何輕鬆對抗網路安全威脅

藍允澤 / Danny Lan



上奇科技



CONTENT

- 網路安全威脅的發展趨勢
- 常見的網路安全威脅及入侵管道
- 如何加強個人網路安全防護降低安全風險
- 我中毒了該怎麼辦？



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 ...
- ...





資訊安全跟我們有什麼關係？

- 試想，當電腦網路出了差錯時？
 - 個人隱私及重要資料的外洩
 - 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



Confidence in a connected world.



網路安全威脅的發展重點及未來發展趨勢



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**) 為目前惡意活動在網際網路上主要的攻擊媒介



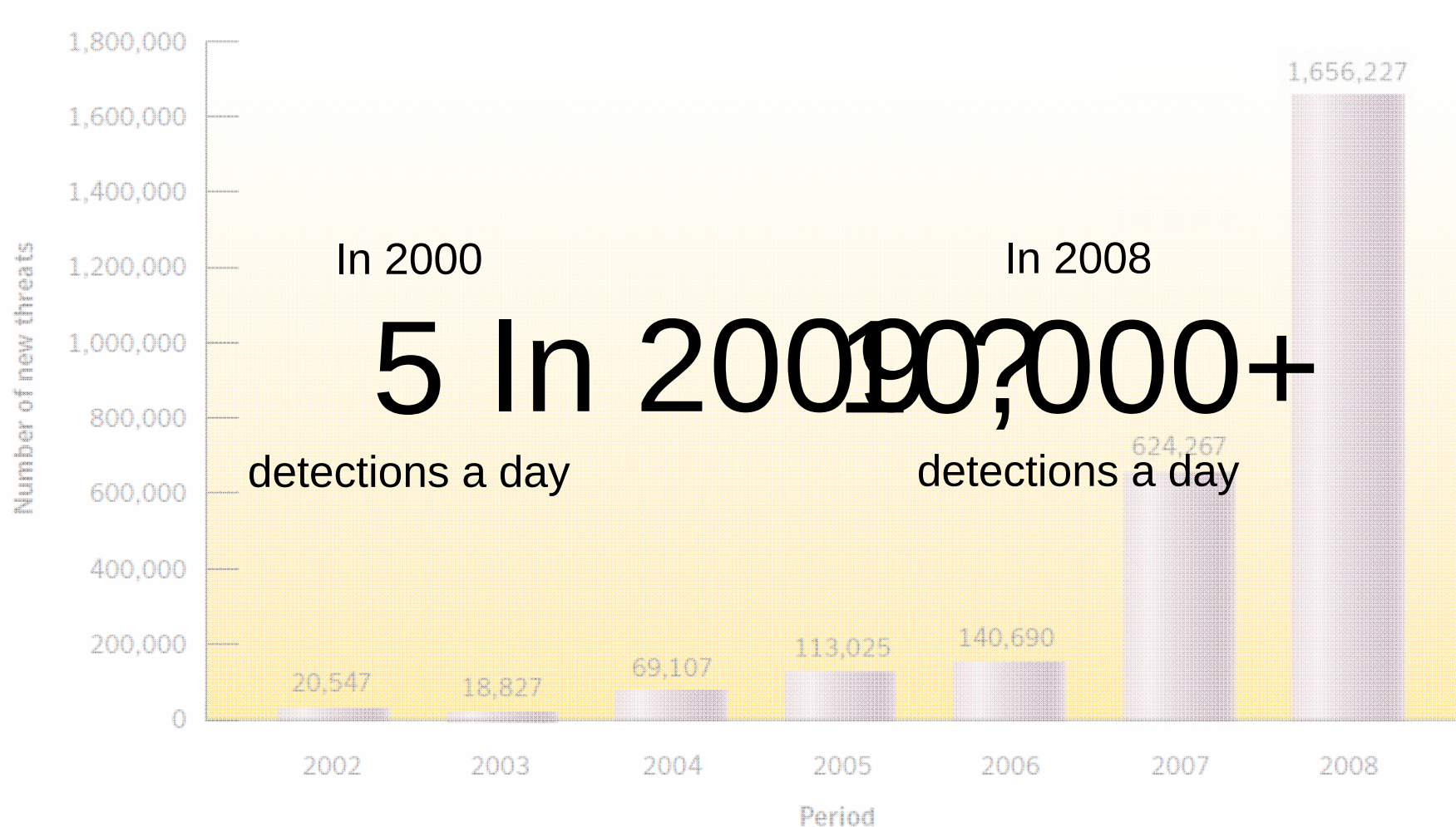
攻擊者比起過去更注重在欺騙一般使用者，目的在於竊取個資以獲取金錢利益



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？





網路安全問題層出不窮

自由電子報 - 駭客入侵網路相簿 正妹裸照外洩 - Windows Internet Explorer

http://www.libertytimes.com.tw/2009/new/mar/12/today

自由電子報 - 駭客入侵網路相簿 正妹裸照外洩

自由時報 電子報

The Liberty Times · 社會新聞

自由新聞 | 影音娛樂 | 讀者園地 | 旅遊玩樂

- 頭版新聞
- 證券表格
- 焦點新聞
- 政治新聞
- 社會新聞
- 生活新聞
- 國際新聞
- 愛心暖流
- 自由言論
- 爆料投訴
- 財經新聞
- 體育新聞
- 運動彩券
- 教育新聞
- 健康醫療
- 地方新聞
- 影視名人
- 流行消費

首頁 > 社會新聞

2009-3-12

駭客入侵網路相簿 正妹裸照外洩

【記者劉慶侯、王珮華／台北報導】「百大正妹」排行榜名單，成為駭客入侵網路相簿，正妹裸照外洩，流到色情網。

Q1台灣電腦中毒近3500萬次 USB病毒最毒-Yahoo!奇摩新聞 - Windows Internet Explorer

http://tw.news.yahoo.com/article?url/d/a/090413/58/1hne.html

Q1台灣電腦中毒近3500萬次 USB病毒最毒-Yahoo...

YAHOO! 奇摩新聞

會員登入
新使用者? 立即註冊

新聞 | 網頁

新聞首頁 | 政治 | 社會 | 地方 | 國際 | 財經 | 科技 | 運動 | 健康 | 教育 | 藝文 | 影劇 | 旅遊 | 生活 | 全民話頭

資訊3C | 科學發展 | 自然環境 | 照片故事 | 專輯 | 領袖專訪 | 民調中心 | 雜誌 | 6行動愛地球 | 冷氣選購指南

2009

新聞首頁 > 科技 > 資訊3C > 央廣

寄給朋友 | 友善列印 | 字級設定: 小 中 大 巨

Q1台灣電腦中毒近3500萬次 USB病毒最毒

更新日期: 2009/04/13 18:27 韓啟賢

資安廠商公佈的報告顯示，今年第一季台灣總共有近3500萬次電腦病毒感染案例，約比去年第四季增加了一成，比去年同期成長將近300%。在各類別的電腦病毒中，以USB病毒最毒，因為台灣第一季的十大病毒中，感染前兩名的病毒就是USB病毒。

資安廠商趨勢科技公布的報告指出，台灣今年第一季總共有3443萬多次的電腦遭受病毒感染案例報告，這個數量大約是去年全台灣總感染數量的四成七，和去年第四季相比，增加了將近一成；與去年同期相比，感染總數則成長高達297%。

完成

網際網路 100%

即使是瀏覽知名網站也會有風險





電腦的使用不當造成資料外洩

下載

搜尋 [全部] : 找到 99 個檔案

檔案名稱	大小	類型
個人資料.doc	31 KB	Microsoft Word
個人資料.doc	61 KB	Microsoft Word
個人資料: 姓名、住址、聯絡電話、電子郵件信箱.doc	19 KB	Microsoft Word
個人資料卡 - 依靜.doc		
個人資料與履歷表.doc		
員工個人資料表 2.doc		
家庭教師每個人資料.doc		
海軍,陸軍,空軍,個人資料,將領通計		
海軍,陸軍,空軍,個人資料,將領通計		
海軍,陸軍,空軍,個人資料,將領通計		
國立屏東科技大學教師個人資料表		
郭先生永豐97年7月版個人資料表		
銀行征信個人資料表(歐).doc		
銀行個人資料-世明.doc		
劉婷-個人資料.doc		
學生個人資料		
憲兵學校第二		
樹德科技大學		
聯誼大成功		
聯誼大成功		
徐藍增96報稅證		
潘真如95報稅證		
劉志魁96報稅證		
劉志魁95報稅證		
徐藍增95報稅證		
施93報稅證明.doc		
薛凱昕96報稅證		
昭明珠96報稅證明.doc		
陳萬福94報稅證明.doc		
蔡玉芳94報稅證明.doc		
陳韻諤95報稅證明.doc		
汪淑敏95報稅證明.doc		
汪淑敏95報稅證明 1.doc		
汪淑敏94報稅證明.doc		
杜阿美95報稅證明.doc		
杜阿美94報稅證明.doc		
李惠安95報稅證明.doc		

下載

搜尋 [文件] : 找到 72 個檔案

檔案名稱	大小	類型
自行車及其零件、配備零售業基本資料		
供應商基本資料表 1.doc		
金泰希Kim Tae Hee 基本資料.txt		
阿京基本資料 1.doc		
客戶基本資料表 1.doc		
個人基本資料.doc		
員工基本資料表(東湖).doc		
員工基本資料表(新莊).doc		
家庭教師的基本資料.txt		
旅客基本資料明細1.doc		
校務基本資料.doc		
航海王基本資料.txt		
軒彥企業(加盟統一超商坎頂門市)新進員		
基本資料 1.doc		
基本資料&在校表現.doc		
基本資料.doc		
基本資料.txt		
基本資料1.doc		
御庭苑基本資料.doc		
推職約聘人員基本資料表.doc		
35 KB Microsoft Word 文件	2 KB/S	1 個來源
35 KB Microsoft Word 文件	1 KB/S	1 個來源
34 KB Microsoft Word 文件	1 KB/S	2 個來源
34 KB Microsoft Word 文件	1 KB/S	1 個來源
34 KB Microsoft Word 文件	9 KB/S	3 個來源
34 KB Microsoft Word 文件	6 KB/S	1 個來源
34 KB Microsoft Word 文件	6 KB/S	1 個來源
34 KB Microsoft Word 文件	6 KB/S	1 個來源
34 KB Microsoft Word 文件	6 KB/S	1 個來源

下載

搜尋 [全部] : 找到 90 個檔案

檔案名稱	大小	類型	速度	來源	狀態
張佩雯-援交30歲_新營分局調查筆錄 1.doc	60 KB	Microsoft Word 文件	2 KB/S	1 個來源	
57-3仲介及從業人員筆錄.doc	60 KB	Microsoft Word 文件	13 KB/S	1 個來源	
44、57-1非法屋主筆錄.doc	60 KB	Microsoft Word 文件	13 KB/S	1 個來源	
57-1、3及人口販運非法屋主筆錄.doc	60 KB	Microsoft Word 文件	13 KB/S	1 個來源	
94〈車禍傷害〉調查筆錄-宣玉華著作權證人.doc	59 KB	Microsoft Word 文件	1 KB/S	3 個來源	
57-3外勞筆錄.doc	59 KB	Microsoft Word 文件	13 KB/S	1 個來源	
57-2非法屋主筆錄.doc	59 KB	Microsoft Word 文件	13 KB/S	1 個來源	
57-2非法外勞筆錄.doc	59 KB	Microsoft Word 文件	13 KB/S	1 個來源	
44、57-1外勞筆錄.doc	59 KB	Microsoft Word 文件	13 KB/S	1 個來源	
施惠婷調查筆錄夫95.doc	59 KB	Microsoft Word 文件	10 KB/S	5 個來源	
06刑案筆錄.doc	59 KB	Microsoft Word 文件	2 KB/S	1 個來源	
940賭博調查筆錄-嫌疑人-藍智賢.doc	58 KB	Microsoft Word 文件	2 KB/S	1 個來源	
張佩雯調查筆錄夫95 2.doc	58 KB	Microsoft Word 文件	2 KB/S	3 個來源	
94〈車禍傷害〉調查筆錄-鍾施華及施施福夫婦證人.doc	58 KB	Microsoft Word 文件	2 KB/S	1 個來源	
黃美麗調查筆錄.doc					
毒品調驗人調查筆錄					
94〈車禍傷害〉調查筆					
57-2合法屋主筆錄.doc					
9402〈詐欺案〉調查筆					
9402〈恐嚇案〉調查筆					
亞東醫院履歷表.doc	69 KB	Microsoft Word 文件	2 KB/S	1 個來源	
依純履歷表.doc	43 KB	Microsoft Word 文件	14 KB/S	1 個來源	
佩雯英文履歷表060611.doc	26 KB	Microsoft Word 文件	5 KB/S	4 個來源	
典雅式履歷表.doc	128 KB	Microsoft Word 文件	2 KB/S	1 個來源	
林芝玉-履歷表+自傳.doc	50 KB	Microsoft Word 文件	10 KB/S	2 個來源	
林恩吟履歷表.doc	137 KB	Microsoft Word 文件	2 KB/S	1 個來源	
林真慧-履歷表[2].doc	90 KB	Microsoft Word 文件	7 KB/S	3 個來源	
林莉莉履歷表和自傳.doc	47 KB	Microsoft Word 文件	4 KB/S	2 個來源	
林雅君-履歷表完成1.doc	67 KB	Microsoft Word 文件	14 KB/S	1 個來源	
林嘉堂履歷表.doc	27 KB	Microsoft Word 文件	14 KB/S	1 個來源	
林靜蓮履歷表-會計助理.doc	24 KB	Microsoft Word 文件	6 KB/S	1 個來源	
林靜蓮履歷表-會計助理.doc	31 KB	Microsoft Word 文件	14 KB/S	1 個來源	
林鈺菁履歷表.doc	1,290 KB	Microsoft Word 文件	14 KB/S	1 個來源	
邱郁婷履歷表.doc	54 KB	Microsoft Word 文件	14 KB/S	1 個來源	
阿滴的履歷表.doc	86 KB	Microsoft Word 文件	2 KB/S	1 個來源	
姚梅華履歷表.doc	69 KB	Microsoft Word 文件	6 KB/S	1 個來源	
研發技術員簡式履歷表-塑膠中心.doc	92 KB	Microsoft Word 文件	2 KB/S	1 個來源	
英文履歷表範例 1.doc	122 KB	Microsoft Word 文件	3 KB/S	2 個來源	
個人資料與履歷表.doc	165 KB	Microsoft Word 文件	3 KB/S	3 個來源	
個人履歷-楊淑嫻.doc	84 KB	Microsoft Word 文件	4 KB/S	1 個來源	



個人資料外洩問題日趨嚴重

 **新聞專區**

Search

[首頁](#) [企業軟體](#) [企業硬體](#) [網路/通訊](#) [數位產品](#) [新聞](#)

 **超過400種新功能，
Visual Studio 2005讓你耳目一新**

[重新播放](#)

[3C風雲產品第一名](#) [刀鋒六訣縱橫江湖](#)

最後更新：2007/04/20 09:42 PM [SAVED STORIES 1](#)

惡意程式、內容冒充外洩筆錄鑽進Foxy用戶PC

記者馬培治／台北報導 18/04/2007

專家警告，有假檔案搭著警方筆錄外洩新聞事件順風車，利用FOXY散佈！

上週爆發警察機關因員警違規使用P2P分享軟體FOXY，而導致內部筆錄外洩，家一度建議使用者在真相未明前刪除該軟體。而刑事局則發現，有部份以假檔案，在新聞熱潮下透過FOXY傳散，實際內容則為援交訊息、惡意程式，警方呼籲使用者不要因好奇下載來路不明的檔案。

「這種手法相當常見，」CA（組合國際）技術顧問林宏嘉指出，檔名與真P2P軟體上相當常見，也是駭客散佈惡意程式的途徑之一，他表示，類似計算新，但常會利用熱門新聞事件的話題性，引誘使用者下載、點選，導致

 **新聞**

[會員登入](#) [新使用者？立即註冊](#)

[新聞](#) [網頁](#)

[新聞首頁](#) [政治](#) [社會](#) [地方](#) [國際](#) [財經](#) [科技](#) [運動](#) [健康](#) [教育](#) [藝文](#) [影劇](#) [旅遊](#) [生活](#)

[資訊3C](#) [科學發展](#) [自然環境](#) [照片故事](#) [專輯](#) [民調中心](#) [雜誌](#) [筆電也吹環保風](#) [節能減碳](#)

2007/04/18

[新聞首頁](#) > [科技](#) > [資訊3C](#) > [中廣](#)

 看完新聞來表達心情 [寄給朋友](#) [友善列印](#) 字級設定: [小](#) [中](#) [大](#) [特大](#)

網站疑個資外洩 網購連續被詐騙

 更新日期：2008/04/18 10:30

台北縣一名謝小姐在網站上購買一千多元化妝品後，接到自稱是客服人員來電表示，謝小姐在超商付款方式勾選錯誤，要她前往提款機前辦理取消，卻被詐騙一萬多元，台北縣瑞芳警分局懷疑化妝品購物網站疑似將個人資料外洩，立即展開調查。

(黃進恭報導)

這名二十四歲謝小姐喜歡上網購買化妝品，她經友人介紹，得知化妝品網站不僅產品種類多，還可以透過住家附近便利超商付款，謝小姐表示，從去年初開始接觸購物網站後，前後消費二十多次，也都沒有問題，沒想到

瞄準Y世代



Sony Ericsson
• 3.5G視訊上
• 橫向網頁

Yahoo!奇摩

思樂冰

Yahoo!奇



網路威脅攻擊目標的轉變



Computers

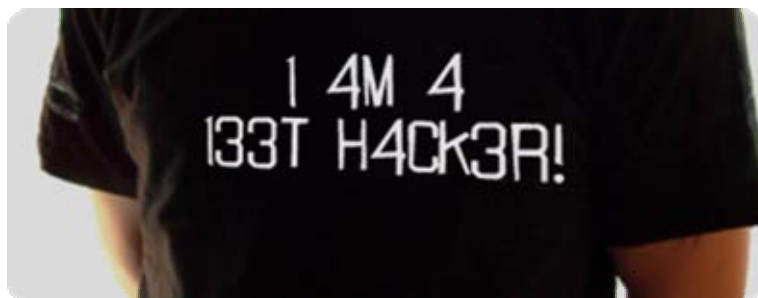


People

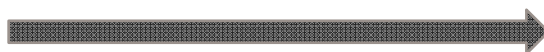




網路威脅攻擊目的的發展趨勢



Fame



Fortune



2009 年網路安全趨勢

- 個人資料以及重要文件的竊取會是惡意程式碼最主要的攻擊目標
- 駭客將繼續利用瀏覽器與其他Web應用程式，作為首選的感染媒介
- 受使用者信任的網站，將會受到更多攻擊者的鎖定，以利用散播惡意程式給非特定的受害者
- 惡意程式將透過更先進的自我隱藏及搜尋防護措施，以躲避偵測
- Mac與Linux攻擊將增加
- 駭客將挑戰Windows 7「可免於病毒危害」的說法
- 利用行動裝置散播惡意程式的時機將在2009年達到高峰
- 全球經濟危機2009年將繼續被駭客操作



Confidence in a connected world.



常見的網路安全威脅及入侵手法





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





可怕的電腦病毒

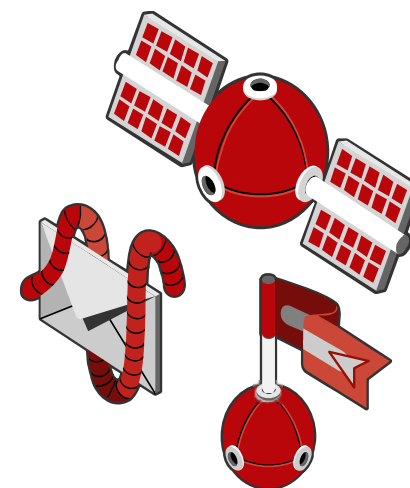
- 什麼是電腦病毒？
 - 電腦病毒原來只是一個遊戲？
 - 誰在寫電腦病毒？
 - 駭客、無聊人士、誤打誤撞 ...
 - 電腦病毒會不會讓人生病？
- 電腦病毒的特徵
 - 會不斷「自我繁殖」及「感染」
 - 會有「潛伏期」
 - 會直接或間接的影響電腦系統運作，損壞軟硬體或資訊
- 電腦病毒的存在方式
 - 隱藏在開機磁區中
 - 寄存在可被執行的檔案之中
 - 隱藏在正常的檔案之中
 - 圖片、MP3、影片、壓縮檔、文件 ...
 - 偽裝成系統檔案





了解病毒的行爲模式

- 病毒會嘗試自動執行
 - 寫入 Windows Registry
 - 寫入「開始」/「所有程式」/「啓動」
- 病毒會嘗試隱藏自己
 - 病毒常見躲藏的資料夾
 - C:\Windows
 - C:\Windows\System32
 - 修改檔案屬性爲「隱藏」或「系統」
- 病毒會嘗試保護自己
 - 修改系統機碼不讓使用者使用管理工具
 - 嘗試阻止使用者安裝防毒軟體或下載防毒更新
 - 被停止程序時會自動呼叫另一程序
- 病毒會尋找其他目標或向攻擊者回報
 - 會開啓特定的通訊埠
 - 會持續對外連線





隱藏的安全風險





安全風險可能造成的影響

- 敏感性資料的流出
 - 帳號、密碼、個人身分資料、信用卡資料...
- 不斷跳出廣告視窗
- 設定遭到更改，無法恢復原本的設定
 - 網頁綁架
- 應用程式出現不曾安裝過的額外元件
 - HotBar、Weather、Gator
- 電腦及網路受到影響
 - 電腦反應遲緩
 - 系統不穩定
 - 網路效能降低
- 被植入木馬或開啓後門
- 不斷從網路上下載惡意程式





系統的安全瑕疵



最新Notebook評測

最後更新：2006/01/11 08:24 PM

微軟WMF又出問題

CNET新聞專區：Joris Evers 10/01/2

微軟才剛推出修補程式解決Windows XP的漏洞，但現在又發現WMF (Windows Media Format) 又出問題。據報導，若不及時解決，可能成為駭客攻擊電腦未作好防護，微軟作業系統的核心程序界面由explorer管理，包括啟動項、工

微軟一名職員表示，微軟知道WMF又出修補程式時，就可以下載。

微軟初步調查發現，瑕疵不影響電腦的安全，但可能導致某些用戶無法正常播放WMF圖片。對於瑕疵會造成影響觀看WMF圖片的軟體，諸如Win

微軟說：「新的瑕疵可能造成播放WMF圖片時，某些用戶無法正常播放。」微軟說，瑕疵不至於造成駭客從遠



微軟釋出Windows、Outlook漏洞修補程式

CNET新聞專區：Joris Evers 2006/01/11

微軟周二發佈針對兩項重大安全瑕疵的修補程式，一個在Windows Exchange Server郵件伺服器中。

該公司在每月定期的安全公告中指出，兩項弱點會導致攻擊者得以控制體的PC。

Windows的弱點存在於該軟體處理網頁字體的過程中，所有現有版訪到包括惡意字體或看了此類郵件，就可能被入侵，微軟發佈的MS

而微軟的MS06-003公告表示，Outlook及Exchange的漏洞則出現在其中。如果攻擊者在郵件中動手腳，則Outlook及Exchange的用戶



微軟再發現2個Windows安全漏洞 籲儘速下載修補程式

【中廣新聞網】

據路透社報導，美國微軟(網站、商品)公司星期二再度發出警告，說他們發現現行的Windows作業系統，又有兩個「嚴重」的安全漏洞，可能會引發駭客(新聞、網站)入侵，呼籲用戶要趕快下載修補程式。

微軟公司上個星期才發佈了一個修補程式，來修補一個系統漏洞；專家表示，還沒有下載修補程式的用戶，如果發現來路不明，其中有附加檔案的電子郵件(新聞、網站)，千萬不要打開，最好立即刪除。



微軟資訊安全公告 - Windows Internet Explorer

http://www.microsoft.com/taiwan/security/bulletins/default.mspx

Live Search

微軟資訊安全公告

請按一下此處安裝 Silverlight

Taiwan 變更 | 所有的 Microsoft 網站

Microsoft

Web Live Search

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

高可信度電腦運算

微軟資訊安全公告

張貼日期: 2003 年 01 月 29 日 | 更新日期: 2009 年 4 月 15 日

本月資訊安全公告

2009 年 4 月

- 2009 年 4 月份安全性更新
- 2009 年 4 月份 Microsoft 安全性公告摘要
- Microsoft 安全性公告 MS09-009 - 重大: Microsoft Office Excel 的弱點可能會導致遠端執行程式碼 (968557)
- Microsoft 安全性公告 MS09-010 - 重大: WordPad 及 Office 文字轉換程式中的弱點可能允許遠端執行程式碼 (960477)
- Microsoft 安全性公告 MS09-011 - 重大: Microsoft DirectShow 中的弱點可能允許遠端執行程式碼 (961373)
- Microsoft 安全性公告 MS09-012 - 重要: Windows 中的弱點可能允許權限提高 (959454)
- Microsoft 安全性公告 MS09-013 - 重大: Windows HTTP 服務中的弱點可能允許遠端執行程式碼 (960803)
- Microsoft 安全性公告 MS09-014 - 重大: Internet Explorer 積存安全性更新 (963027)
- Microsoft 安全性公告 MS09-015 - 中度: SearchPath 中的混合威脅弱點可能允許權限提高 (959426)
- Microsoft 安全性公告 MS09-016 - 重要: Microsoft ISA Server 與 Forefront Threat Management Gateway (Medium Business Edition) 中的弱點可能導致拒絕服務 (961759)

2008 資訊安全公告

- 2009 年 3 月
- 2009 年 2 月
- 2009 年 1 月
- 2008 年 12 月
- 2008 年 11 月
- 2008 年 10 月



網路釣魚 (Phishing)

- 釣魚攻擊的操作手法和數量已超越一般電腦病毒和木馬程式，成為網路安全的最大威脅。
- 利用偽造電子郵件或網站作為誘餌，且利用知名公司所建立的信賴感，提高詐騙的成功機率，讓受害者洩漏個人資料
- 主要在於騙取受害者的身分證字號、銀行帳號、密碼、信用卡號碼等機密資料
- 常見的網路釣魚方式
 - 詐騙網址
 - 電子郵件表單
 - 彈出式的視窗
 - 偽造 IE 網址列
 - 偽造知名網站



網路釣魚典型案例 - 'Citibank Alert Service' 2004-11-10

Dear Citibank Customer

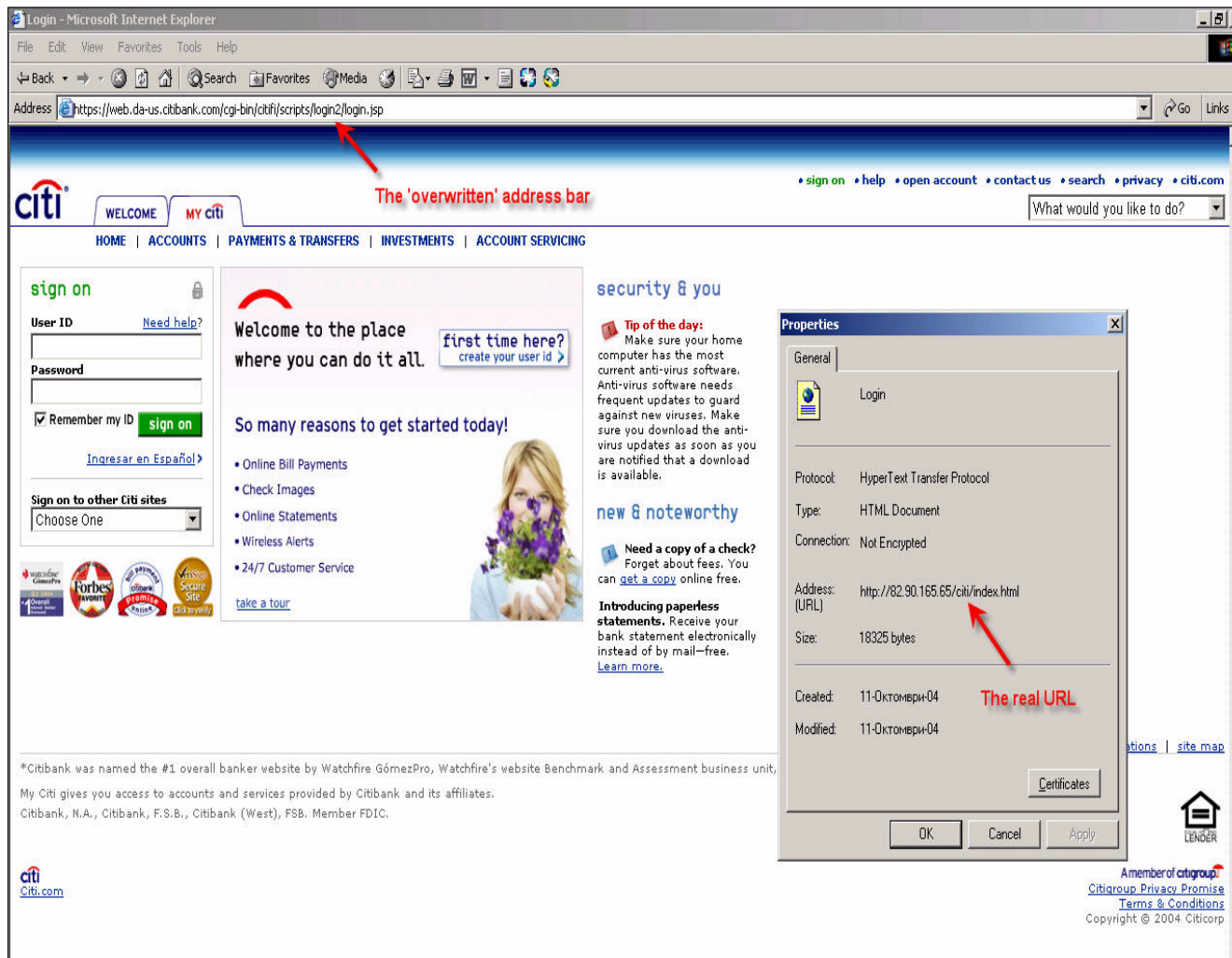
We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking [here](#).

If you have recently updated your information, please disregard this message as we are processing the changes you have made.

Citibank Customer Service
Citibank Alerting Service
Citibank [alert@citibank.com]

Web Site

Visible link:	'here'
Called link :	http://82.90.165.65/citi
Phish website hosted on :	82.90.165.65



The screenshot shows a Microsoft Internet Explorer browser window. The address bar displays a URL that has been overwritten by a malicious script, indicated by a red arrow and the text "The 'overwritten' address bar". The page content is a phishing site for Citibank, featuring a login form and various links. A "Properties" window is open, showing the "General" tab with the "Address (URL)" field containing the real URL: <http://82.90.165.65/citi/index.html>, also indicated by a red arrow and the text "The real URL".



社交工程術 (Social Engineering)

- 利用人性弱點或人際互動上的技巧，以影響力與說服力來欺騙他人進而獲取資料的行為
- 方法是進行巧妙的騙術，或令對方相信其假冒的身分
- 社交工程駭客得以利用他人，不管有無動用到科技、電腦或程式，都可以獲取帳號、密碼、信用卡號碼、身分證號碼、姓名、地址或其他可確認身分或機密資料
- 『跟你裝熟，以達到特定的目的』





常見的社交工程手法

- 假冒同事
- 假冒廠商、合作夥伴、或是執法單位的員工
- 假冒具有權威的人
- 假冒新進員工，需要幫忙
- 請求總機幫忙接傳真，然後再要求轉傳
- 請求將檔案傳至公司內部的地方
- 謊稱是公司外地員工，要求設立可以在當地存取的電子郵件
- 使用內行人術語和行話來取得信任
- 假冒廠商打電話來提供系統修補程式或更新程式
- 告訴對方如果發生問題可以找他，然後製造問題，讓對方打電話來求援
- ...



社交工程術的真實案例 (2006-02-11)

總機：「XXX科技您好」

駭客：「妳好，請問 Trista 在嗎？」

總機：「她現在不在座位上，需要我幫您留言嗎？」

駭客：「沒關係，我只是要寄個東西給 Trista，可是我不太確定妳們公司的地址，妳能夠告訴我妳們公司的地址嗎？」

總機：「沒問題，我們的地址是台北市長安東路一段xx號xx樓之3。」

駭客：「謝謝，請問我只要寫 Trista 收，她就會收到了嗎？」

總機：「沒錯，不然你也可以寫給許xx小姐收。」

駭客：「請問她的分機號碼是？」

總機：「她的分機號碼是XXXX」

駭客：「這樣我知道了，謝謝妳！」

總機：「不客氣」

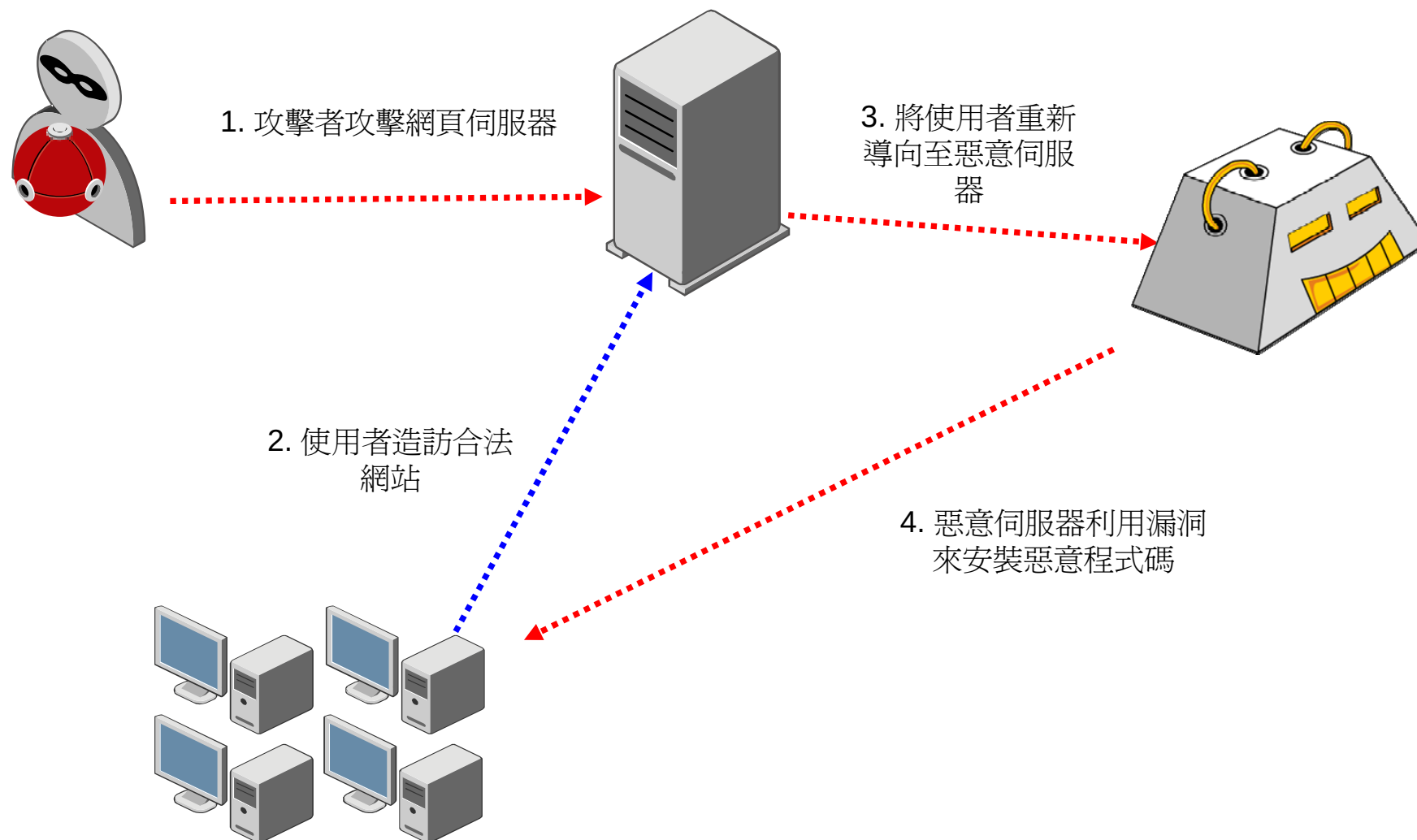


惡意威脅入侵手法解析

- 駭客利用工具將惡意程式偽裝
 - 照片、小遊戲、掃毒軟體、工具...
- 透過網路散播含有惡意程式的檔案
 - 放在網站上或透過P2P軟體供人下載
 - 傳遞給 Mail 或即時通訊軟體上的好友名單
- 誘騙使用者接收並開啓惡意程式
 - 告訴使用者是好用的工具或好玩的遊戲
 - 透過文字說明誘騙使用者點選網址
 - 帥哥美女照
- 取得敏感性資料
 - 帳號、密碼、個人資料...
- 儘可能隱藏自己的行蹤
 - 變更檔案屬性、檔名或變更系統設定
 - 從網路下載新版本更新以逃避防毒軟體的掃描
- 利用各種手法尋找下一個攻擊目標



網頁掛馬過程示意





Confidence in a connected world.



如何加強個人的網路安全防護降低風險

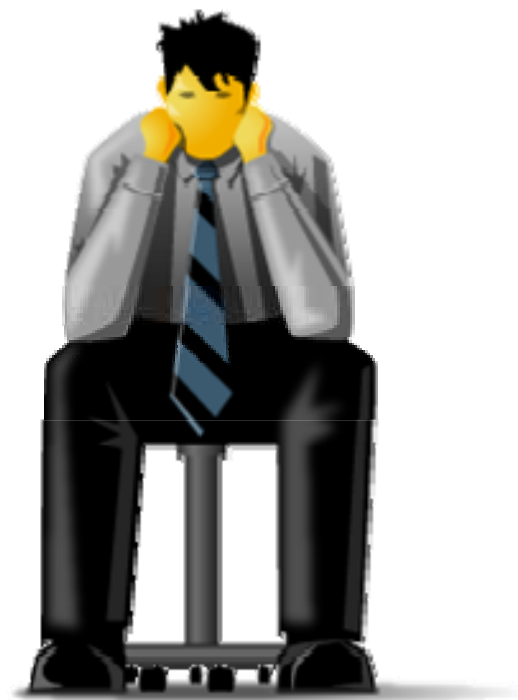


上奇科技



為什麼會中毒？

- 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





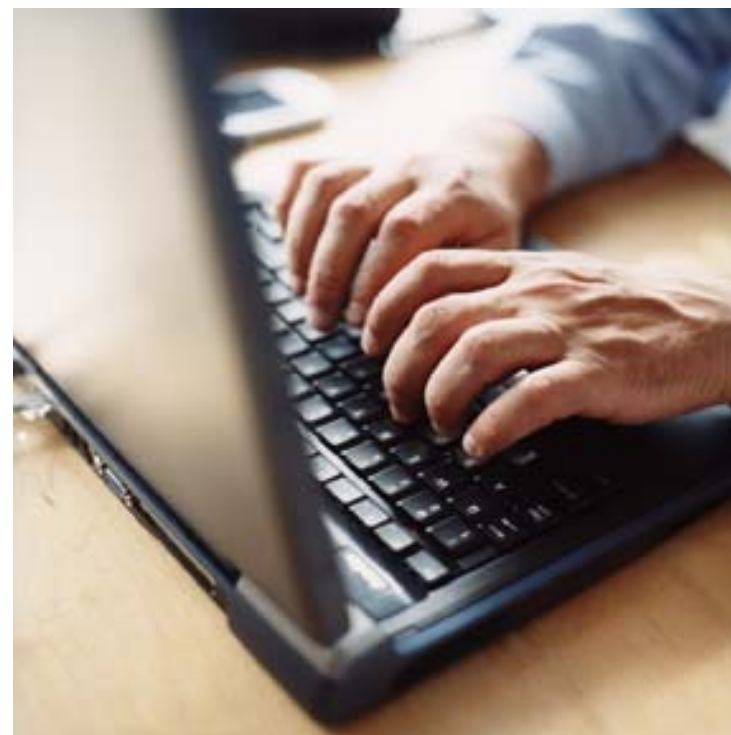
良好的使用習慣

- 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



如何加強系統安全

- 使用個人防火牆
- 使用 IP 分享器或建立 DMZ 區域
- 隨時保持系統軟體在最新狀態
- 使用複雜度及強度高的密碼
- 停用沒有用到的服務
- 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	Grand Tech	GRANDTECH		Grand Tech	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





Confidence in a connected world.



我中毒了嗎？



上奇科技



我中毒了嗎？

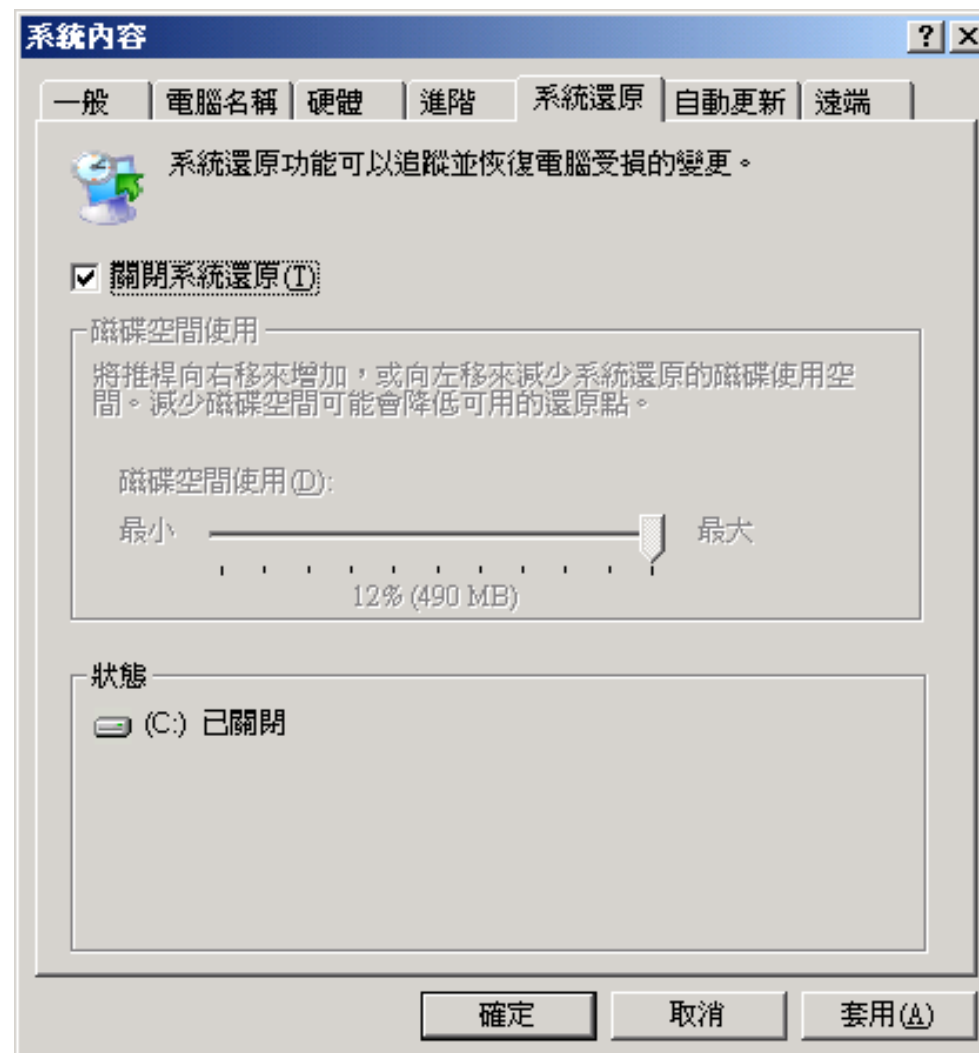
- 即使是防毒專家也無法告訴您是否真的中毒
- 常見的疑似中毒症狀
 - 無法開機
 - 不正常的網路通訊
 - 記憶體內增加了來路不明的常駐程式
 - 系統執行速度比平常緩慢
 - 不尋常的錯誤訊息出現
 - 系統記憶體容量忽然大量減少
 - 磁碟可利用空間突然減少
 - 可執行檔的檔案大小改變了
 - 檔案名稱、副檔名、日期、屬性被更改過
 - 應用程式無法正常開啓
 - 防毒軟體無法正常運作
 - 不斷跳出廣告視窗
 - 設定遭到更改，無法恢復原本的設定
 - 網頁瀏覽器出現不曾安裝過的額外元件





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(SAFE 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





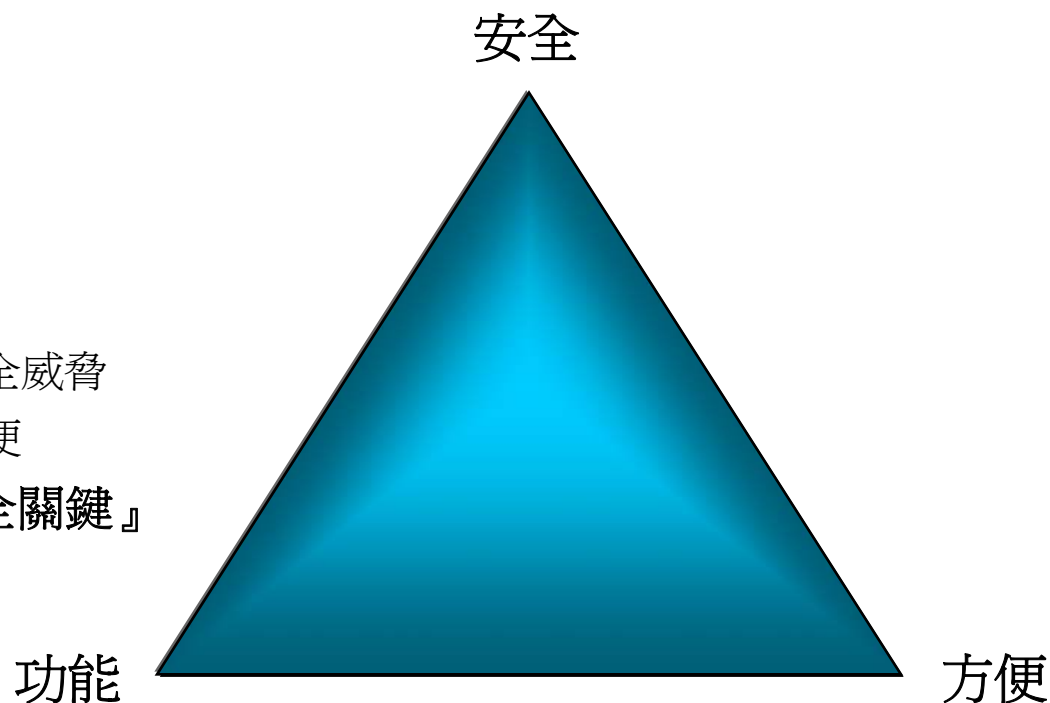
防毒軟體的迷思

- 只要有安裝防毒軟體就能萬無一失嗎？
- 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
 - 防毒軟體也有可能成為攻擊的目標
 - 防毒軟體無法防禦網路攻擊行為
 - 防毒軟體可能會誤判
- 到底哪一家的防毒軟體比較好？
 - 有抓到病毒的防毒軟體不一定是好的防毒軟體，防毒軟體也有可能誤判
 - Windows Explorer 被防毒軟體誤判為惡意程式 (2007-12)
 - Windows 重要元件(Isasrv.dll)被誤判為惡意程式導致系統當機 (2007-06)
 - 效能、防護能力、誤判率、定義檔的更新速度、是否影響系統正常運作 ...



面對未來的網路安全威脅應該有的認知

- 資訊安全是一種持續的過程而不是一種結果
- 「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
- 沒有一種方法可以完全防止病毒或駭客入侵
 - USB 卸除式磁碟病毒
 - 不要使用 USB 卸除式磁碟？
 - 被植入惡意連結的網頁
 - 不要瀏覽網頁？
- 「安全」？「方便」？「功能」？
 - 越方便，隨之而來的可能就是安全威脅
 - 強化安全，可能造成使用上的不便
- 『個人的使用行為才是最後的安全關鍵』
 - 您要的是方便還是安全呢？





Confidence in a connected world.



Thank you!

dannylan@pixnet.net

<http://security.magicworks.net>



上奇科技