由電腦鑑識看帳號/密碼的竊取

2009/July

講師:鑒真數位 黃敬博

po@iforensics.com.tw

(EnCE/CCE/CIFI/CHFI/CEH/CISSP)

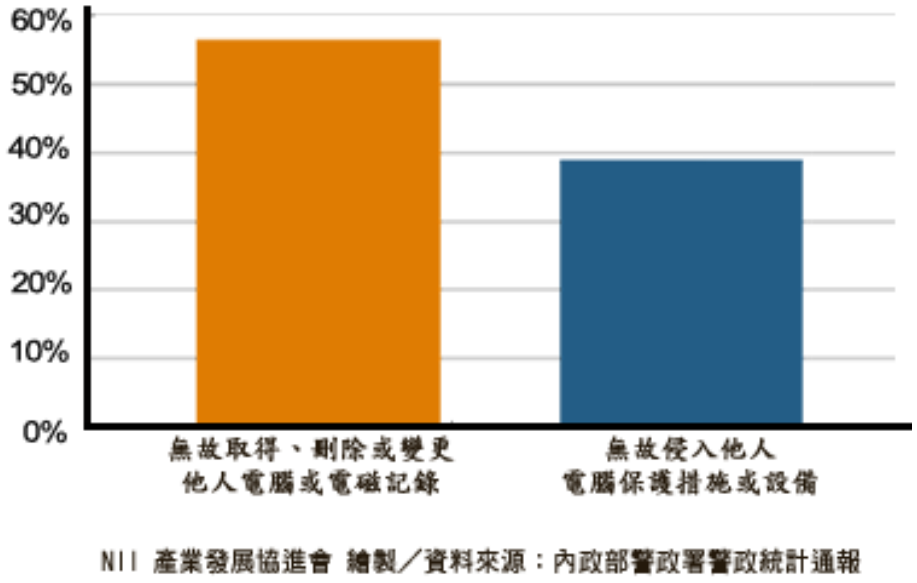
簡報大綱

- **帳號密碼遭竊的嚴重性**
- 不可知的殘留
- 帳號/密碼存在的位置及方式
- 破密的邏輯
- 常用的竊取手法
- 問題與討論

國內趨勢

- 根據內政部警政署的統計資料顯示

  去年(97年)妨害電腦使用案，犯罪方式第一名爲無故取得、刪除或變更他人電腦或電磁紀錄(56.47%)



NII 產業發展協進會 繪製／資料來源：內政部警政署警政統計通報

案例說明

有組織的犯罪結構

- 中國駭客黑色產業鏈:2.38億年產值帶來76億損失
  - 僵屍電腦租借
  - 帳號/密碼 (其中每天有超過上萬人次填寫申訴資料，反映QQ密碼被盜)

簡報大綱

- 帳號密碼遭竊的嚴重性
- 不可知的殘留
- 帳號/密碼存在的位置及方式
- 竊取的手法
- 破密的邏輯
- 問題與討論

不可知的殘留

- 根據加州柏克萊大學的研究，目前公司中有超過93%的資訊產出是以數位格式分散貯存在各個系統中，同時相同的研究也指出在所有的資訊犯罪、侵權案例中，有超過85%的案例均會留下數位遺趾。 (Foot print)
  è 示範

硬碟Unallocate區的殘留

- File Slack
- Unallocated cluster
- Hardisk Unallocated area

虛擬記憶體的殘留

- Pagefile.sys

  爲Windows平台中的虛擬記憶體,程式執行中的資訊很多會殘留在此部份,且可能以明文的方式顯示

  - 帳號/密碼
  - Instant Message 聊天的內容

Windows 休眠

- Hibernate.sys 及 Hiberfil.sys

  爲Windows平台中休眠時，將記憶體中的資訊貯存檔案名稱，可於停止休眠時迅速回復系統原始運行的狀態

Memory Dump

- 作業系統中所有正在執行的程式及保留的輸入資料存在許多有用的資訊

- 使用記憶體傾印工具可將記憶體資料完整保留爲一個映像檔

記憶體殘留的密碼分析

- Strings 將ASCI字串取出
  - 採用支援Uni-code的Strings
  - 輸出檔案輸入編輯器搜尋(Ex: UltraEdit)

- 使用商業軟體進行檢視及搜尋
  - Encase / FTK / X-Ways Forensics

簡報大綱

- 帳號密碼遭竊的嚴重性
- 不可知的殘留
- 帳號/密碼存在的位置及方式
- 破密的邏輯
- 常用的竊取手法
- 問題與討論

帳號/密碼存在的形式

- 貯存在檔案中
- 貯存在Registry中
- 貯存在Cookie中
- 貯存在Data Base中
- 貯存在Token Card/iKey

MSN的帳號/密碼

- MSN version 8.x/9.x 的密碼:

  The passwords are stored in the Credentials file, with entry name begins with "WindowsLive:name="

- MSN version 7.x/6.x 的密碼:

  則貯存在Registry 機碼中

  V7.0: HKEY_CURRENT_USER\Software\Microsoft\IdentityCRL\Creds\[Account Name]

  V6.0: HKEY_CURRENT_USER\Software\Microsoft\MSNMessenger or Microsoft\MessengerService

Yahoo messenger 及Google talk的帳號/密碼

- Yahoo messenger 最新版爲 Ver 9.x:

  歷來8/7/6的版本密碼主要均貯存於機碼中

  HKEY_CURRENT_USER\Software\Yahoo\Pager

- Google talk 最新版爲 Ver 1.0.x:

  密碼主要均貯存於機碼中

  HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts\[Account Name]

Outlook/Outlook express 帳號/密碼

Outlook

- Outlook 2002-2008 帳號密碼貯存在同一個 Registry Key中
- 但是若經由AD認證去取Exchange 伺服器的信件則帳號/密碼則存在於Credential file中

Outlook Express

- 密碼貯存Protected Storage
- Protected Storage information is saved in a special location in the Registry.

IE Auto-complete 的帳號/密碼

- 新版IE V7及V8 貯存密碼於兩個地方
- AutoComplete passwords are stored in the Registry under
  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2.
- HTTP Authentication passwords are stored in the Credentials file

WebMail 的帳號/密碼

- Hotmail
- Yahoo Mail
- Gmail

Web mail 的密碼主要還是存在於不同的 Registry Key中,但均經過加密處理的密文

使用工具進行帳號/密碼的揭露

- 示範: 整合揭密的軟體工具(LiveDetector)

簡報大綱

- 帳號密碼遭竊的嚴重性
- 不可知的殘留
- 帳號/密碼存在的位置及方式
- **破密的邏輯**
- 常用的竊取手法
- 問題與討論

瞭解加密的強度並預估所需時間

- 瞭解你所面對加密強度及應用程式爲何?
  - AES (Truecrypt)
  - PGP
  - Skype
  - Wipe /Completely deleted tool

Brute force – Time (How long ?)

- 當破密的強度超過一定程度後
  - CPU 及 電腦數已不具任何意義 !

  - 一台Core2的PC當要破一個PGP的加密檔案
    使用暴力破解約需1千萬年時
    - 等於1千萬台PC要同時跑一年來破密
    - ....

密碼破解的邏輯

- 先瞭解你的目標對象
  - PGP/SSL/AES/WEP/3DES…
- 柿子挑軟的吃 － 先從簡單著手 ？
  - Social Engineering
  - 使用習慣
  - 先破 MSN/DOC/RAR 密碼
  - 刪除的檔案
  - 搜尋password/account/密碼…等相關字
  - 非不得已,不用暴力破解

刪除的檔案找線索

- 先救回已刪除檔案,方式主要有兩種:

  1. 修改檔案系統的索引區(FAT/FDT/MFT/InodeTable),將標示已刪除的Tag及相關資料回復為未刪除的型態

  2. 在Unallocate資料區搜尋符合檔頭格式及檔尾格式的資料，擷取出來另存為新的檔案

- 直接在已刪除檔案的區域找線索

加密的文件檔案

- 不同的加密文件有不同的破密困難度:

1. 先從Office 文件下手(必可破的文件)
2. 再從PDF文件下手
3. RAR/ZIP的文件
4. 付費服務(國外有許多的破密服務/破了再付費)

密碼破解 – 實務操作

- 範例: 使用破解的方式

- 明文破解

密碼破解 – 字典檔攻擊

- 大部份的破密軟體均大同小異
  - 主要的區別在於字典檔的完整性及組合方
  - 字典檔買得到嗎？
  - 如果是有經驗的駭客,密碼的選取...(Non-english)
  - 如何製作字典檔

HardDisk indexing

- 非常有效的字典檔製作方式

- 不只整顆硬碟也特別適用於 記憶體資料
  - Memory dump 檔案
  - pagefile.sys 檔案
  - hiberfil.sys 及hibernate.sys

RainBow Table – 最快的密碼破解

- 什麼是RainBow Table
  - 彩虹表 (用空間換取時間?? …)

- 速度多快?
  - Windows 密碼安全嗎?
  - Office/PDF 文件加密安全嗎 ?
  - Zip/RAR 文件加密安全嗎 ?
  - 什麼才安全 ?

Linux 或 Window 密碼遺忘

- 使用更改而非破解,此為 Non-forensics 作法
  - Windows Administrator密碼忘了如何?
  - Linux root密碼忘了如何?
  - Vmware 內的作業系統該如何?

使用chntpw 製作開機光碟後可更改windows的密碼,linux只要mount檔案系統後更改/etc/shadow即可

簡報大綱

- 帳號密碼遭竊的嚴重性
- 不可知的殘留
- 帳號/密碼存在的位置及方式
- 破密的邏輯
- 常用的竊取手法
- 問題與討論

鎖定目標-瞭解使用者的軟體環境

- 電子郵件 (Outlook/Outlook Express/Lotus Notes /其它...)
- 即時通訊軟體(MSN/Yahoo/Google Talk...)
- 文件保護的機制(PGP/Truecrypt/...)
- 防毒系統
- 其他應用...

硬體式 KeyLogger

Product selector

KeeLogger™ Flash USB

Version	4 MB	2 GB
Price	**€52.99** or $73.99	**€66.99** or $92.99
Black	Add to cart	Add to cart
White	Add to cart	Add to cart

KeeLogger™ Flash PS/2

Version	4 MB	2 GB
Price	**€28.99** or $39.99	**€47.99** or $65.99
Black	Add to cart	Add to cart
Gray	Add to cart	Add to cart
Purple	Add to cart	Add to cart

軟體式(最普遍) - 植入木馬

- Screen capture
- Keylog
- URL log
- Files open log
- Application open log

使用社交工程方式騙取

- E-mail 網路釣魚的手法
- 設立的登入網站,詐取帳號/密碼
  (一般人重複使用密碼的習慣)
- 3M/便利貼/圾垃中尋找.
- 台灣人最常接到的詐騙電話
- 其它...

Network Sniffer

- 哪些帳號/密碼 爲明文,最容易在網路中竊聽

  1.POP3 取信(Outlook/Outlook express/Windows Mail/Live Mail...)

  2.BBS (Telnet)

  3.FTP 傳檔

  4.Web (Basic authentication)

Wireless hacking

- Wep authentication (收集封包量夠多即可破解)

- Wireless Open Site
  - 咖啡店...
  - Wifly...
  - 其它

Network attack

- 若你的網路應用帳號/密碼 可以持續被猜而不鎖定
  - 則可用類似Hydra/Brutus 最後try出可用的帳號及密碼
- Web 認證的其它攻擊...

意見回饋與討論