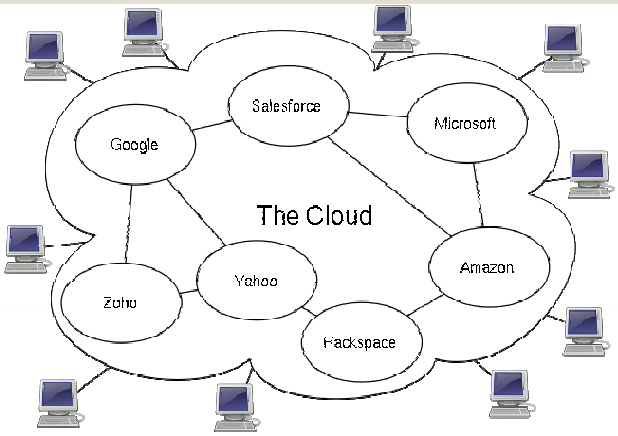
網路攻防戰
之
實務案例
密碼防竊篇

講師 呂守箴

大綱：

- 何謂雲端運算
- 密碼竊取
- 單機電腦
  - 單機電腦常見的錯誤方式？
  - 重設登入密碼
  - 挖出電腦密碼
  - 破解文件密碼
- 網路上的芳鄰
  - 網路上的芳鄰常見的錯誤方式？
  - 側錄網路封包密碼
  - 破解無線網路密碼
  - 是否跨Switch監聽？
  - 預設帳號/密碼的問題
- 網際網路
  - 網際網路常見的錯誤方式？
  - 上網密碼
  - 外洩管道
  - 側錄、搜尋、中毒、社交網站
- 防竊對策
  - 密碼設定與保護
  - 密碼學
  - 竊取密碼的4大手段：
    - 暴力破解密碼
    - 顯示密碼
    - 側錄sniffer密碼
    - 木馬竊取

何謂雲端運算



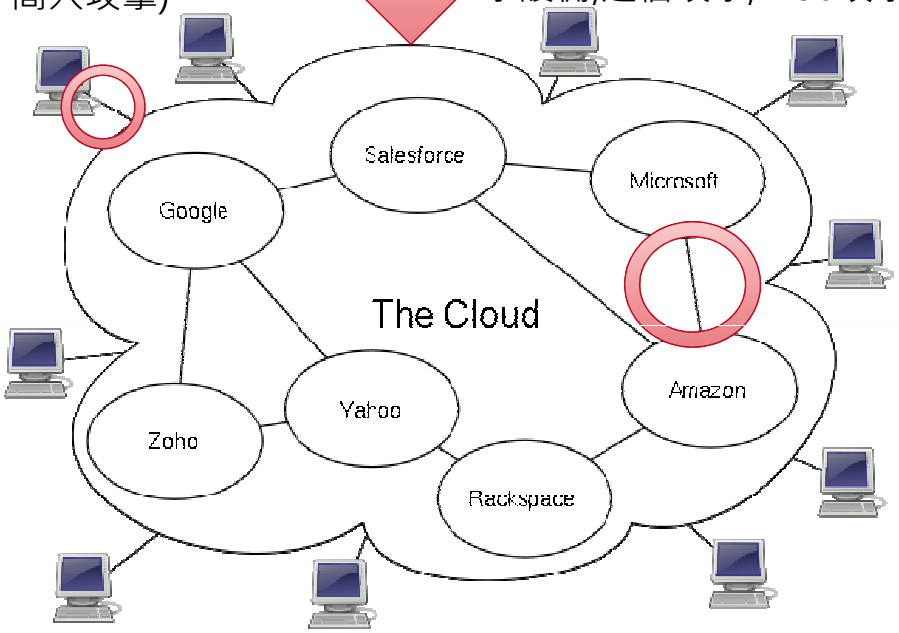
- 雲端的基本概念，是透過網路將龐大的運算處理程式自動分拆成無數個較小的子程式，再由多部伺服器所組成的龐大系統搜尋、運算分析之後將處理結果回傳給使用 者。
- 透過這項技術，遠端的服務供應商可以在數秒之內，達成處理數以千萬計甚至億計的資訊，達到和「超級電腦」同樣強大效能的網路服務。

何謂雲端運算

- 雲端運算可以認為包括以下幾個層次的服務：基礎設施即服務（IaaS），平台即服務（PaaS）和軟體即服務（SaaS）。
- 雲端運算服務通常提供通用的透過瀏覽器存取的線上商業應用，軟體和資料可儲存在資料中心。
- 維基百科對於雲端服務的說明：
- http://zh.wikipedia.org/wiki/雲端運算

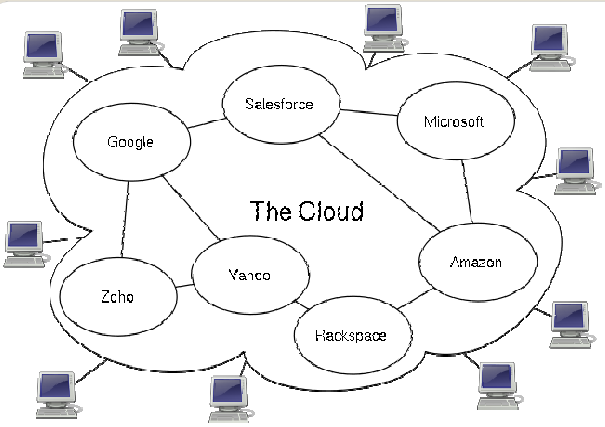
3.攻擊使用者與雲端之間的連線。(例：DDoS,中間人攻擊)

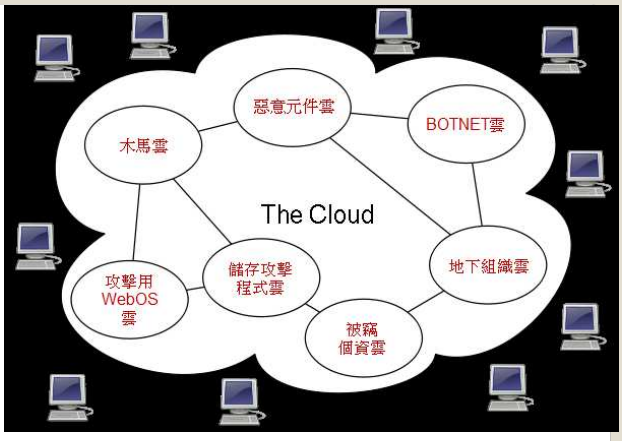
1.攻擊雲端本身。(例：DDoS,攻擊設備,退信攻擊,Web攻擊)

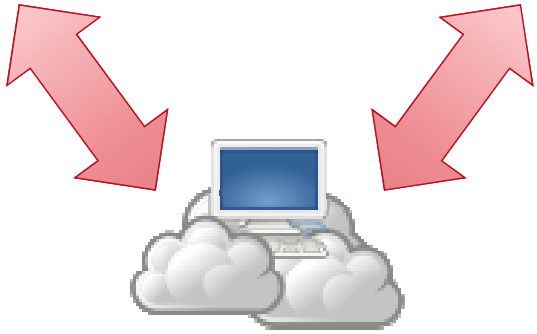


2.攻擊雲端週邊。(例：DNS欺騙,憑證偽冒,中間人攻擊)

4.攻擊雲端使用者。(例：社交工程,竊取帳號/密碼)







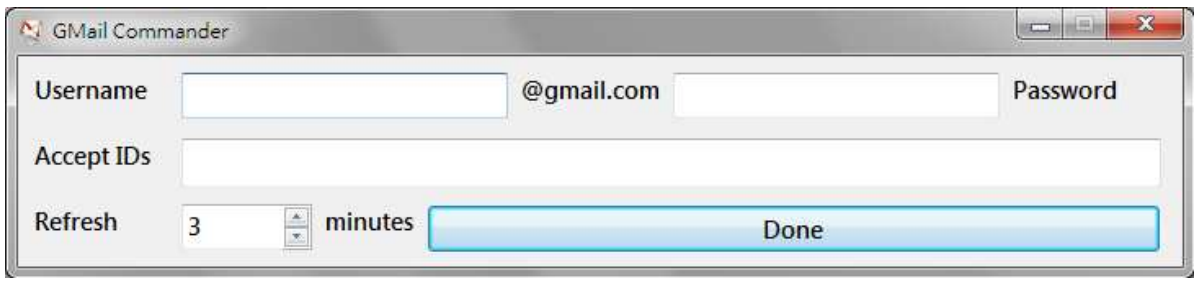
5.建立駭客雲利用合法管道攻擊(例：以合法掩護非法)

雲端攻擊入侵：

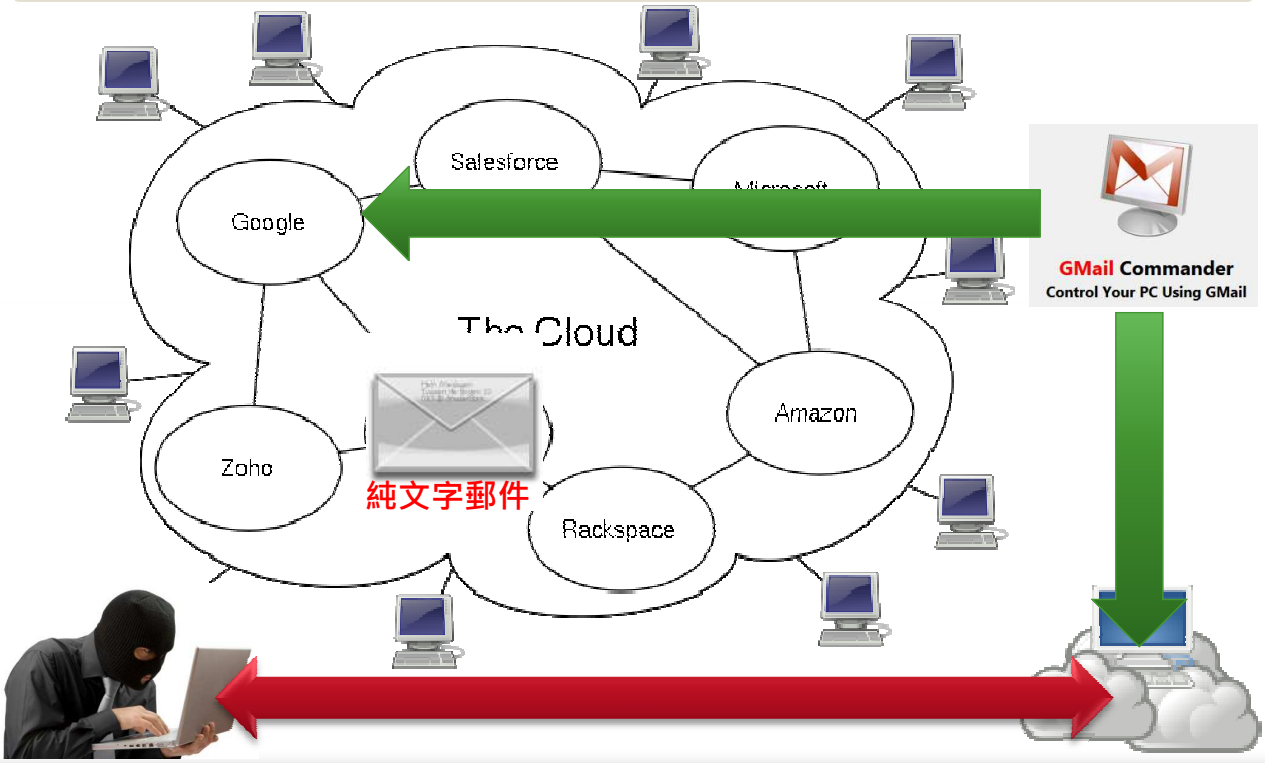
1. 攻擊雲端本身。(例：DDoS,攻擊設備,退信攻擊,Web攻擊)
2. 攻擊雲端週邊。(例：DNS欺騙,憑證偽冒,中間人攻擊)
3. 攻擊使用者與雲端之間的連線。(例：DDoS,中間人攻擊)
4. 攻擊雲端使用者。(例：社交工程,竊取帳號/密碼)
5. 建立駭客雲利用合法管道攻擊(例：以合法掩護非法)

GMail Commander

- GMail Commander 是一種檢查信件的軟體，它允許於檢查信件的同時，接受來自於Gmail信箱所發送的各種控制指令，來進行遠端遙控。
- 註：遠端遙控部分需自行於Gmail中撰寫批次檔，或者呼叫系統的捷徑列。

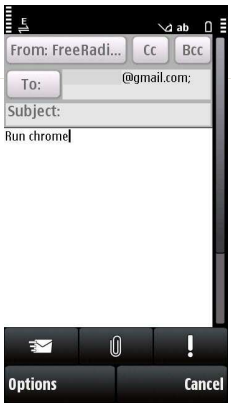


GMail Commander



GMail Commander

- 問題點：
- 發送純文字檔的信，而目標電腦並沒有把信接收下去的狀態下去控制及觸發對方電腦起床工作了。



- 參考資料 (原始碼)：
- http://www.autohotkey.com/forum/topic67120.html

單機電腦：

- 重設登入密碼
  - ERD Commander
  - Offline NT Password & Registry Editor
- 挖出電腦密碼
  - Windows Password Recovery Tools 工具組
  - 星號密碼顯示器
- 破解文件密碼
  - ElcomSoft Password Recovery Tools 工具組

單機電腦：重設登入密碼

- 狀況：
- 突然忘記XP的登入密碼怎麼辦？
- 萬一急需要用這台電腦不就沒轍了嗎？
- 如果有同事離職，沒有交接電腦登入密碼，剛好有些客戶資料在他電腦裡怎麼辦，要拆硬碟嗎？
- 幸好XP的密碼保護機制很不完善我們需要特殊軟體來重設密碼。

單機電腦：重設登入密碼

- 軟體名稱：ERD Commander
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：讓使用者利用光碟開機的方式使用電腦，修復已毀損的Windows作業系統。屬於一種Windows Live CD雖然可以自己動手做出來(前提是你要有原版光碟才合法)，且在網路上有流傳ISO檔，但由於內含Windows核心，不能公開散佈，在此僅做特殊功能介紹。
- 註：此為利用開機光碟”重設”administrator密碼。
- 參考網址：http://pcnoproblem.twbbs.org/erd-commander-windows-lock/

單機電腦：重設登入密碼

- 軟體名稱：Offline NT Password & Registry Editor
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：Windows核心作業系統的使用者帳戶資訊和密碼，都在一個"SAM"檔案裡面。路徑通常在\windows\system32\config，是registry的一部分。因此本軟體就是在進入作業系統前，更改"SAM"檔案的內容，達到破解密碼的目的。
- 參考網址：http://pcnoproblem.twbbs.org/offline-nt-password-registry-editor/

單機電腦：挖出電腦密碼

- 狀況：
- 平常沒有記憶密碼的習慣，如果電腦有自動記錄，就讓電腦記憶。
- 密碼設定得太複雜或改得太頻繁，改到自己忘了到底現在該用哪一組進去？
- 萬一電腦要重灌，麻煩的是到底有多少軟體、網站，當初申請的密碼是多少？
- 也許我不需要破解別人的密碼，因為我連自己的密碼都記不起來。

單機電腦：挖出電腦密碼

- 軟體名稱： Windows Password Recovery Tools 工具組(包含：如下表格)
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：原理：從系統的暫存檔、登錄檔、cookies、應用程式的安裝檔、設定檔內將儲存的密碼檔案"顯示"出來，並非使用暴力破解所計算出來。
- 註：部分防毒軟體可能會認為這類軟體為木馬或惡意程式，如果有疑慮請勿使用 。
- 參考網址： http://briian.com/?p=6910

軟體名稱	主要功能：顯示以下軟體的密碼
MessenPass	顯示MSN /Windows Live Messenger, Yahoo Messenger, ICQ , AOL , Trillian, Miranda, GAIM
Mail PassView	顯示Windows Live Mail, Outlook Express, Microsoft Outlook 2000/2002/2003/2007, Eudora, Mozilla Thunderbird, HotMail, Yahoo!, Gmail
IE PassView	顯示 IE 4, IE5, IE6, IE7, IE8 所暫存的密碼
Dialupass	Windows 2000, XP, Vista, 2003, 2008, 7的撥號軟體
Network Password Recovery	Windows 2000, XP, Vista, 2003, 2008, 7的網芳密碼
SniffPass	側錄 Web/FTP/Email 的密碼
WebBrowserPassView	顯示Internet Explorer (Version 4.0 ~ 8.0), Mozilla Firefox (All Versions), Google Chrome, Opera 密碼
WirelessKeyView	顯示 WEP/WPA 所儲存在電腦的密碼
Remote Desktop PassView	顯示 遠端桌面軟體 所暫存在電腦的密碼
VNCPassView	顯示 VNC遙控軟體 所儲存在 Registry(HKEY_CURRENT_USER) 的密碼

單機電腦：挖出電腦密碼

- 軟體名稱：星號密碼顯示器 (俠客密碼查看器)
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：通常軟體介面所顯示的*****是利用程式語法"遮蔽"所出現的效果，顯示程式只是還原該遮蔽原本的樣子。所以依其設計原理"無法顯示"儲存在資料庫並經加密處理過的密碼。
- 註：本軟體為：大陸貨。防毒軟體可能會認為這類軟體為木馬或惡意程式，如果有疑慮請勿使用 。
- 參考網址： http://www.ancisoft.com/password/viewpass/viewpass.htm

單機電腦：破解文件密碼

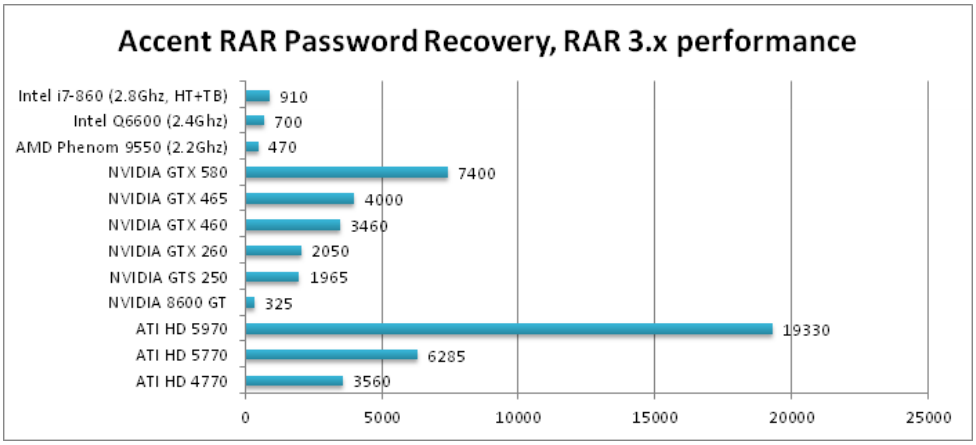
- 狀況：
- 為什麼文件要鎖密碼？
  - 鎖定部份功能：禁止修改、禁止列印
  - 防止被他人盜用
  - 防止格式跑掉
- 為什麼要破解文件密碼？
  - 該死的又忘記密碼了
  - 原稿已經遺失
  - 陳年舊檔找不到當初鎖定的人了

單機電腦：破解文件密碼

- 軟體名稱：ElcomSoft Password Recovery Tools 工具組(包含：如下表格)
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：支援 NVIDIA 及 ATI 的獨立繪圖處理器(GPU)提高運算功能 ，視不同軟體提供：覆蓋密碼、暴力破解、字典檔比對、分散式運算等。
- 註：本軟體為：商用軟體(試用版僅提供破解部份密碼)。防毒軟體可能會認為這類軟體為木馬或惡意程式，如果有疑慮請勿使用 。
- 參考網址： http://www.elcomsoft.com/products.html

顯示卡GPU取代CPU成為暴力運算新選擇

- 透過顯示卡GPU龐大的平行運算效能來猜密碼、也就是所謂的暴力破解（Brute Force）方式，將近100張顯示卡的測試數據建立成龐大的GPU運算效能資料庫。



- 參考資料： http://www.golubev.com/blog/

軟體名稱	主要功能：
ElcomSoft Password Recovery Bundle	針對企業及政府單位所推出的密碼復原軟體。
Elcomsoft Wireless Security Auditor	提供 WPA/WPA2 的密碼運算與 Wi-Fi sniffer 的功能。
Elcomsoft Internet Password Breaker	提供 Internet Explorer, Firefox, Safari, Chrome, and Opera, Outlook Express, Microsoft Outlook, Windows Mail, Windows Live Mail 的密碼運算。
Advanced Archive Password Recovery	提供所有 ZIP 及 RAR等壓縮軟體的密碼運算，包含：PKZip, WinZip, WinRAR 等
Advanced Office Password Recovery	提供 Microsoft Office 97~2010等版本的密碼運算，包含：Word, Excel, Powerpoint, ACCESS, Outlook, Project, OneNote, Visio, Publisher, VBA等
Advanced PDF Password Recovery	一般格式的PDF檔案，在平均 40-bit keys 以下可以在不到1分鐘之內被運算出來。
Advanced SQL Password Recovery	提供 Microsoft SQL Server 2000, 2005, 2008等版本的密碼運算。
Advanced IM Password Recovery	提供 MSN, Yahoo, AOL, ICQ等軟體的密碼運算。
Elcomsoft Phone Password Breaker	提供 BlackBerry, iPhone, iPad, iPod 的備份檔密碼運算。
Lightning Hash Cracker	提供 MD5 hashes 的密碼運算。

網路上的芳鄰：

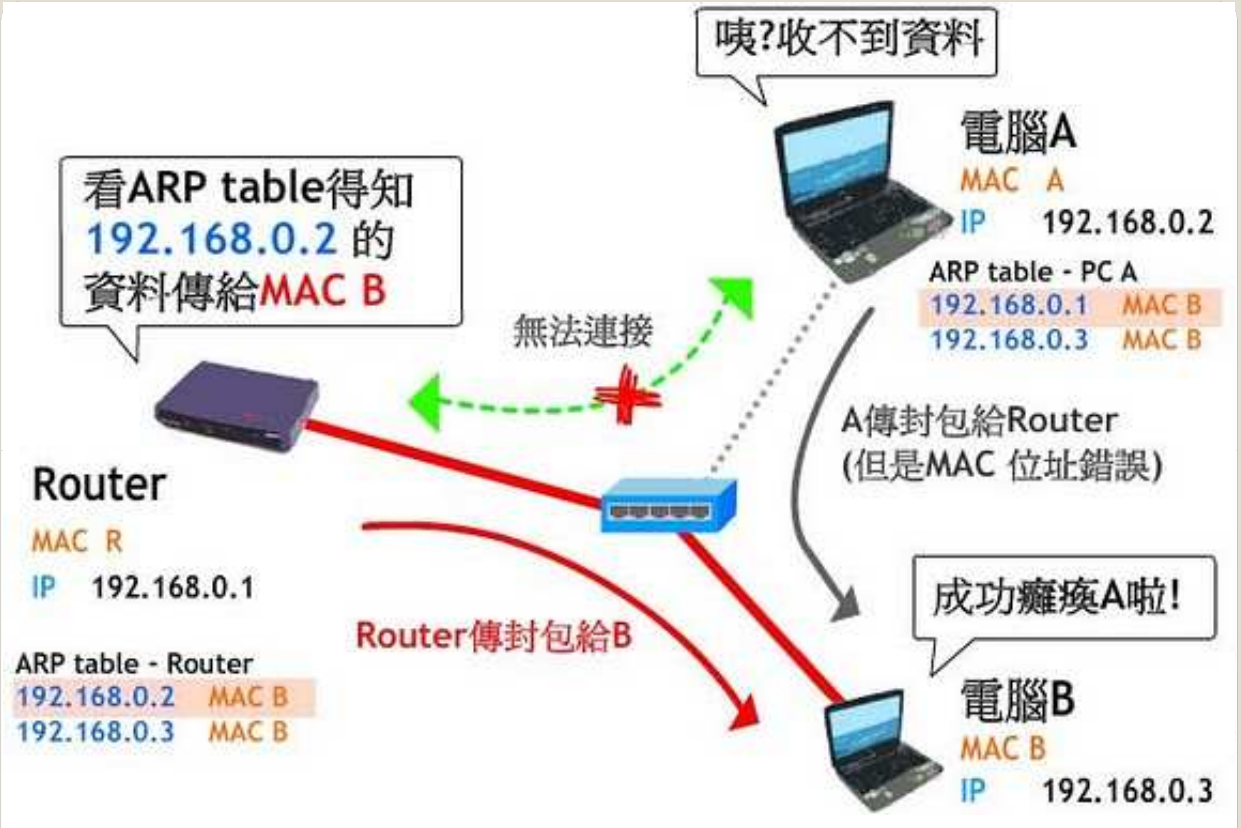
- 側錄網路封包密碼
  - Network Password Recovery
  - SniffPass
  - Remote Desktop PassView
  - Cain & Abel (該隱與亞伯)
- 破解無線網路密碼
  - WirelessKeyView
  - Elcomsoft Wireless Security Auditor
  - NetStumbler, Airopeek, WEPCrack, AirDump
- 是否跨Switch監聽？
- 預設帳號/密碼的問題

網路上的芳鄰：側錄網路封包密碼

- 軟體名稱： Wireshark (以前稱Ethereal)
- 下載網頁： http://www.wireshark.org
- 軟體說明： Wireshark 是一個網路封包分析軟體。網路封包分析軟體的功能是截取網路封包，並盡可能顯示出最為詳細的網路封包資料。
- 註：
- Wireshark不是入侵偵測軟體，對於網路上的異常流量行為，不會產生警示或是任何提示。
- Wireshark不會對網路封包產生內容的修改，也不會送出封包至網路上。
- 參考網址： http://sls.weco.net/CollectiveNote20/Wireshark

網路上的芳鄰：側錄網路封包密碼

- 軟體名稱：Cain & Abel (該隱與亞伯)
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：Cain & Abel利用的是ARP這個協定的漏洞，透過一種叫做「ARP Spoofing」的技巧，欺騙特定的電腦取得封包資料，簡稱中間人攻擊(Man-in-the-middle attack,MITM)。
- 註：防毒軟體可能會認為這類軟體為木馬或惡意程式，如果有疑慮請勿使用 。
- 參考網址： http://mmdays.com/2008/11/10/mitm/



參考網址： http://forum.icst.org.tw/phpbb/viewtopic.php?t=15631

網路上的芳鄰：是否跨Switch監聽？

- Port Mirror 的好處：
- 內建於網路設備能看到通過交換器的流量。

- Port Mirror 的缺點：
- Port Mirror 是在交換器管理軟體中設定的，而錯誤的設定可能導致網路擁塞。且並不是100%的流量都被複製到輸出埠，所以當交換器擁塞時，複製的流量可能會有封包遺失的狀況。

網路上的芳鄰：預設帳號/密碼的問題

- 軟體名稱：Ncrack
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：Ncrack是一個高速的網絡認證破解工具，採用了模塊化設計其類似Nmap的命令行語法和動態的引擎，可以幫助企業測試所有的網絡主機和網絡設備的密碼強度，提高企業網絡的安全性。。
- 註：Ncrack屬於開放原始碼軟體，支援 RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, and telnet 等通訊協定。
- 參考網址： http://nmap.org/ncrack/

網路上的芳鄰：預設帳號/密碼的問題

- 網路設備完成安裝作業後，應立即變更該設備之預設帳號密碼/原廠密碼。

- Default Password List
- http://www.phenoelit-us.org/dpl/dpl.html

網際網路：

- 上網密碼
  - 遊戲密碼
  - 相簿密碼
  - 網站、論壇密碼
- 外洩管道
  - 側錄
    - HTTP sniffer
    - MSN sniffer
  - 搜尋
    - Google
    - P2P
  - 中毒
    - 木馬程式鍵盤側錄
    - Facebook社交網站

網際網路：外洩管道：側錄(sniffer,嗅探器)

- Wireshark (以前稱Ethereal)
- Cain & Abel (該隱與亞伯)
- MSN Sniffer
- HTTP Sniffer

網際網路：外洩管道：側錄(sniffer,嗅探器)

- 軟體名稱：EffeTech Network Monitoring Software 工具組(包含：如下表格)
- 下載網頁：請利用搜尋引擎搜尋
- 軟體說明：提供了一系列網絡診斷和網絡管理軟的軟體，幫助家長、網絡管理員和網絡開發者加速開發與確認網路的濫用。
- 註：本軟體為：商用軟體(試僅提供15天完整版試用)。防毒軟體可能會認為這類軟體為木馬或惡意程式，如果有疑慮請勿使用 。
- 參考網址： http://www.effetech.com

軟體名稱	主要功能：
MSN Sniffer	MSN嗅探器
EtherDetect Packet Sniffer	網路封包嗅探器
EffeTech HTTP Sniffer	http嗅探器
Ace Password Sniffer	http, ftp, smtp, pop3, telnet 的密碼嗅探器
AIM Sniffer	AIM (AOL Instant Messenger)嗅探器
ICQ Sniffer	ICQ嗅探器
EtherBoss MSN Monitor	MSN嗅探器

網際網路：外洩管道：搜尋

- 網路蜘蛛是搜尋引擎用來自動搜集資訊的程式，對它而言，網站上的內容不分機密與否，只要有路可進，它就會登臨造訪，並且將內容回傳搜尋業者的資料庫。
- 網路蜘蛛也可稱為網路機器人，當網路蜘蛛掃描網站時，通常從一個或多個網站開始，它會掃描頁面中的連結並記錄，透過鎖定網頁HTML語法中的HREF標籤，抓取尾隨其後的網址連結，並比對後端資料庫，檢查是否有新的連結產生，以及是否有斷裂、失效的連結。

  因為有網路蜘蛛，除了致使企業有不當資訊外洩的風險，有時也會造成網頁伺服器的負擔，例如短時間內不斷且大量擷取資料，而使伺服器服務品質變差。
- 不能『搜』的秘密：
  - Google
  - P2P

網際網路：外洩管道：搜尋：google

- 基本語法與關鍵字

- site: (搜尋特定網址)
- inurl: (搜尋特定連結)
- intext: (搜尋網頁內文字)
- intitle: (搜尋網頁標題)
- filetype: (搜尋特定檔案格式)
- link: (搜尋互相連結的網頁)
- "index of" (搜尋開放目錄瀏覽)
- cache: (顯示網頁在google中的暫存資料)

- 參考網址：
- http://www.google.com/advanced_search
- http://www.google.com/codesearch?hl=zh-TW
- http://anti-hacker.blogspot.com/2007/01/web.html

網際網路：外洩管道：搜尋：google

"Index of /admin"
"Index of /password"
"Index of /mail"
"Index of /" +passwd
"Index of /" +password.txt
"Index of /" +.htaccess
index of ftp +.mdb allinurl:/cgi-bin/
+mailto

administrators.pwd.index
authors.pwd.index
service.pwd.index
filetype:config web
gobal.asax index

allintitle: "index of/admin"
allintitle: "index of/root"
allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:gov

allinurl: winnt/system32/ (get cmd.exe)
allinurl:/bash_history

inurl:passwd filetype:txt
inurl:admin filetype:db
inurl:iisadmin
inurl:"auth_user_file.txt"
inurl:"wwwroot/*."

top secret site:mil
confidential site:mil

intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"index of" passwd
intitle:"index of" people.lst
intitle:"index of" pwd.db
intitle:"index of" etc/shadow
intitle:"index of" spwd
intitle:"index of" master.passwd
intitle:"index of" htpasswd
intitle:"index of" members OR accounts
intitle:"index of" user_carts OR user_cart

網際網路：外洩管道：搜尋：google

網際網路：外洩管道：搜尋：google

- 搜尋引擎過濾單位機密資料方法
- http://gsn-cert.nat.gov.tw/forgoogle.html

- 從 Google 的索引中移除我的內容
- http://www.google.com/support/webmasters/bin/answer.py?hl=b5&answer=136868

- 知名搜尋引擎Web入侵手法
- http://anti-hacker.blogspot.com/2007/01/web.html

- Google Hacks
- http://anti-hacker.blogspot.com/2007/06/google-hacks.html

- 入侵你家的網路監視器！
- http://anti-hacker.blogspot.com/2007/06/blog-post_18.html

網際網路：外洩管道：中毒

- 木馬程式鍵盤側錄
  - 遊戲木馬
  - 網頁木馬
- Facebook社交網站
  - XSS病毒
  - 隱私與安全性設定

網際網路：外洩管道：中毒：木馬程式側錄

- 木馬程式技術發展可以說非常迅速。主要是有些年輕人出於好奇，或是急於顯示自己實力，不斷改進木馬程式的編寫。至今木馬程式已經經歷了六代的改進：
- 第一代：
- 是最原始的木馬程式。主要是簡單的密碼竊取，透過電子郵件發送資訊等，具備了木馬最基本的功能。
- 第二代：
- 在技術上有了很大的進步，冰河是中國木馬的典型代表之一。
- 第三代：
- 主要改進在資料傳遞技術方面，出現了ICMP等型別的木馬，利用畸形報文傳遞資料，增加了防毒軟體查殺識別的難度。
- 第四代：
- 在行程隱藏方面有了很大改動，採用了核心插入式的嵌入方式，利用遠端插入執行緒技術，嵌入DLL執行緒。或者掛接PSAPI，實作木馬程式的隱藏，甚至在Windows NT/2000下，都達到了良好的隱藏效果。灰鴿子和蜜蜂大盜是比較出名的DLL木馬。
- 第五代：
- 驅動級木馬。驅動級木馬多數都使用了大量的Rootkit技術來達到在深度隱藏的效果，並深入到核心空間的，感染後針對防毒軟體和網路防火牆進行攻擊，可將系統SSDT初始化，導致防毒防火牆失去效應。有的驅動級木馬可駐留BIOS，並且很難查殺。
- 第六代：
- 隨著身份認證UsbKey和防毒軟體主動防禦的興起，黏蟲技術型別和特殊反顯技術型別木馬逐漸開始系統化。前者主要以盜取和篡改使用者敏感資訊為主，後者以動態口令和硬證書攻擊為主。PassCopy和暗黑蜘蛛俠是這類木馬的代表。
- 維基百科對於木馬的說明：
- http://zh.wikipedia.org/wiki/特洛伊木馬 (電腦)

網際網路：外洩管道：中毒：社交網站

- 傳遞病毒管道：

- 聊天室
- 塗鴉牆
- 轉貼連結
- 讚
- 照片標記
- Facebook Hack
  - Facebook hack password
  - Facebook XSS

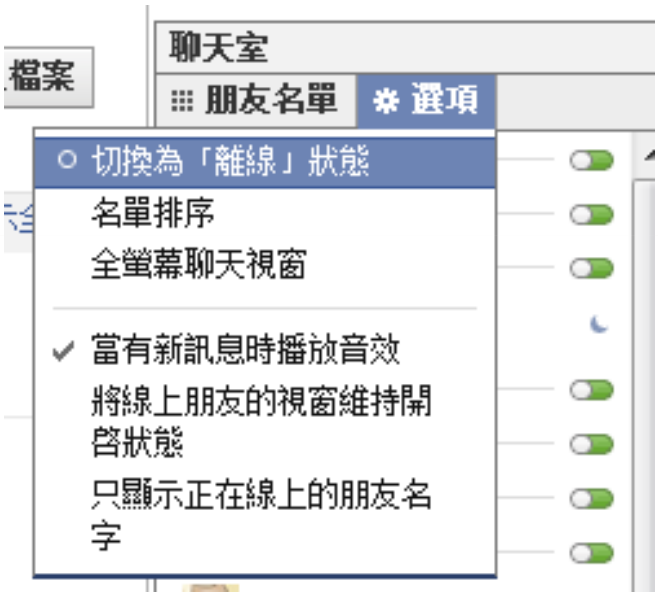
Facebook傳輸病毒管道：聊天室

- 症狀：
- 不斷從你的好友名單中，透過聊天室傳遞有毒的連結與網址，好友不留意點選即會感染。

Facebook傳輸病毒管道：聊天室

- 解決策略：

- 不要點擊
- 重複確認
- 掃毒連結
- 關閉聊天室

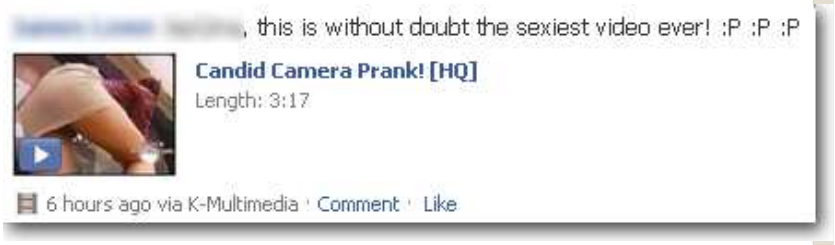


Facebook傳輸病毒管道：塗鴉牆\按讚

- 症狀：
- 在你自己的塗鴉牆，大量出現朋友，轉貼好康或者警告的訊息，不斷傳遞連結、圖片、影片，誘發你的好奇心來點選。

Facebook傳輸病毒管道：轉貼連結

- 症狀：
- 遭到鎖定的使用者會收到假冒的聯絡人送來的訊息。



- 此訊息內含一個連結並會要求使用者必須下載 撥放軟體才能觀賞影片。。

Facebook傳輸病毒管道：塗鴉牆

- 解決策略：

- 不要點擊
- 重複確認
- 掃毒連結
- 關閉塗鴉牆(設定你的隱私分享權限)

Facebook傳輸病毒管道：照片標記

- 症狀：
- 打開facebook到自己的個人首頁，一堆來自於朋友的「心理唬弄測驗」、「送你一個什麼碗糕」、「今天誰是你的最佳煞星」、「每日精選一坨狗屎」....
- 這些訊息如果您覺得不舒服，但自己也有玩這些什麼東東的，您可能一樣洗了朋友的塗鴉牆，並且也正令您的朋友不舒服中...

Facebook傳輸病毒管道：照片標記

- 解決策略：
- **不要玩**
- 不要點擊
- 關閉照片標記(設定你的隱私分享權限)

密碼設定與保護：

- 密碼學
- 竊取密碼的4大手段：
- 暴力破解密碼 →防範：密碼複雜化
  - 密碼設定的相關事項
  - 圖形密碼驗證
- 顯示密碼passview →防範：清除暫存資料
- 側錄sniffer密碼 →防範：加密
- 木馬竊取 →防範：掃毒
  - 螢幕小鍵盤
  - 動態鍵盤
  - 密碼安全鎖
  - 修補漏洞

密碼設定與保護

- 密碼學：
- 傳統意義上來說，是研究如何把資訊轉換成一種隱蔽的方式以防止其他人獲得。

- 維基百科對於密碼學的說明：
- http://zh.wikipedia.org/wiki/Category:密碼學

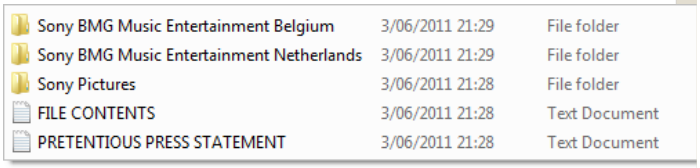
竊取密碼的4大手段：暴力破解密碼

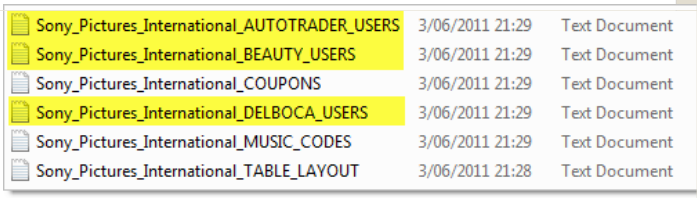
- 防範措施：
- 將密碼增加字串長度並複雜化，使其需要花費相當長的運算時間來破解，來換取保護的時間。

- 密碼設定的相關事項
- 圖形密碼驗證

關於被竊取的帳號與密碼分析

- 相信許多人都已經知道Sony 被駭客入侵，除了七千多萬筆的SonyPlaystation Network帳號被入侵盜走之外，並且發現有超過一百萬筆的帳號密碼是以明碼儲存，這些資料已經被人放到BT上提供下載。





- 參考資料：
- http://www.inside.com.tw/2011/06/13/sony-password
- http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html

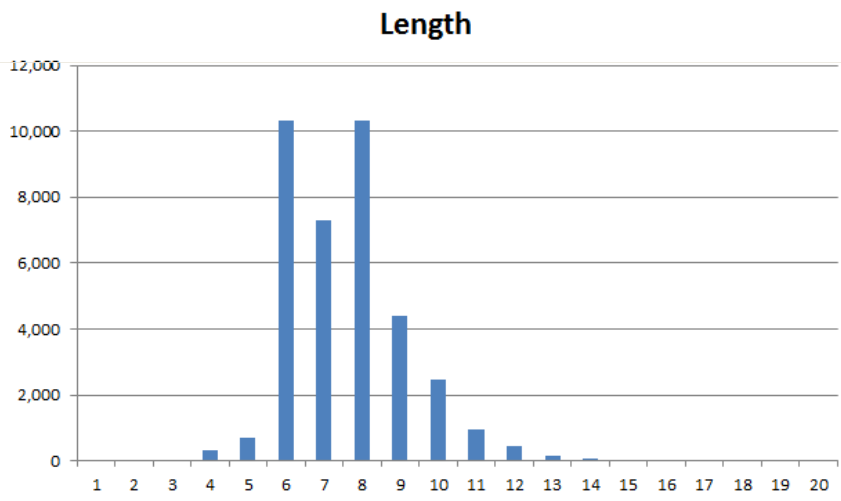
關於被竊取的帳號與密碼分析

- 微軟的 Tory Hunt把駭客組織釋出的百萬筆資料中的3萬7千多筆資料拿出來，並針對以下特徵進行分析：

- 密碼長度
- 字元類型的變化
- 隨機性
- 獨特性

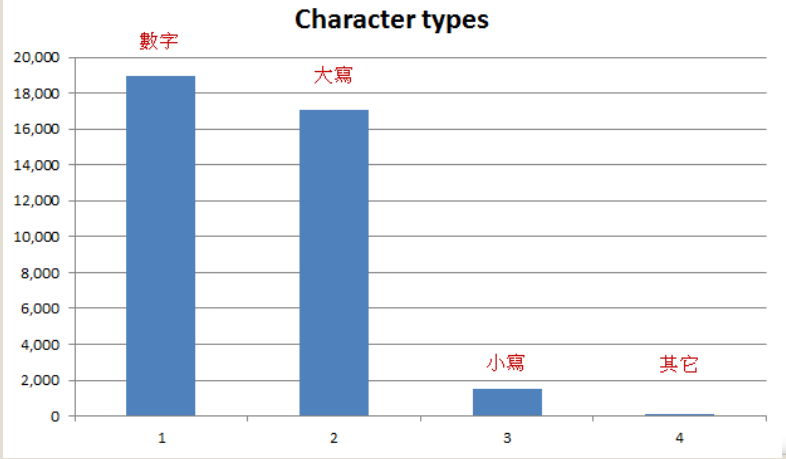
關於被竊取的帳號與密碼分析：密碼長度

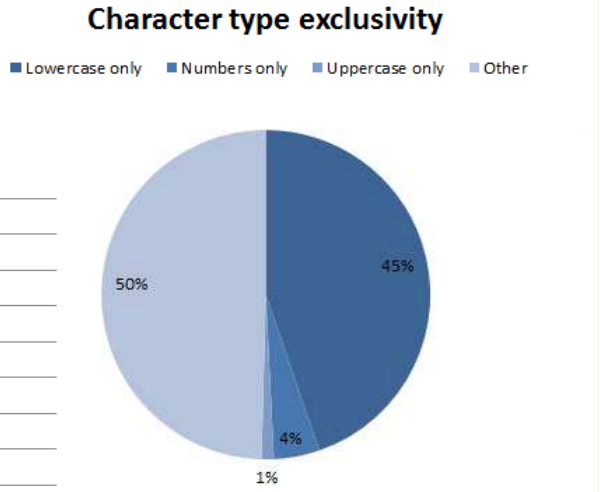
- 93%的密碼長度介於6 ~ 10位數之間，50%以上的密碼少於8位數，7位數密碼的使用者比6位數以及8位數的使用者少上一些。



關於被竊取的帳號與密碼分析：字元類型

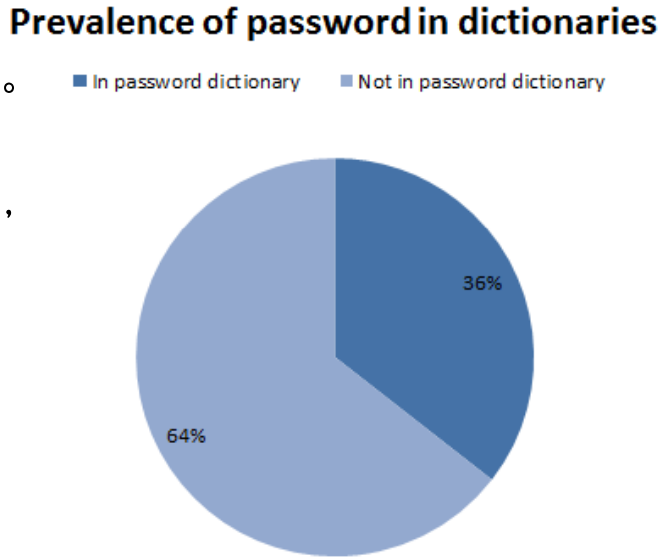
- 只有1%不到的人會使用非英文字母以及數字的字元（像是 # $ %之類的）。





關於被竊取的帳號與密碼分析：隨機性

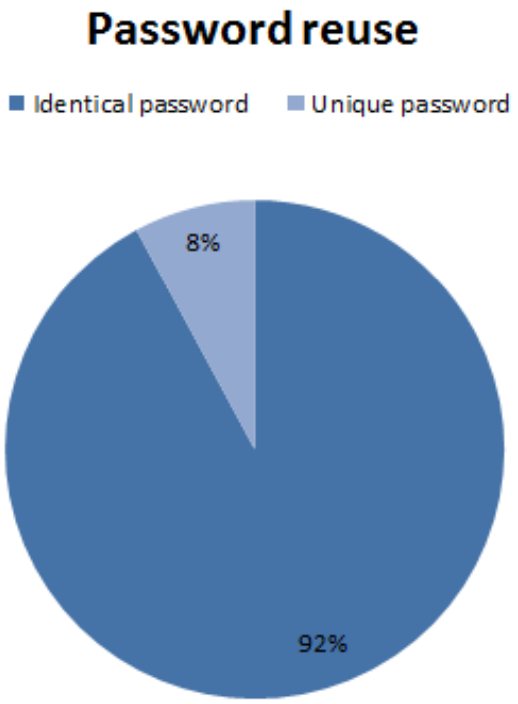
- 作者使用密碼字典檔，。**結果是36%的帳戶密碼包含在這份字典檔中**。



- 這不代表這些密碼太短，而是有些太容易被追蹤出來軌跡的密碼已經被放入這份字典檔中，像是「1qazZAQ!」（看鍵盤上的排列）這類型的密碼，通常都是不合格的。

關於被竊取的帳號與密碼分析：獨特性

- 作者在Sony不同的資料庫，找出相同的Email，並試著比對是否這些Email在不同的網站時，會採用不同的密碼，答是是 **92%的人都是用相同的密碼。**
- 如果有一個人的Google帳號被盜了，那麼也許Facebook、Yahoo帳號被盜的機率也大幅度提升。



密碼設定與保護

- 密碼強度：
- 指一個密碼被非授權的使用者或電腦破譯的難度。密碼強度通常用「弱」或「強」來形容。

- 維基百科對於密碼強度的說明：
- http://zh.wikipedia.org/wiki/密碼強度

竊取密碼的4大手段：防護措施：密碼強度測試

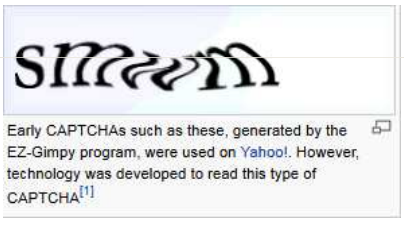
- Password Recovery Speeds
- http://www.lockdown.co.uk/?pg=combi&s=articles

- The password Meter
- http://www.passwordmeter.com/

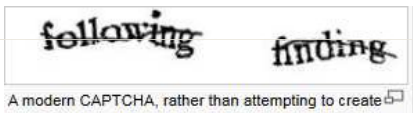
- Microsoft
- http://www.microsoft.com/taiwan/athome/security/privacy/password_checker.mspx

圖形密碼驗證

- 為了防止 Cracker 猜測密碼、大量惡意註冊帳號以及匿名的垃圾留言...等等，圖形密碼驗證 (CAPTCHA) 已經是常見的技術之一。



Early CAPTCHAs such as these, generated by the EZ-Gimpy program, were used on Yahoo!. However, technology was developed to read this type of CAPTCHA[1]



A modern CAPTCHA, rather than attempting to create a distorted background and high levels of warping on the text, might focus on making segmentation difficult by adding an angled line

Another way to make segmentation difficult is to crowd symbols together, as in Yahoo's current CAPTCHA format.

- http://en.wikipedia.org/wiki/Captcha

圖形密碼驗證

- 一般常見的驗證是都是背景圖加英文文字，由於在技術上很容易被破解，因此只好儘量把字型變形扭曲到人類難以辨識的地步，再加上用字型同色的線條來干擾畫面，簡直匪夷所思。
- 還沒防到駭客，連正常使用者都不想使用。
- 這到底是不是在　整人　？

圖形密碼驗證

- 在技術上　圖形密碼驗證(CAPTCHA) 雖然有其破解的方法，實務上於”註冊”、”驗證身份” 時又不能不設計。
- 建議：

竊取密碼的4大手段：顯示密碼passview

- 防範措施：
- 清除”所有”暫存資料檔案。
  - Clipboard Cache
  - Flash Player History
  - Google Chrome Traces
  - Internet Explorer Traces
  - Java Cache Logs and Temp Directory
  - Mozilla Firefox Traces
  - Opera Traces
  - Registry MRU Lists
  - Thumbs.db files
  - Windows and Internet Traces
  - Windows Log Files
  - Windows Temp Directories
  - index.DAT Files
  - Locked Files
  - IconTray Support
  - user-friendly GUI

竊取密碼的4大手段：防護措施：清除軟體

- 軟體名稱：Square Privacy Cleaner

- 下載網頁：
- http://www.novirusthanks.org/product/square-privacy-cleaner/

- 軟體說明：把常見的電腦操作痕跡、隱私資料分為「Windows General」、「Web Browsers」、「Temp Folders」、「Applications」與「Junk Files」等5個分類，我們可以依照實際需求勾選你要清除的項目。

- 註：使用方法很簡單，就是勾選你要清除的項目後再按一下「Delete Traces」按鈕即可搞定。

- 參考網址： http://briian.com/?p=7291

竊取密碼的4大手段：防護措施：清除軟體

- 軟體名稱：Ccleaner
- 下載網頁：
- http://www.piriform.com/ccleaner
- 軟體說明：網路上頗受好評的系統維護軟體，不但可以幫我們清除IE、Firefox等瀏覽器的瀏覽紀錄，還可清除一些暫時用不到的暫存檔、操作紀錄、登錄檔垃圾或一些很難用的Toolbar、垃圾軟體等。
- 註：這種類型的清除程式，主要就是清除系統的暫存資料，但在下列情狀中"不適宜使用"。例：Windows Update重大更新前後、安裝大型軟體、會使用暫存資料的軟體(沙盒)、磁碟重整程式。
- 參考網址： http://briian.com/?p=3167

竊取密碼的4大手段：側錄sniffer密碼

- 防範措施：
- 加密保護確保資料不被截取或解碼。
- 大略上可分為：
- 檔案加密
- 傳輸加密
  - SSL (https)
  - 聊天加密程式

竊取密碼的4大手段：防護措施：檔案加密

- 軟體名稱：AxCrypt
- 下載網頁：
- http://www.axantum.com/Default.html
- 軟體說明： AxCrypt 是一款開放原始碼且免費的檔案加解密工具，它能夠與檔案總管進行高度的整合，讓使用者可以直接透過滑鼠右鍵來對檔案進行加密的動作。而被加密過的檔案都將帶上特有的副檔名，因此當你要開啟這些檔案的時候，AxCrypt 就會自動詢問你解密所需的密碼以確保檔案的安全性。
- 註：英文介面，且千萬不要忘了自己設的密碼。
- 參考網址： http://jackbin.blogspot.com/2007/09/axcrypt.html

竊取密碼的4大手段：防護措施：檔案加密

- 軟體名稱：Encrypt Files
- 下載網頁：
- http://www.encryptfiles.net/
- 軟體說明：是一款免費的檔案加密軟體，提供多種加密的演算法來保護你的重要檔案。在操作方面，Encrypt Files須透過工具本身的應用程式介面，對指定的檔案及資料夾加密，同時還能一併加入隱藏屬性，使機密資料隱藏得更好。
- 註：英文介面，且功能比較多。一樣千萬不要忘了自己設的密碼。
- 參考網址： http://www.techbang.com.tw/posts/5078--drj-free-encryption-software

SSL / https

- SSL：
- SSL(Secure Sockets Layer)採用公開金鑰技術，保證兩個應用間通信的**保密性**和**可靠性**，使客戶與伺服器應用之間的通信不被攻擊者竊聽。

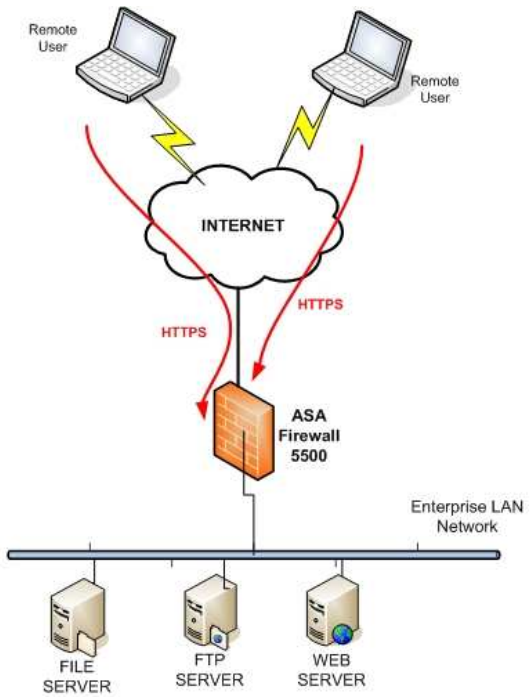
- HTTPS (Hypertext Transfer Protocol Secure)是http和SSL/TLS的組合，用以提供加密通訊及對網路伺服器身份的鑑定。

- 維基百科對於Https的說明：
- http://zh.wikipedia.org/wiki/Https

SSL / https

- 換句話說：
- https只保障瀏覽器與網站之間的利用SSL所產生的網路傳輸安全；

- 也就是說，如果資料(帳號/密碼)在傳輸前或傳輸後被竊取，那是端點的安全控管與資料傳輸一點都無關。

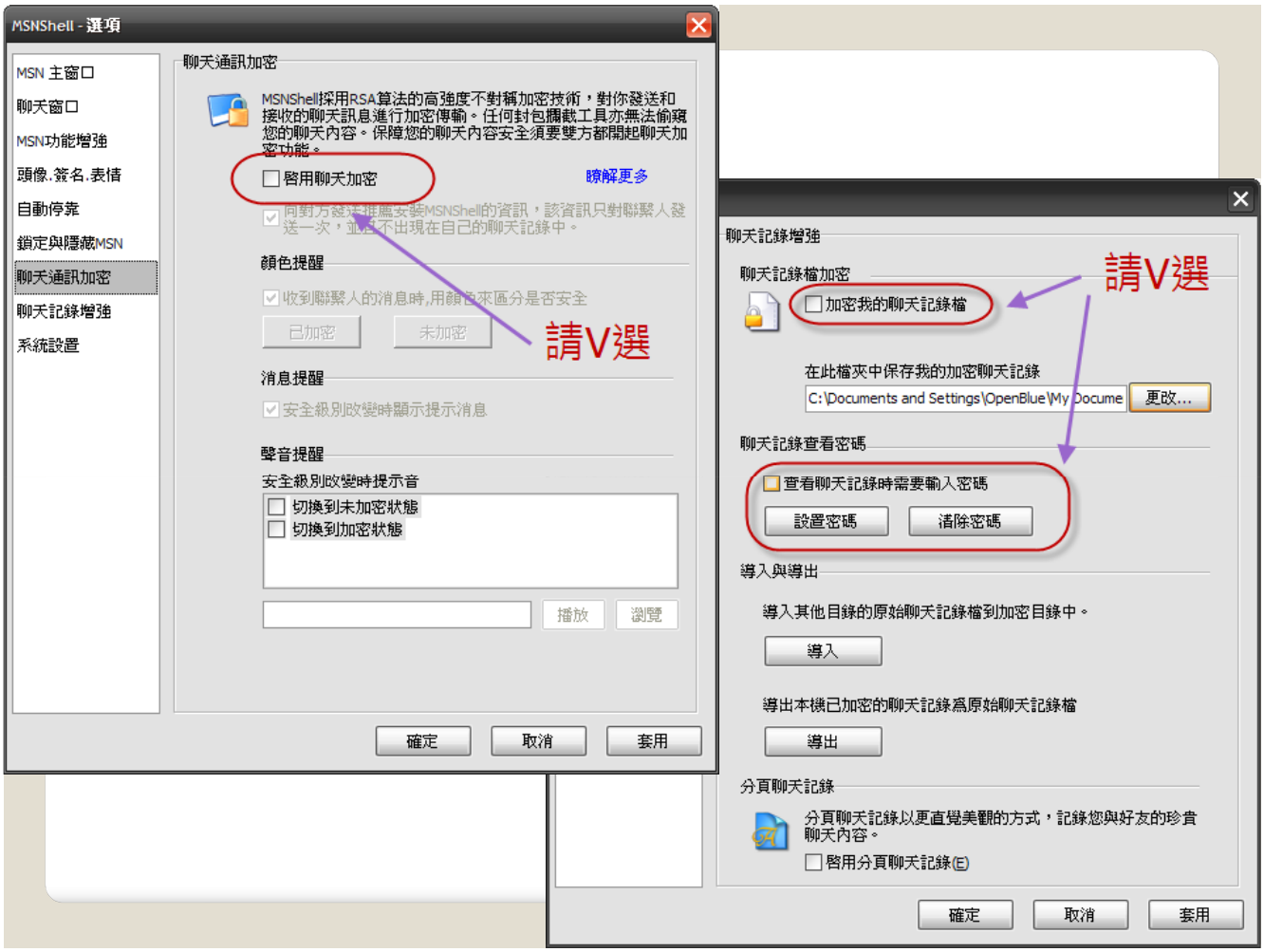


竊取密碼的4大手段：防護措施：傳輸加密

- 軟體名稱：SimpLite for MSN / SimpLite for Yahoo!
- 下載網頁：
- http://www.secway.fr/us/products/
- 軟體說明：透過最高2048位元的RSA keys與128 bits AES及Twofish加密演算法來幫我們傳送出去的訊息進行重新編碼、偽裝保護，可以躲過監控軟體的側錄與追蹤，讓雙方對話更保密、更安全。
- 註：英文介面，需要對話的雙方都有安裝才有效。
- 參考網址： http://briian.com/?p=7343

竊取密碼的4大手段：防護措施：傳輸加密

- 軟體名稱：MSN Shell
- 下載網頁：
- http://my.msnshell.com/
- 軟體說明：透過最高加密演算法來幫我們傳送出去的訊息進行重新編碼、偽裝保護，可以躲過監控軟體的側錄與追蹤，讓雙方對話更保密、更安全。
- 註：需要對話的雙方都有安裝才有效。
- 參考網址： http://briian.com/?p=299



竊取密碼的4大手段：木馬竊取

- 防範措施：
- 利用木馬程式的鍵盤側錄來竊取密碼是目前密碼外洩的最大宗管道，因其變化多，再加上網路詐騙、病毒感染盛行，使其得手成功率高。唯有勤加經常變更密碼與掃毒才能有效防範。

- 螢幕小鍵盤
- 動態鍵盤
- 動態密碼(密碼安全鎖)
- 修補漏洞

竊取密碼的4大手段：防護措施：螢幕小鍵盤

- 當您使用『螢幕小鍵盤』輸入密碼時，一般鍵盤側錄軟體或惡意程式無法記錄、監控您點擊的按鍵，在不安全公共場所操作電腦輸入密碼，透過滑鼠點擊『螢幕小鍵盤』的方式輸入密碼，可以有效的避免密碼被側錄與盜用。(需搭配https加密傳輸)

- Windows作業系統內建的『螢幕小鍵盤』

竊取密碼的4大手段：防護措施：動態鍵盤

- 更進一步採用『動態鍵盤』輸入密碼，可於登入WebATM或需要輸入密碼時，可由顧客自己選擇是否要開啟動態鍵盤，此功能可有效防止鍵盤側錄程式來記錄固定的滑鼠點選的鍵盤位置。

竊取密碼的4大手段：防護措施：動態密碼(密碼安全鎖)

- 有些銀行則搭配了硬體裝置，採用動態密碼(One Time Password)進行認證。由於密碼每次都不同(一般多為30或60秒變動一次)，這種方法擁有更佳的安全性，而使用者也不再需要記憶密碼。只不過因成本較高，目前僅有少數銀行或線上遊戲業者採用。

竊取密碼的4大手段：防護措施：修補漏洞

- 漏洞可分為：
- 作業系統的漏洞：→系統會自動更新
- 應用程式的漏洞：→需要使用者自行操作
  - 文書處理、Office軟體
  - 圖片、影音撥放程式
  - 雜7雜8亂裝的軟體→手機程式
  - 電腦自動裝的莫名其妙的軟體→flash、adobe、java
- 開發程式的漏洞：→需要開發人員改版

竊取密碼的4大手段：防護措施：修補漏洞

- Adobe Reader / Flash Player 更新 。
- 官方下載更新：
- http://get.adobe.com/tw/reader/
- http://get.adobe.com/flashplayer/
- 更新：
- 在Adobe Reader點選→說明→現在檢查更新

軟體列表：

密碼竊取：

- 重設登入密碼：
  - ERD Commander
  - Offline NT Password & Registry Editor
- 挖出電腦密碼：
  - Windows Password Recovery Tools 工具組
  - 星號密碼顯示器
- 破解文件密碼：
  - ElcomSoft Password Recovery Tools 工具組
- 側錄網路封包密碼：
  - Network Password Recovery
  - SniffPass
  - Remote Desktop PassView
  - Cain & Abel (該隱與亞伯)
  - EffeTech Network Monitoring Software 工具組
  - MSN Sniffer、HTTP Sniffer
- 破解無線網路密碼：
  - WirelessKeyView
  - Elcomsoft Wireless Security Auditor
  - NetStumbler, Airopeek, WEPCrack, AirDump

防竊對策：

- 防護軟體：
  - Square Privacy Cleaner
  - Ccleaner
  - AxCrypt
  - Encrypt Files
  - SimpLite for MSN / SimpLite for Yahoo!
  - MSN Shell

結論：

- 何謂雲端運算
- 密碼竊取
- 單機電腦
  - 單機電腦常見的錯誤方式？
  - 重設登入密碼
  - 挖出電腦密碼
  - 破解文件密碼
- 網路上的芳鄰
  - 網路上的芳鄰常見的錯誤方式？
  - 側錄網路封包密碼
  - 破解無線網路密碼
  - 是否跨Switch監聽？
  - 預設帳號/密碼的問題
- 網際網路
  - 網際網路常見的錯誤方式？
  - 上網密碼
  - 外洩管道
  - 側錄、搜尋、中毒、社交網站
- 防竊對策
  - 密碼設定與保護
  - 密碼學
  - 竊取密碼的4大手段：
    - 暴力破解密碼
    - 顯示密碼
    - 側錄sniffer密碼
    - 木馬竊取

- 講師：　呂守箴
- E-Mail：shooujen@gmail.com

- 部落格：
- 網路攻防戰：http://anti-hacker.blogspot.com

- Plurk噗浪：http://www.plurk.com/openblue
- FaceBook：http://www.facebook.com/openblue
- 粉絲團：http://www.facebook.com/NetWarGame

- 網路直播頻道：http://zh-tw.justin.tv/openblueTV