台東縣消防局
Fire Bureau, Taitung County Government

103 年 資訊安全教育訓練

『社交工程與 P2P 威脅防護』

講義

103 年 5 月

資立電腦股份有限公司
HTTP://www.tzli.com.tw/

資訊安全議題：社交工程與P2P威脅防護

資立電腦

課程大綱

- 當前政府資安威脅
- 社交工程與網頁惡意掛馬
- P2P的危害與防護
- 結論

過去

現在

政府資通安全問題

- 外部威脅
  - 組織型駭客針對性攻擊
  - 鎖定特定對象或單位
  - 攻擊型式變化快速
- 內部問題
  - 政府資安人力、經費及能量相對不足
  - 資安事件通報意願不高
  - 委外開發軟體及品質管理問題
  - 資訊作業委外處理衍生資安管理問題
  - 人員資安意識不足
  - 各機關橫向聯繫機制尚待建立
  - 資安相關法令尚未完備

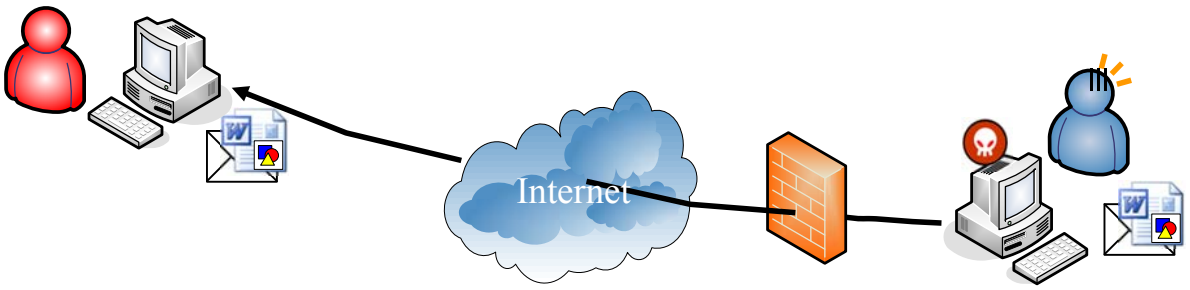
資料來源：吳啟文，行政院資通安全會報通報應變組主任

政府機關資料外洩主要管道

- 以社交工程手法寄發惡意電子郵件
- 網頁惡意掛馬：網頁插入惡意連結內容，使用者不自覺下載惡意程式
- 外接式儲存裝置安全問題
- 使用P2P軟體、IM (Instant Message)即時通訊軟體、社群網站可能造成個人資料外洩風險

資料來源：吳啟文，行政院資通安全會報通報應變組主任

收*E-mail*可能的風險

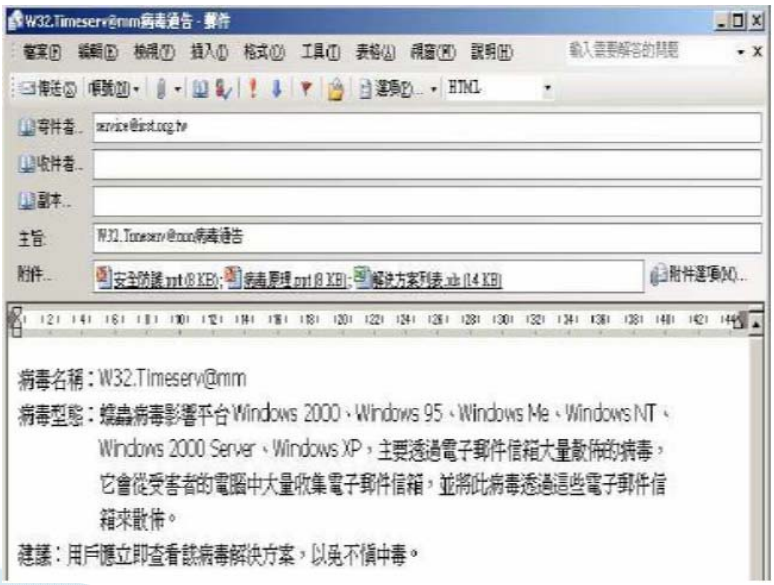


1. 駭客設計攻擊陷阱程式(如特殊Word 檔案)
2. 將攻擊程式埋入電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，並被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到
7. 遠端駭客進行資料竊取

資料來源：吳啟文，行政院資通安全會報通報應變組主任

社交郵件案例-資通安全會報技服中心的通知

- **假冒信件訊息如下:**
  - 寄件者：service@icst.org.tw
  - 主旨為「W32.Timeserv@mm 病毒通告」
  - 附件有3 筆名稱分別為「安全防護.ppt」、「病毒原理.ppt」、「解決方案列表.xls」。



Demo

- 電子郵件的木馬屠城

資立電腦股份有限公司 ISLEADER

社交工程

「社交工程」攻擊定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務、時事相關或令人感興趣的郵件內容
  - 含有惡意程式的附件
  - 利用應用程式之弱點(包括所謂零時差攻擊)

社交工程_手法

- 偽社群網站釣魚郵件
  - 由駭客發出的單純交友邀請並沒有放任何的惡意連結或程式，「交朋友」只為了觀察生活習慣，拼湊出個人的資訊地圖，再做進一步利用
- 帶有惡意附件郵件
  - 在電子郵件中置入一般認為安全的文件檔，.doc、.xls、.pdf、.html…等，或將這些攻擊程式放在網路上，電子郵件內容僅放置簡單的下載連結
- 電子郵件帳密竊取問題
  - 「P@ssw0rd」是公認常用的弱密碼之一，如果採用常用弱密碼表進行猜測，此密碼很可能在十次嘗試以內便遭破解

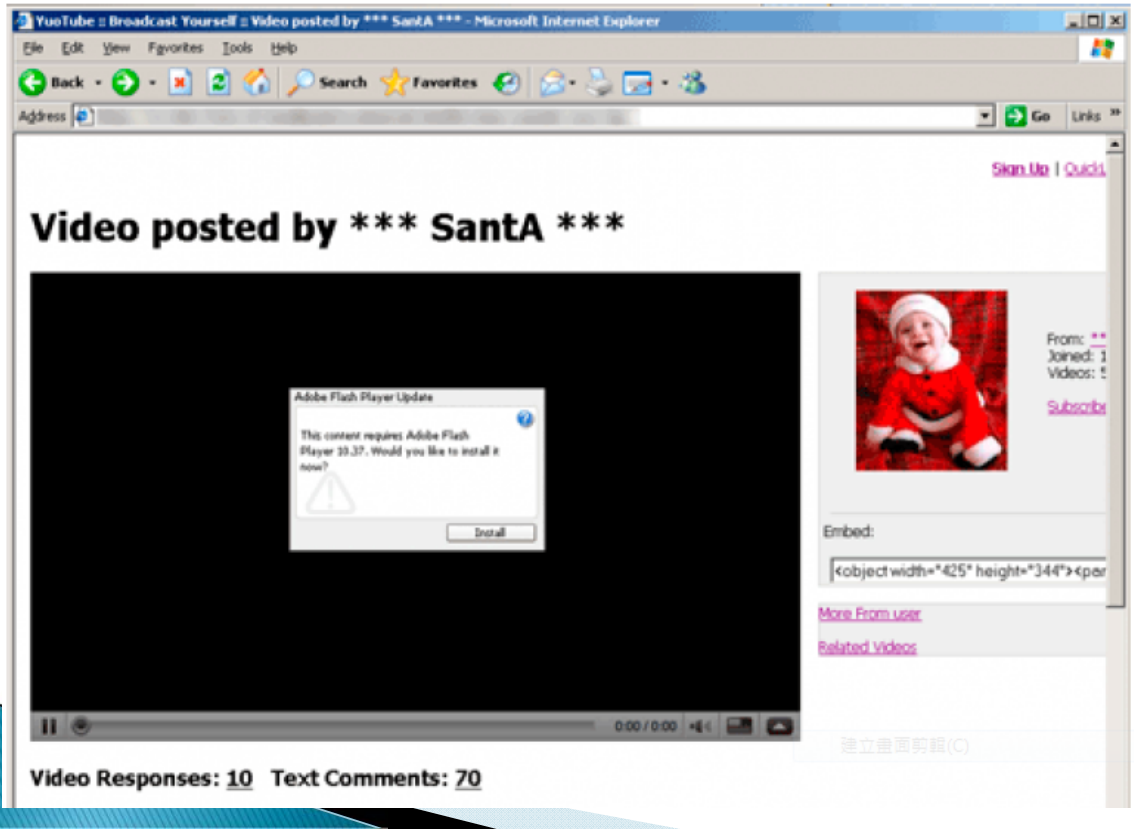
釣魚網頁 Phishing

- 利用合法網站本身的漏洞
- 置入幾可亂真的網頁頁面(置換網頁 Defacement)
- 或藉由知名網站廣告，連結惡意網頁
- 以誘騙使用者輸入帳號、密碼及信用卡資料為主要目的
- 常見的手法有[近似]及[延伸]
  - 近似範例：login.live.com→login-live.com

偽冒網站(1):假造的Facebook網站

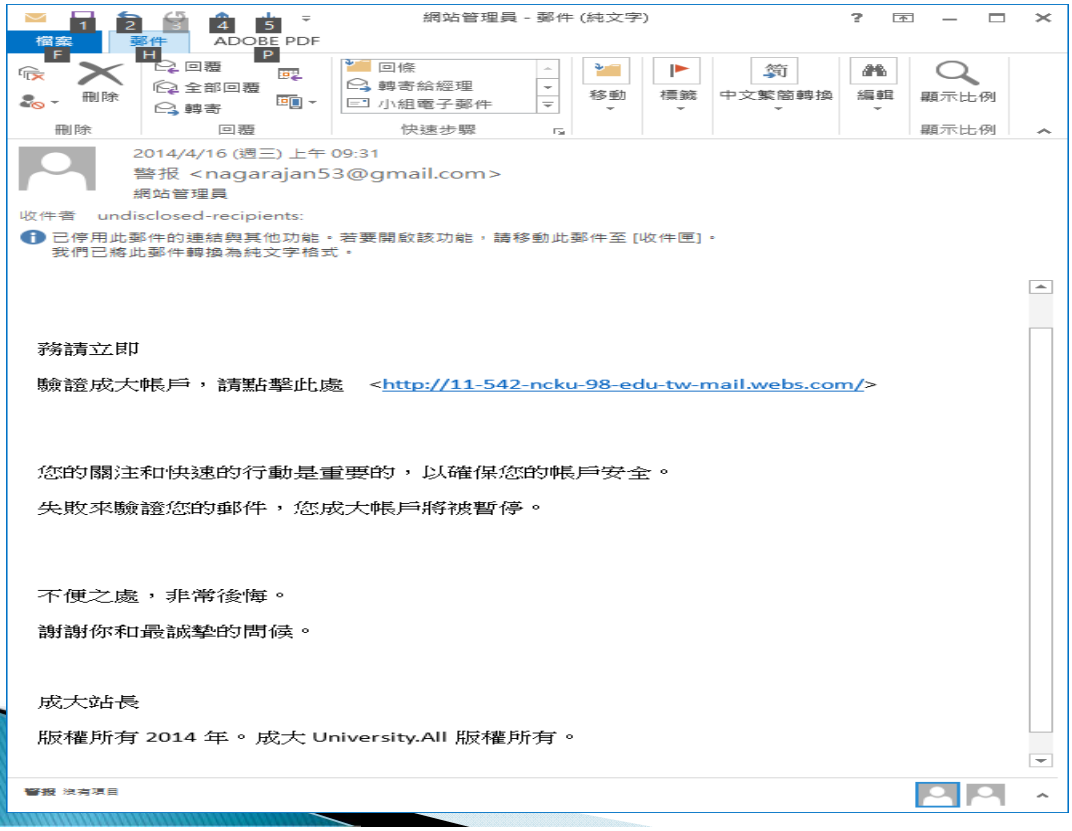
偽冒網站(2)

Fake YouTube site created by W32.Koobface



最常被攻擊的網路釣魚(知名銀行/信用卡公司/網路購物/拍賣)網站排行

釣魚郵件：偽造的電子郵件



假的網站
<http://11-542-ncku-98-edu-tw-mail.webs.com/>

真的網站
http://mail.ncku.edu.tw/

小心被騙個人資料

Google備用地址電子郵件驗證

不明電子郵件要來加入你的Google

點選左列連結，狀態列會出現實際連結位址，檢視是否與狀態列出縣之內容相符

小心被騙個人資料

請你登入，如果你輸入密碼，個人資料將會被攻擊者取得

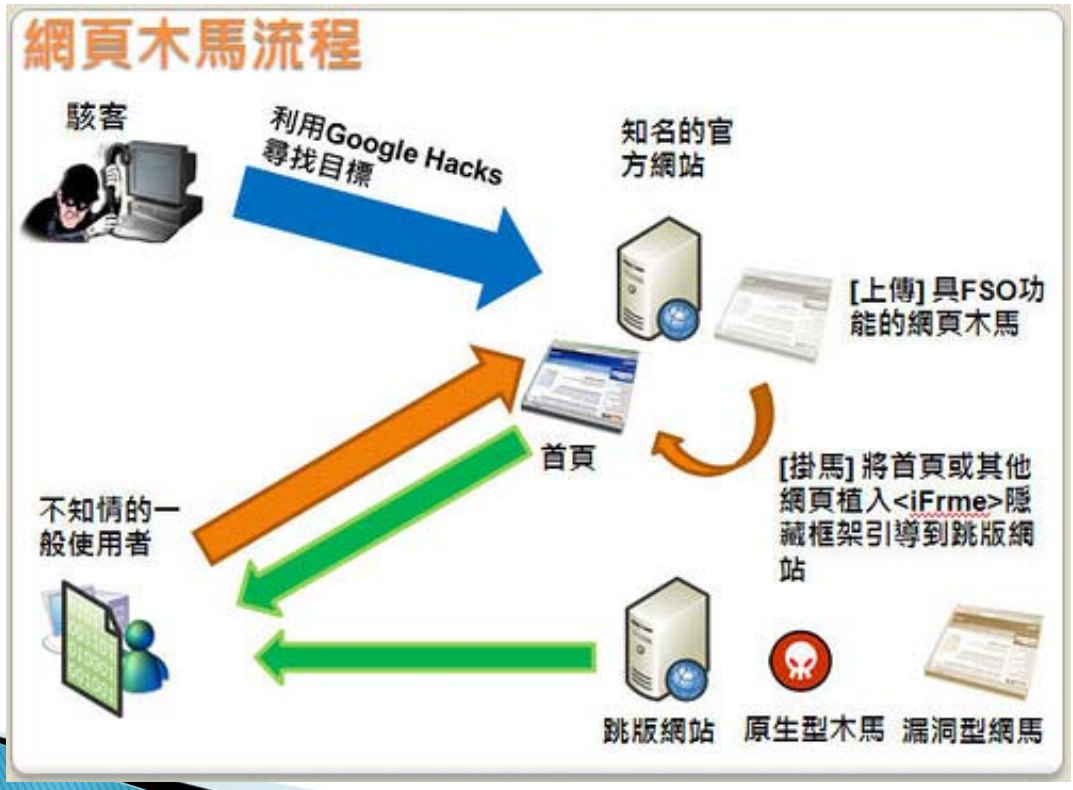
釣魚郵件：偽造的電子郵件

- 如何區分偽造的*網路釣魚（Phishing）*跟正常郵件，就要檢查下列蛛絲馬跡：
  - 偽造的電子郵件通常會使用通用問候語，而不是給收件者
  - 正常的電子郵件通常不會有明顯的語法錯誤、拼寫和格式問題
  - 偽造的電子郵件會有一種「危言聳聽」的感覺，通常會要求使用者點入連結或給個人資料
  - 有些看起來可能跟原公司的電子郵件一模一樣。因此，使用者應該仔細閱讀電子郵件。而且去驗證電子郵件內容的正確性。
  - 強烈建議使用者要避免打開任何附件檔或點入任何連結，即使這些來自看似認識的來源。要習慣去複製快捷連結，然後仔細檢查其正確性。仔細閱讀郵件全文來避免詐騙攻擊。
  - 要始終保持系統在安全狀態，更新軟體廠商所發佈的修補程式和最新的安全更新。

網頁掛馬

- 「**網頁掛馬**」又稱之為**網頁隱藏式惡意連結**
- 駭客入侵(知名的)網站
- 不更動原有的畫面下，修改網站內容，加入**惡意程式碼**
- 使瀏覽該網站的使用者**被植入惡意程式**
- 進而**竊取個人資料**或**當成跳板主機**

網頁掛馬攻擊模式

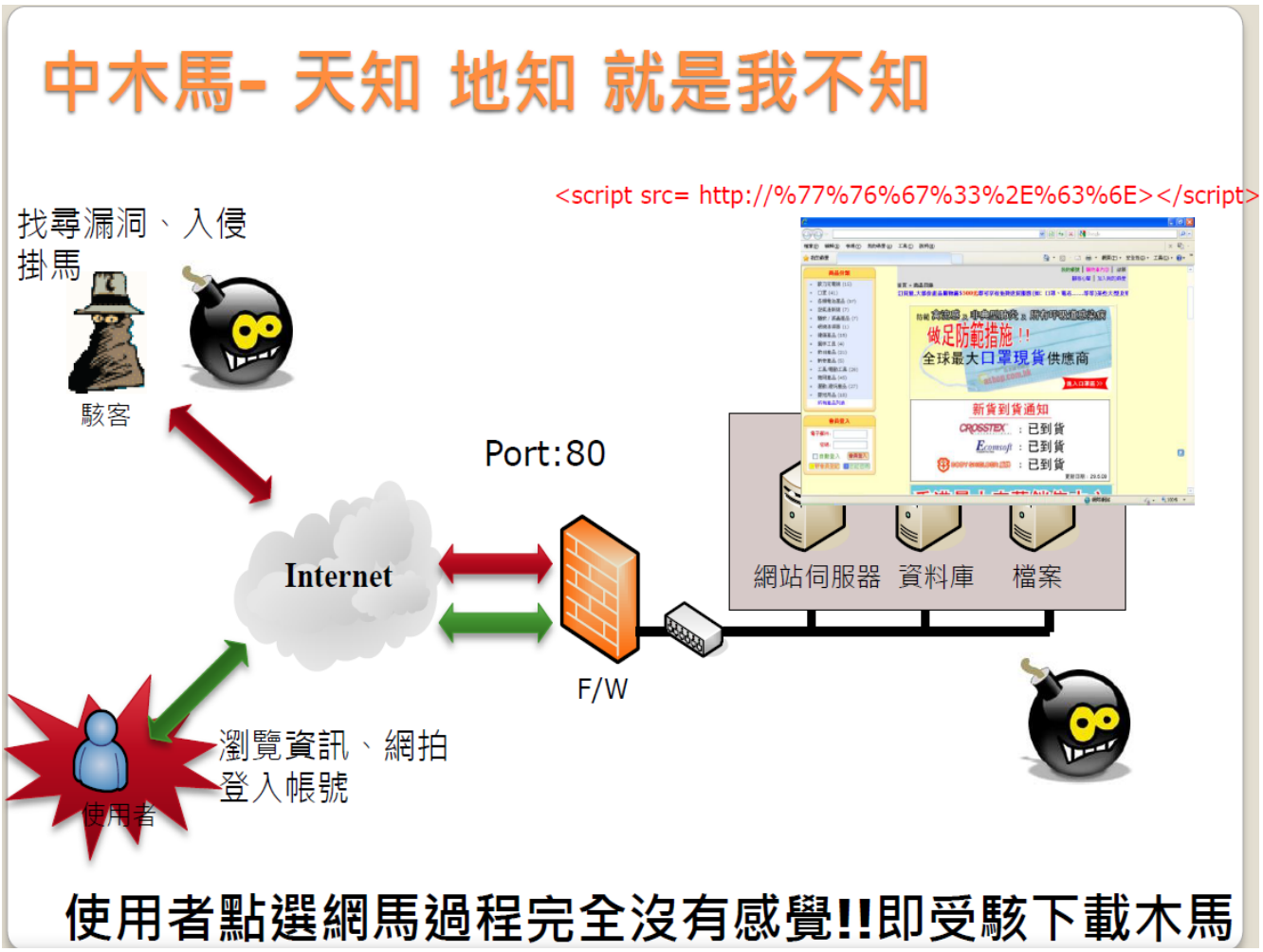


躲在正常網站後的惡網站

網頁掛馬的危害

- 對網站擁有者而言
  - 因管理不善導致他人被入侵而負上法律責任
  - 商譽的損失
- 對一般使用者而言
  - 資料失竊
    - 隱私資料、信用卡資料、線上遊戲虛擬寶物等
  - 被當跳板主機
    - 可能面臨法律責任

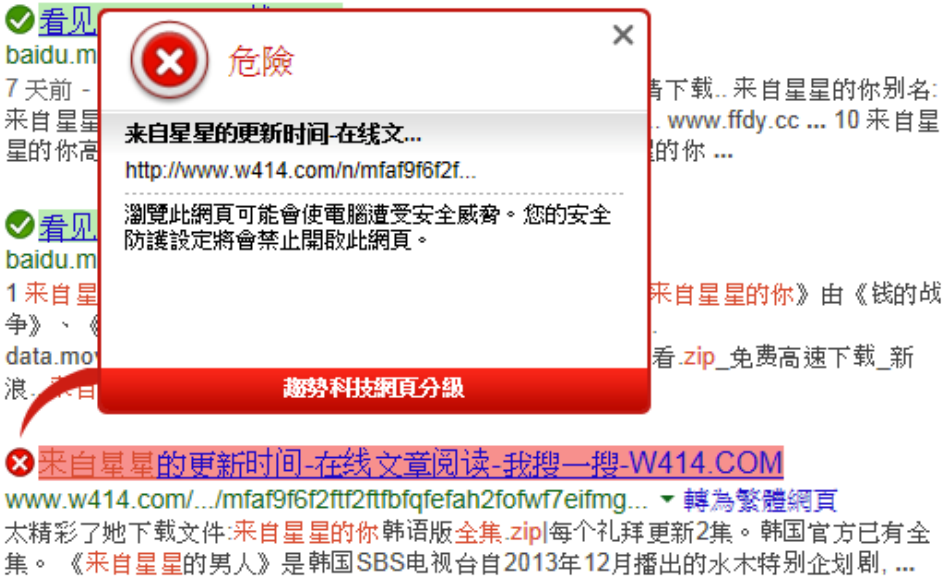
中木馬- 天知 地知 就是我不知



使用者點選網馬過程完全沒有感覺!!即受駭下載木馬

網頁掛馬
DEMO

- 瘋「來自星星的你」大結局,當心中毒!很多標示「全集」、「大結局」的連結夾帶木馬

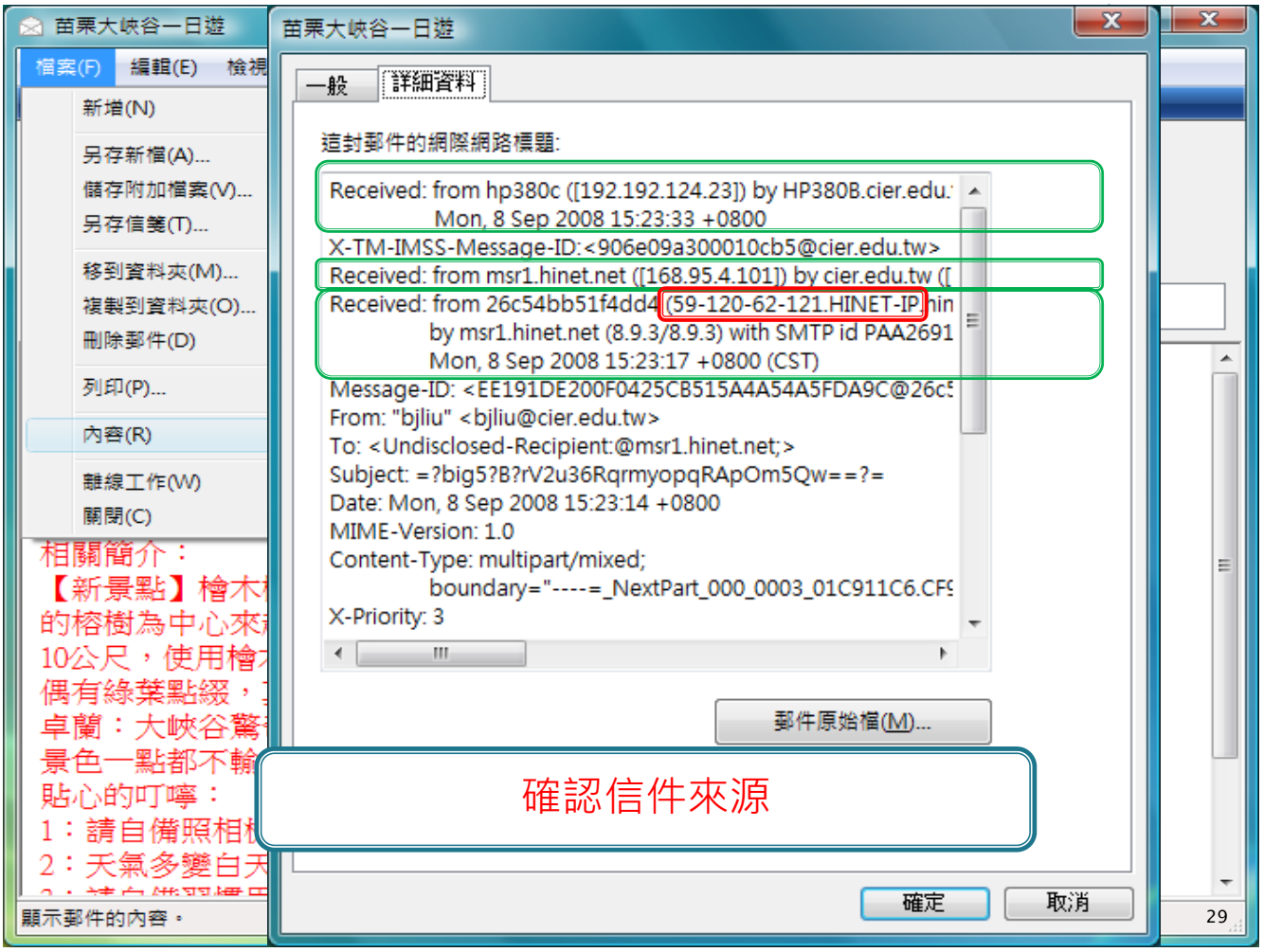


網站惡意掛馬預防方法

- 安裝修補程式
- 使用防毒軟體
- 不隨意瀏覽網站
- 提高IE的安全性設定，停用Script和ActiveX元件下載
- 經常檢視重要機器其開機執行程序狀態，例如：使用ProcessExplorer、Autoruns等程式或其它廠商開發之工具來比對
- 降低網頁瀏覽權限
- 危機意識與正確的資安觀念

社交工程防護
從電子郵件開始

- 良好的電子郵件使用習慣
  - 使用電子郵件前先確認以下設定：
    - 必須安裝防毒軟體並更新病毒碼
    - 必須純文字模式開啟郵件
    - 取消預覽功能
  - 收到郵件後必須注意事項：
    - 主旨是否與本身業務相關
    - 收到不明郵件應立即刪除
    - 不要任意點閱郵件中超連結或網站郵件提示贈獎活動不要任意點閱或填寫個人資料
    - 不要任意打開不明郵件的附加檔案
    - 避免回覆或轉寄不明信件

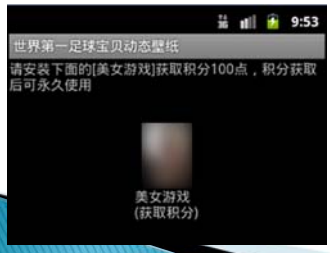


避免被釣魚

- 確認！確認！在確認！！
  - 連接的網站
  - 收到的訊息
  - 朋友的post文
- 不要隨便下載
  - 從可信賴的來源
- 使用安全的密碼

倫敦奧運會票務網站在臉書 facebook 開賣!?網路釣客騙個資

Figure 1. Sample "London 2012 Olympics Tickets" Facebook post



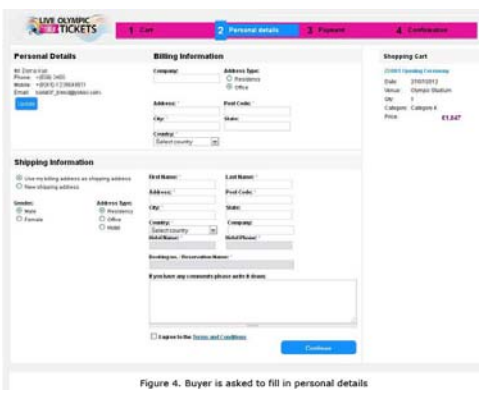


Figure 4. Buyer is asked to fill in personal details

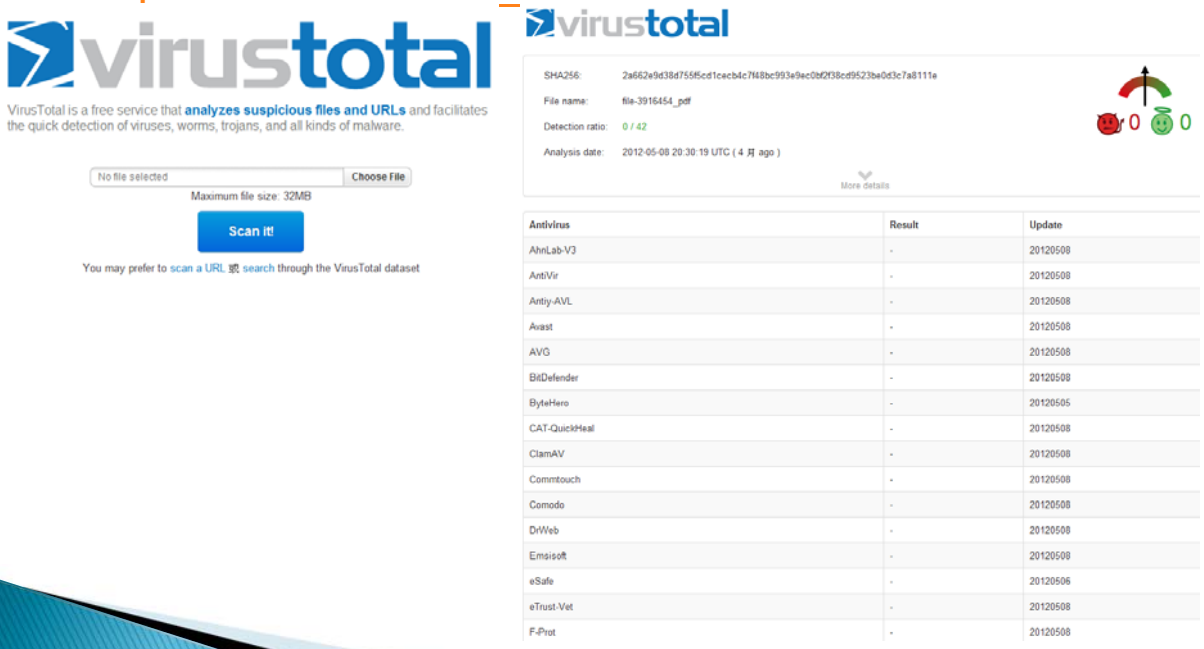
Domain name與IP 查詢

- Check 連結連結之Domain name為何IP address(如：為140.116.XX.XX)
- 開始/所有程式/附屬應用程式/命令提示字元
- 鍵入 nslookup命令後, 輸入欲查詢的 Domain name 或IP address。

Domain name與IP 查詢

確認是不是惡意程式

- https://www.virustotal.com/

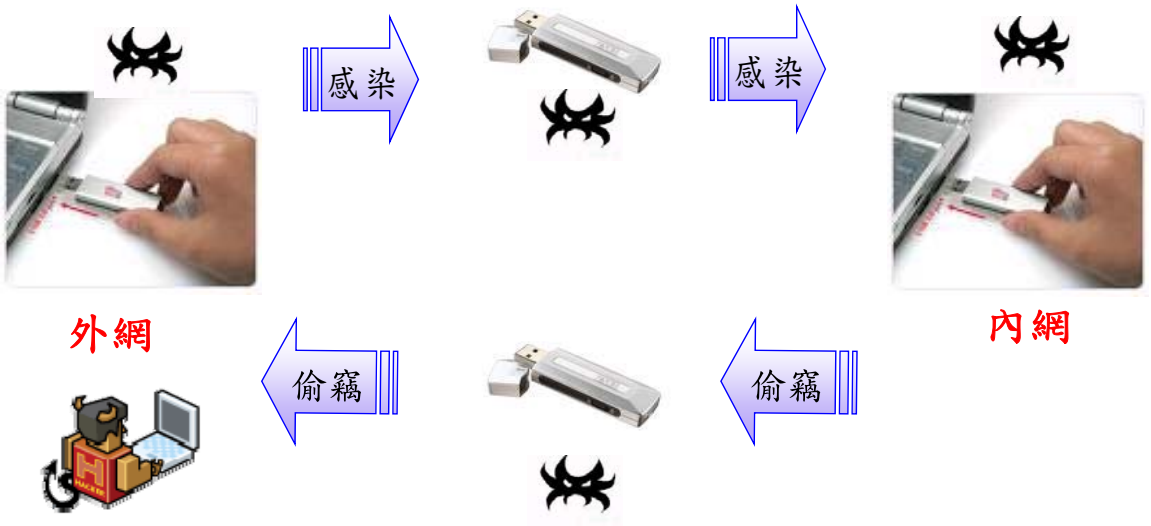


*USB*隨身碟的風險

- 自動播放：尋找Autorun.inf檔案，並執行該檔案所描述之動作，會自動執行惡意程式並將惡意程式複製至系統磁碟機內，再進一步擴散

用戶A　　用戶B

隔離網路設備感染方式

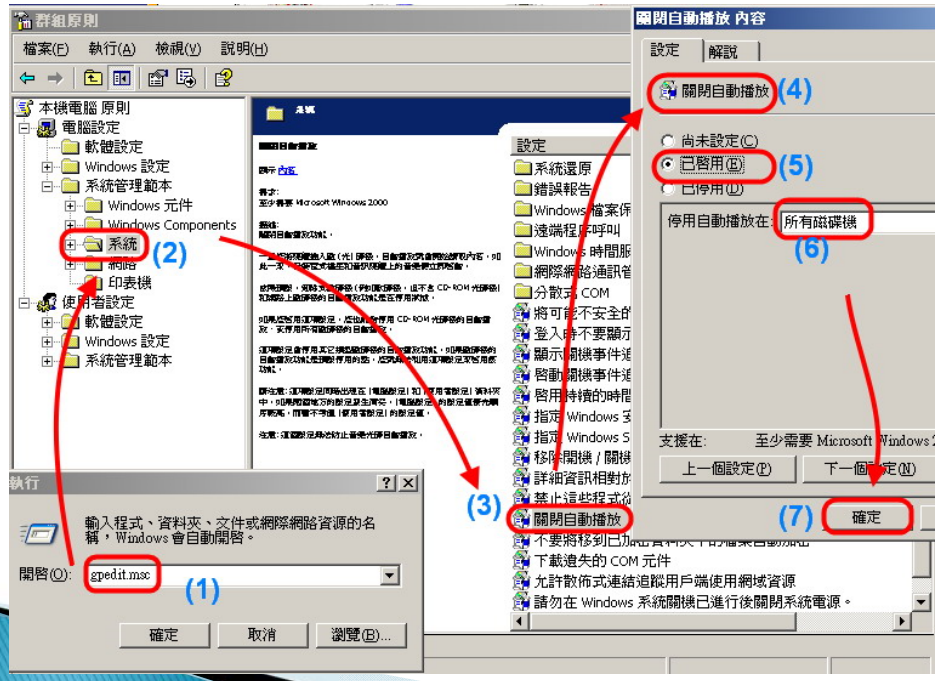


解毒的迷思

網路偏方	效果	說明
建立 Autorun.inf 資料夾 停用 Autorun 功能	部份有效	可以暫緩病毒發作。新的變種病毒會先刪除舊有的 Autorun.inf 資料夾或檔案，或是自行啟動 Autorun 功能。 建議移除該資料夾安全性頁籤中的所有使用者及群組，才能防止被竄改。
按住 Shift 鍵開啟隨身碟	無效	只能關閉 Autoplay，無法關閉 Autorun。
在隨身碟上按右鍵開啟檔案總管	部份有效	透過「我的電腦」去點選，仍會遭感染。若正確地透過「檔案總管」來開啟，則不會感染。
啟用隨身碟的唯讀功能	無效	若是隨身碟已感染病毒，只要能執行，就可以感染作業系統。
軟體限制原則	部份有效	能阻止病毒從 USB 裝置擴散，但無法防範從網路磁碟或郵件附件檔執行。
禁用 USB 裝置	部份有效	能阻止病毒從 USB 裝置擴散，但無法防範從網路磁碟或郵件附件檔執行。
USB 病毒專殺工具	短期有效	若未定期更新，只能清除舊病毒。而且工具來源不一定安全。

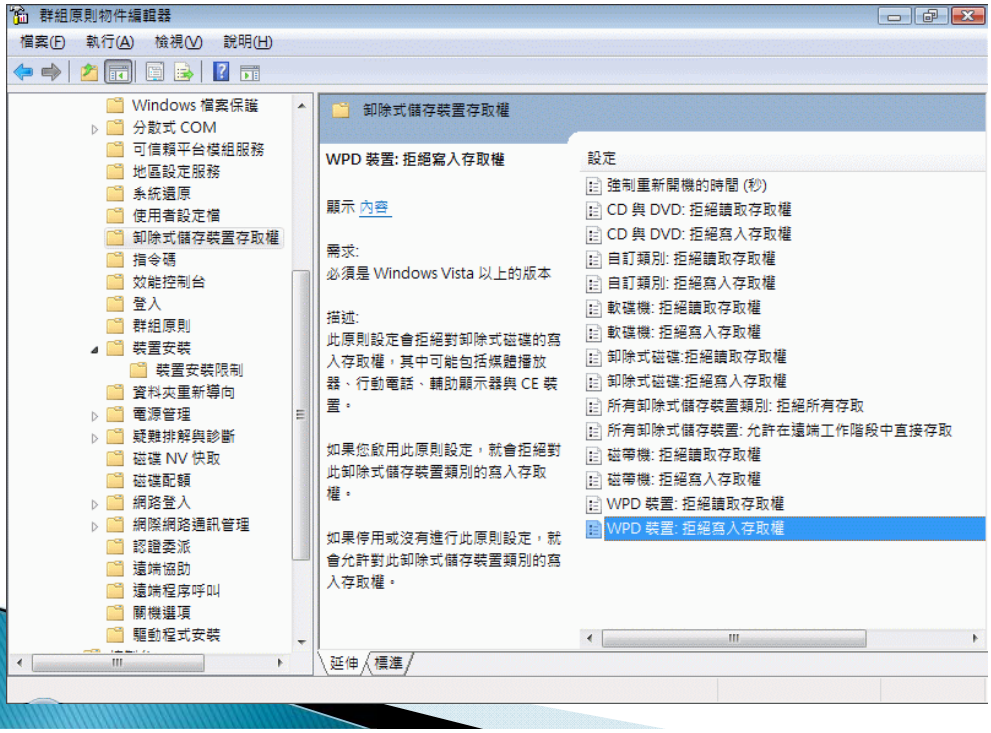
@方法:關閉自動撥放

〔開始〕\執行，輸入「gpedit.msc」，再按一下〔確定〕按鈕，開啟群組原則設定頁面。



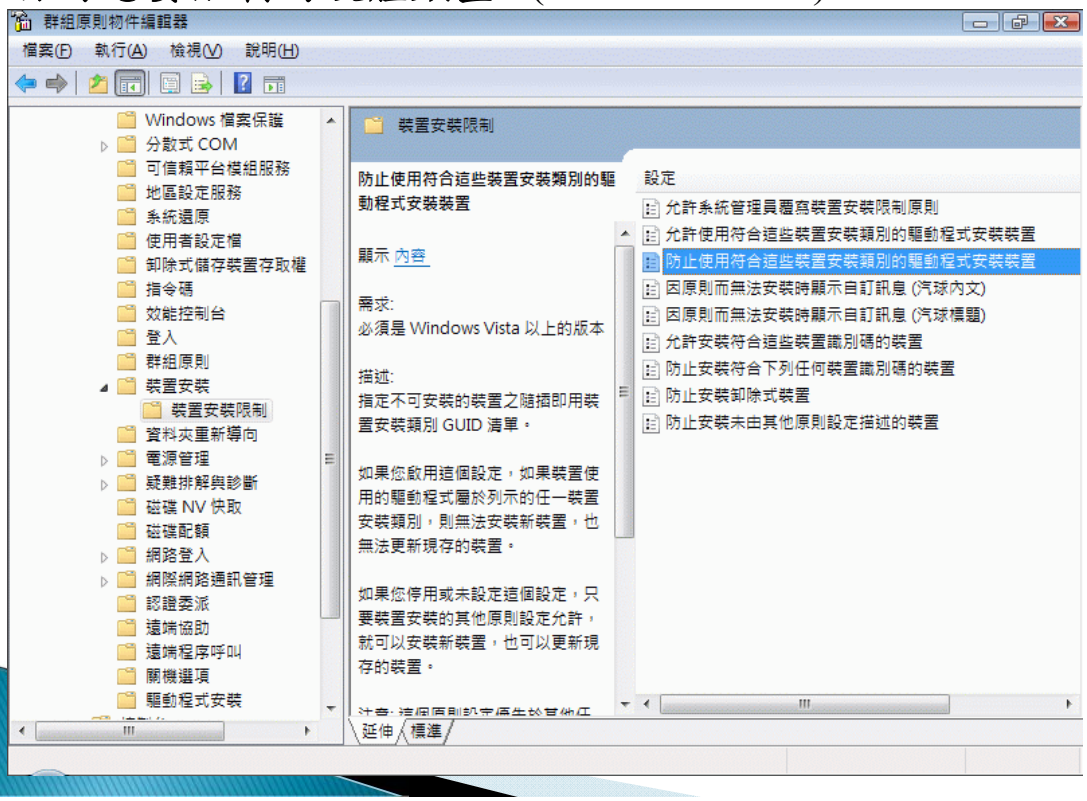
@方法:硬體限制原則

群組原則中預先定義的硬體限制 (Windows Vista)

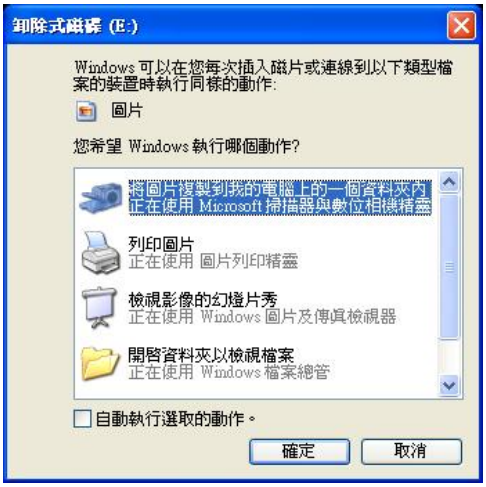


@方法:硬體限制原則

自訂您要限制的硬體類型 (Windows Vista)



@方法:按shift



是關掉autoplay(自動撥放)，不是關掉autorun(自動執行)

@方法:放個autorun.inf

在根目錄下（C.D槽下，和USB中）建立一個檔案夾，名字就叫autorun.inf

這樣一來，因為在同一目錄下，同名的檔案和檔案夾不能共存的原理，病毒就無能為力。但是現已經有新的變種，病毒會自動刪去此資料夾，建立autorun.inf，所以這種方法也變得無效了。

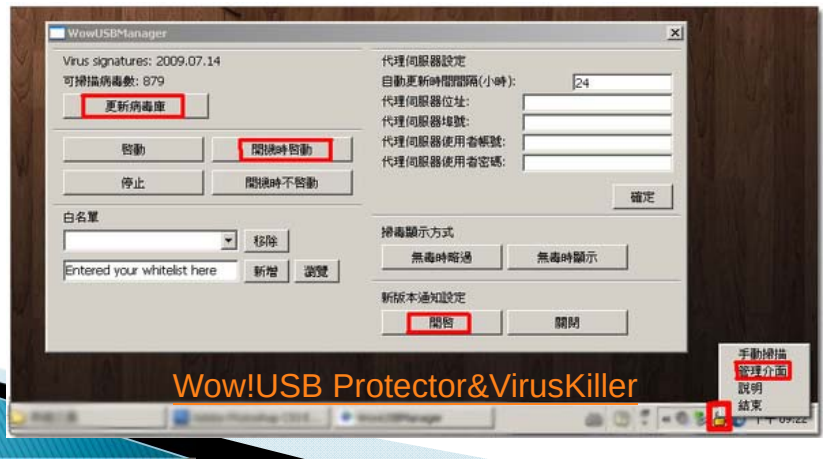
解毒的迷思

- 為什麼防毒軟體有時無法提供有效防護呢？
- 防毒軟體屬於被動防護，必須要有病毒特徵碼，才能偵測與解毒
- 現今病毒都是小區域暴發，不易收集樣本（之前是全球大規則暴發）
- 化被動為主動，善用新的防護技術（免疫防護、啟發式分析、HIPS）才能偵測未知病毒

如何預防USB病毒

如何防範USB類型病毒? (預防勝於治療)

- 不要因為一時好奇，而任意開啟或執行來路不明的檔案
- 在開啟檔案之前，建議先以防毒軟體進行掃瞄
- 定期更新防毒軟體、並執行完整掃瞄
- 透過教育訓練灌輸使用者正確防護概念與良好電腦操作習慣



Wow!USB Protector&VirusKiller

P2P軟體

- Peer to Peer(點對點通訊傳輸工具)
- 檔案分享是目前 P2P 最主要的一種應用，P2P 檔案分享軟體本身是合法的，合不合法 則是在分享的檔案。目前美國的八大影片公司、台灣的 BSA 商業軟體聯盟、 台灣的IFPI 國際唱片業 交流基金會等機構對其 所屬成員的著作權很重視， 而且警方也配合加強取締 ，故請勿下載 非法檔案以免官司上身。

P2P軟體

- P2P軟體透過點對點方式傳輸檔案，例如BitTorrent 、Foxy 、迅雷、PPStream等。
- 有版權的檔案或軟體未經授權而下載使用，即會侵犯到智慧財產權。
- 檔案來路不明，可能包含木馬或病毒程式，容易使您的個人資料曝露在網路當中。

常見的P2P的種類

BitTorrent系列(BT)	BitComet、 BitLord 、BitSpirit、 uTorren、clubbox
eDonkey系列	eDonkey、eMule
Gnutella系列	Gnutella、 ezPeer、 Mxie、Foxy
FastTrack系列	FastTrack、 KaZaA
WinMx系列	WinMx、 Winny、 NapMx
其他	Thunder、Kuro、Azureus、kkbox、Shareaza、BearShare、DC (Direct Connect)、Fileguri/Freechal、Gnucleus、Grokster、Groove Virtual Office、LimeWire、Blubster、Piolet、RockItNet、OpenLITO、Morpheus、Mutella、PeerEnabler、Phex、Pruna、Soribada、SoulSeek、Swapper、XoloX等...

P2P的安全問題

- P2P軟體可能影響的網路安全問題
  - P2P工具包，可能被惡意人員放置木馬後門程式，與病毒蠕蟲。
  - P2P軟體本身的漏洞，造成駭客入侵。
  - 使用P2P軟體，易將本機目錄開放共享，造成資料外洩。
  - 可能造成侵權行為。

Foxy露底好工具

[2011-10-18]

Foxy，是一個強制上傳分享的繁體中文P2P軟件，主要流行在臺灣、香港及澳門。由於Foxy的用戶對該軟件不熟識，在公職場所會下載Foxy軟件的用戶常把政府機關之文件及表格檔案、公司行號之內部文件（會議記錄、採購記錄等）及個人私密資料（賬號、密碼等）洩漏。

2007年4月，Foxy遭發現只要在Foxy的搜尋欄位中鍵入「賬號」、「密碼」，就可以找到其他Foxy使用者儲存在各自電腦內的各種賬號與密碼，包括線上遊戲、即時通訊軟體、ADSL與網路銀行的賬號與密碼。對此，Foxy官方網站論壇發出回應：Foxy 爲單純P2P分享下載軟件，軟件本身不提供、儲存、控制、編輯或修改網路上的任何可被連結或被搜尋的訊息內容或其表現形式。

Foxy也提醒用戶在分享檔案時小心管理資料夾。再次提醒用戶，個人機密性檔案請不要放在共享資料夾，也不要勾選分享資料夾以外的資料夾。

Foxy作爲分享下載軟件，2008年1月至2月，陳冠希裸照事件時，大量網友以Foxy軟體作爲傳播裸照的工具；同年4月，香港亦發生Foxy洩露政府機密事

國泰世華帳號密碼

國泰世華帳號密碼

Foxy P2P造成線民資料外洩

2010-9-7 字型：＋ － | 看推薦 | 發言 | 列印 | 轉寄 | 分享：

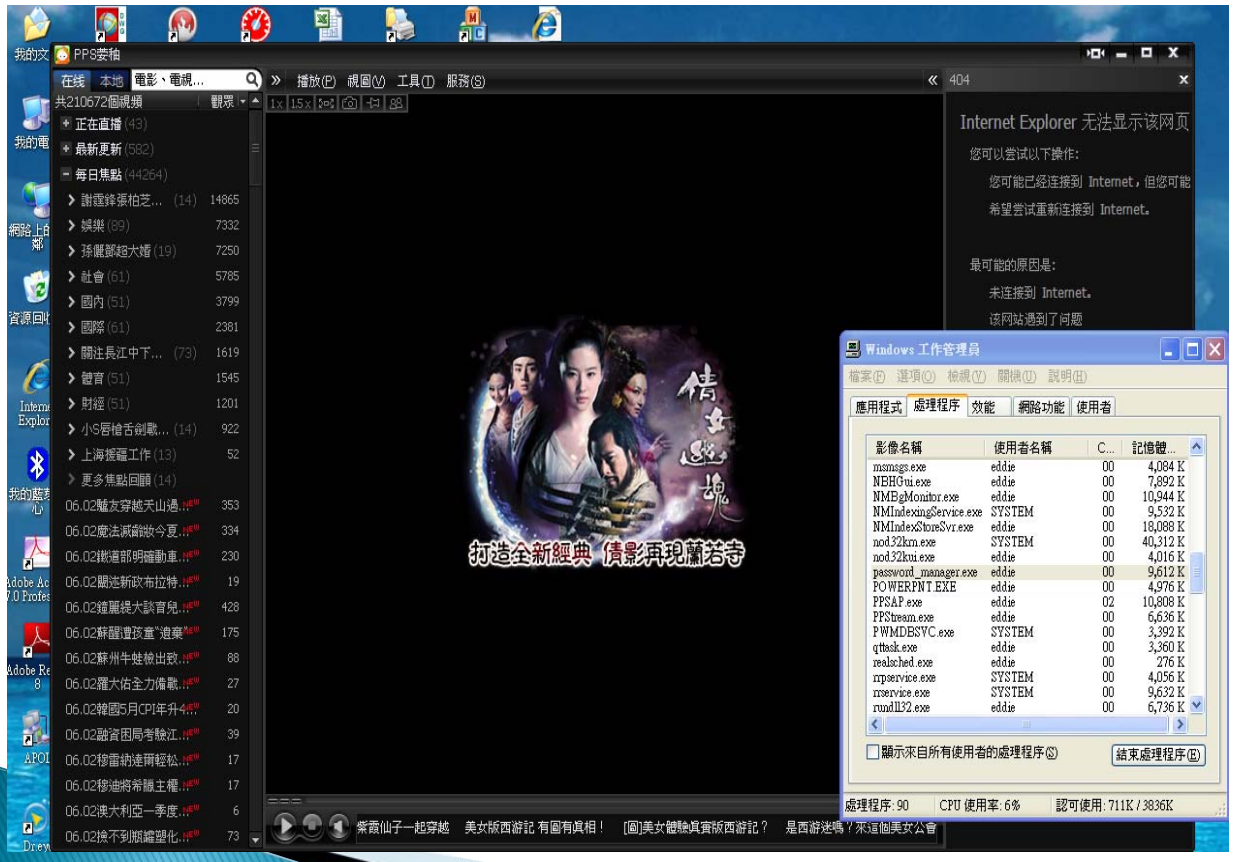
高雄縣調站搞烏龍 線民資料Foxy外洩

〔記者林慶川、黃敦硯／台北報導〕調查局高雄縣調查站一名組長，涉嫌違反資訊通訊安全規定，將佈建的線民資料表存放在隨身碟中，不慎遭Foxy網路共享檔案傳輸，軟體開放分享後遭人下載，造成資料外洩；這是調查局成立至今，首度爆發線民資料外洩事件。

高縣調查站發生線民資料外洩事件。（記者王榮祥攝）

線民資料存在隨身碟

調查局昨晚證實，確有資料外流，但沒有外傳13位線民那麼多，且外洩的只是一般性對象，未造成重大危害，考量當事人並非故意，調查局最後將這名組長記兩次申誡。



P2P預防之道

天下沒有白吃的午餐，用P2P會有潛在的代價

1.不使用P2P軟體。

2.若要安裝，請由官方網站下載，切勿從入口網站隨意下載。

3.請注意分享的資料夾，切勿整顆硬碟分享。

4.請勿長時間開啟P2P軟體，造成駭客入侵。

上網安全守則

- 社交工程與惡意程式防護
  - 防毒軟體不一定有用
    - 病毒碼更新要能即時
  - 作業系統或軟體弱點修補
    - 防止利用弱點進行入侵及植入惡意程式
  - 不隨意下載非法軟體、影片、音樂
  - 不要使用P2P軟體
  - 對可疑電子郵件應有警覺性
- 使用強韌的密碼

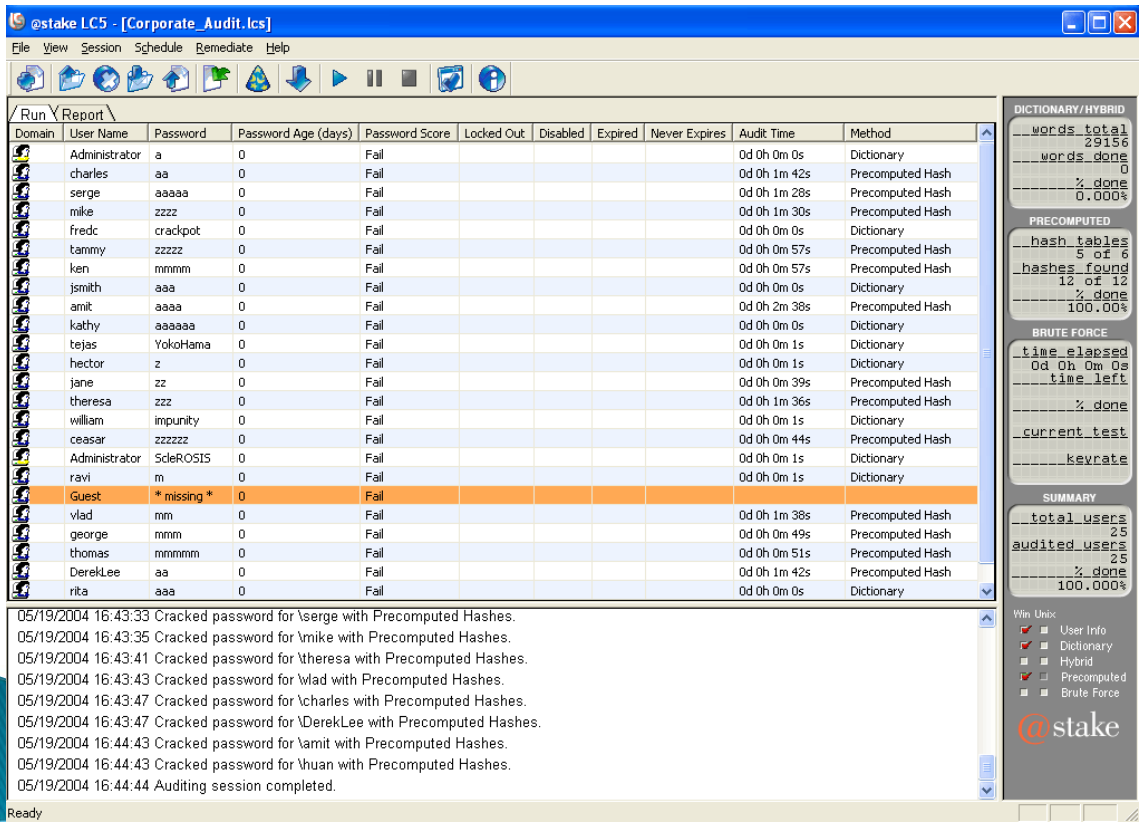
安全的個人密碼設定

- 帳號/密碼的組合，是最常用的身分驗證機制
- 亦是駭客最常攻擊的部分
- 您的密碼不應該包含：
  - 生日組合(601023)
  - 太短或英文單字(hsiuping)
  - 家人、情人、寵物的名字
  - 倒著打(gnipuish)
  - 出現頻率太高(0000)或太連續(abc123)
  - 一組密碼行遍天下

安全的個人密碼設定

- 您的密碼應該要：
  - 大小寫英文、符號、數字混合(I'mGaY@5438)
  - 長度足夠，建議六個字元以上
  - 使用國語或台語拼音，組合成較長且無英文字義的字母串，卻又容易記憶。例如「warDerMeeMar」(我的密碼)。
  - 不要使用自己的基本資料當密碼，例如：出生日期、身份證字號、姓名。
  - 不要依英文及數字在鍵盤上的排列位置輸入密碼，例如：qwerty、asdfgh等。
  - 定期變更密碼(很難做到)
- 不在不安全的電腦(網咖、共用電腦)輸入密碼

密碼破解軟體



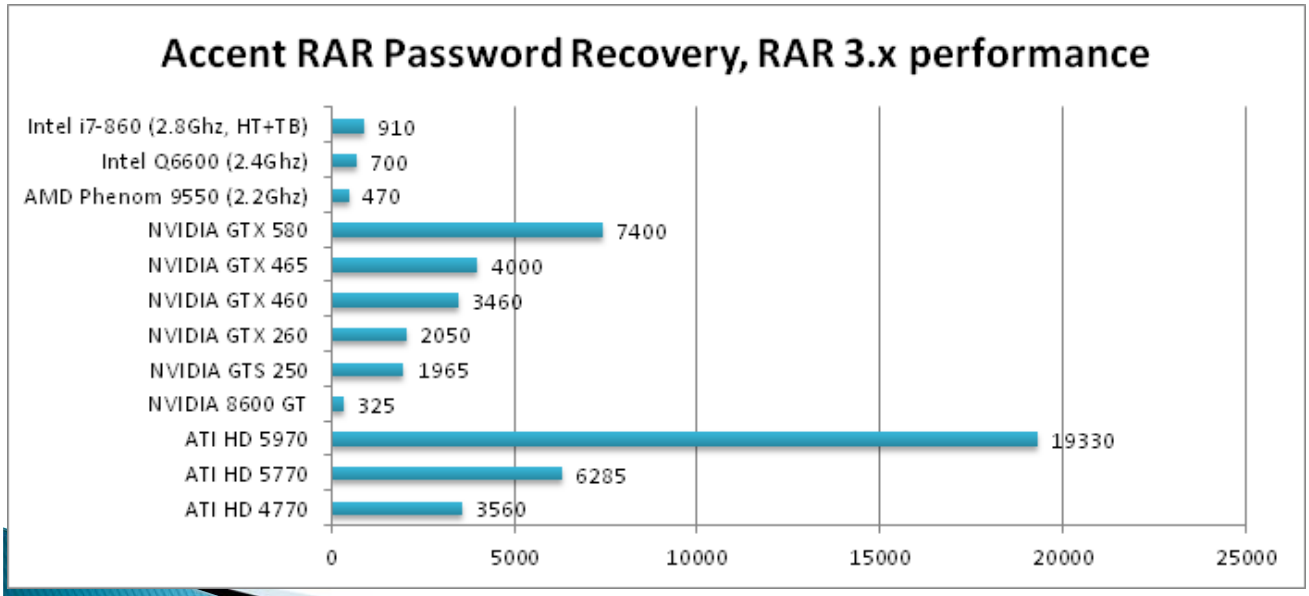
雙核心CPU電腦破解密碼時間統計表

密碼組合內容	破解時間	
	密碼長度六位	密碼長度八位
數字密碼（10）	1秒以內	348分鐘
大小寫字母（52）	33分鐘	62天
大小寫字母＋數字（62）	1.5小時	253天
大小寫字母＋數字＋符號（96）	22小時	23年

本研究整理，資料來源：http://www.lockdown.co.uk (2006)

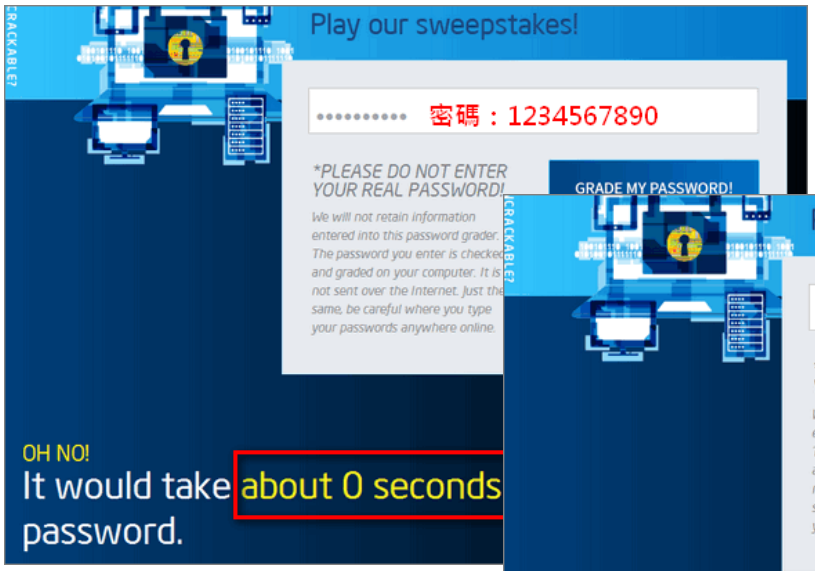
顯示卡GPU

- 顯示卡GPU取代CPU成為暴力運算新選擇



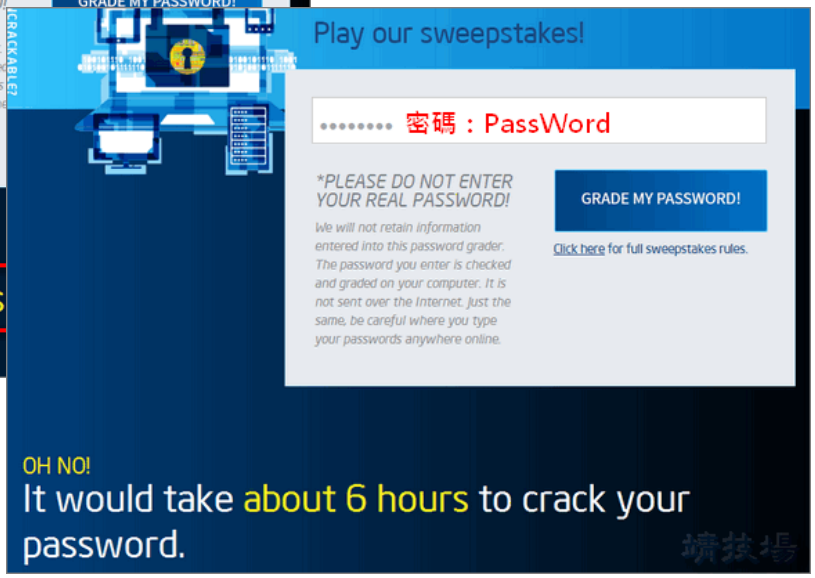
你的密碼強度夠安全嗎？多久會被破解？

https://www-ssl.intel.com/content/www/us/en/forms/passwordwin.html



簡單的密碼

英文字配合大寫



你的密碼強度夠安全嗎？多久會被破解？

以英文、數字、特殊符號的組合測試，沒想到不到1秒鐘就被破了，可見若字母、數字的排列若是常見的，應該也很容易被破解

線上產生器來產生長度8的密碼

你的密碼強度夠安全嗎？多久會被破解？

超長的「簡單」密碼

簡單的英文，只是長度比較長一點

結論

- 結合社交工程攻擊為我政府機關公務資訊遭竊之最主要威脅
- 鎖定目標、假冒身份及公務相關訊息之偽冒電子郵件防不勝防
- 最大的問題可能也來自於自己本身，畢竟每人都參與其中，若想解決，另一方法是從自己開始。
- 政府資訊安全工作除了健全的基礎設施外，最重要的是先做好個人的資訊安全，只要機關同仁養成良好的使用習慣，人人隨時做好資訊安全第一線防護，機關內部資訊安全就能得到保障，進而提升我國整體資訊安全防護

問題與討論