防外洩更要抓內賊

登豐數位科技-台灣特約講師 黃建笙

Microsoft® Most Valuable Professional

CISSP® Certified Information Systems Security Professional

ISSMP® Management

活動議程

- 網路攻擊趨勢
- 資料安全防護
- 你不知道的Windows
- 如何找出內部攻擊來源

2016 Mandiant 網路攻擊趨勢報告

攻擊目標產業

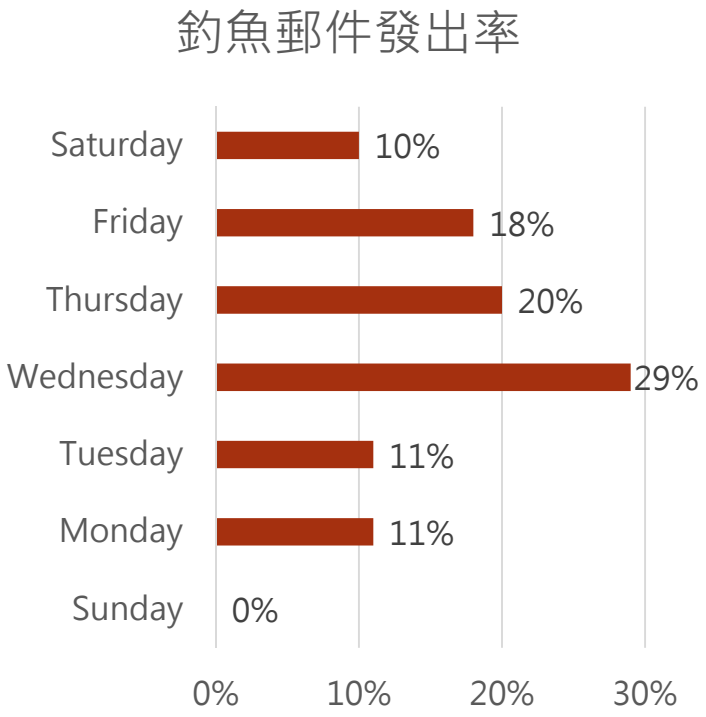
- 高科技產業成為主要目標(13%)
- 商務及專業服務與媒體及娛樂並列第二(11%)
- 財務服務及保險與零售業並列第三(10%)

2015年調查樣本平均攻陷潛伏期146天

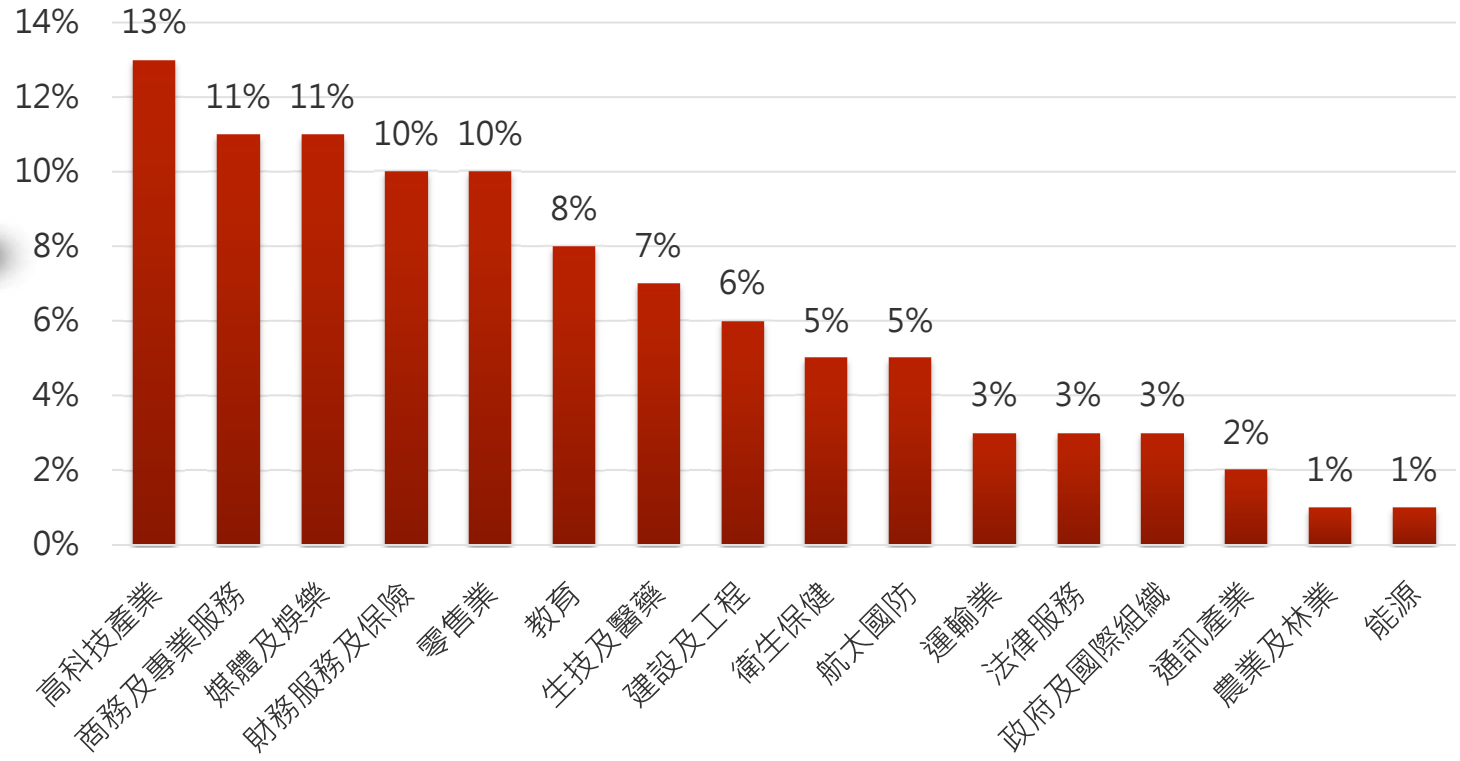
- 53%由外部人員通知被攻陷，潛伏期320天
- 47%由內部人員發現被攻陷，潛伏期56天

魚叉式釣魚的電子郵件僅有10%在假日發出

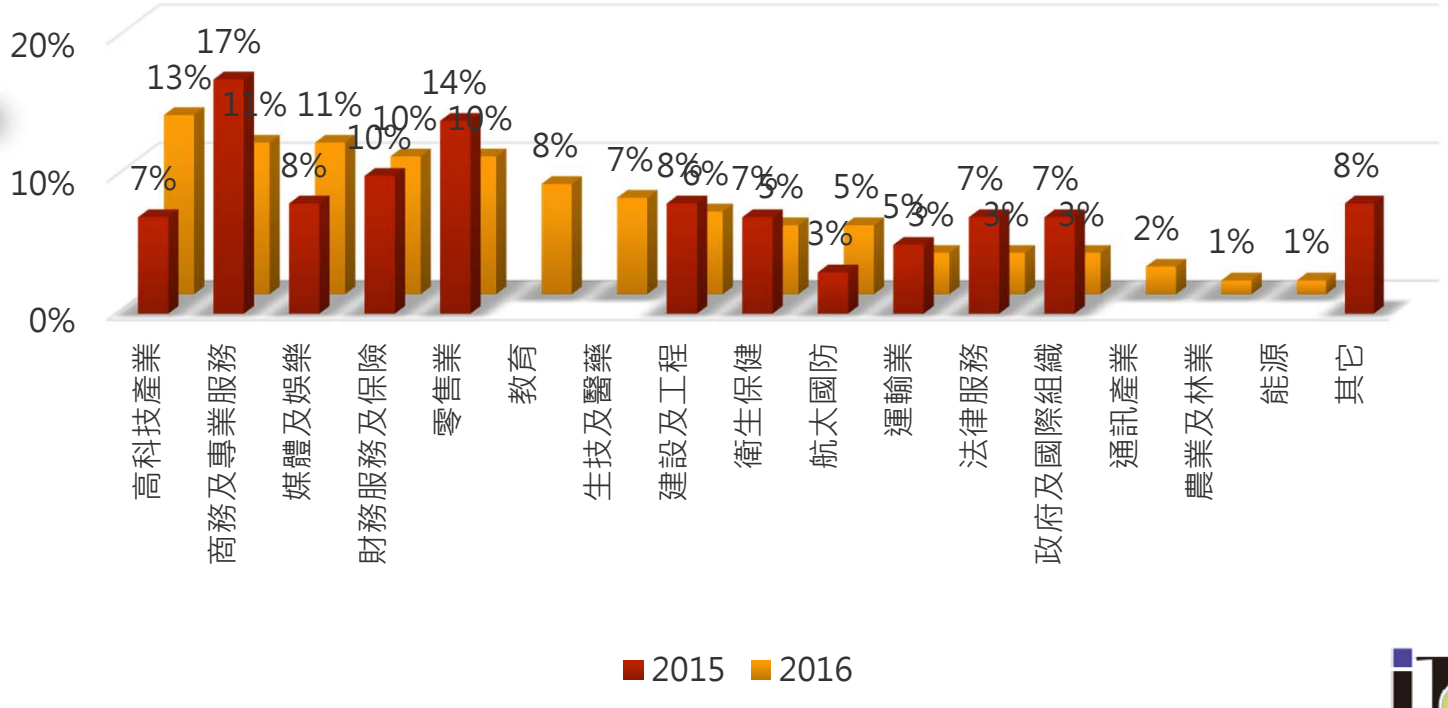
- 星期三發出為29%
- 星期日發出為0%



2016 Mandiant 網路攻擊趨勢報告



2015~2016 Mandiant 網路攻擊趨勢報告



決戰境外

- 想把戰線拉到境外，你必須先知道你有那些戰力!
- 管理觸及愈廣、愈深，才有辦法決戰境外!
- 安全防護能力：

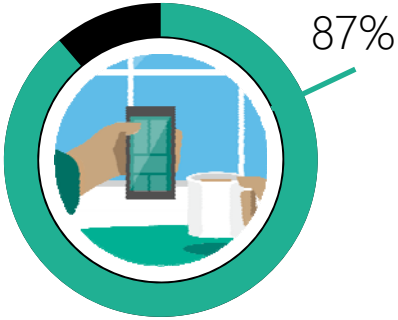
  導引(Directive)　預防(Preventative)　矯正(Corrective)

  嚇阻(Deterrent)　偵測(Detective)　復原(Recovery)

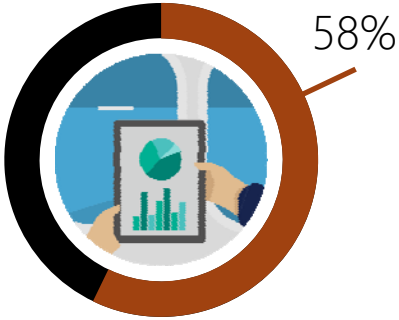
  補償(Compensating)

- 資安事件不是單一事故，而是一連串的錯誤!

實現資料保護



87% 的高階管理主管承認，會定期的將工作的文件上傳到私人的電子郵件信箱或雲端儲存帳戶上。



58%的人曾不小心將敏感的資訊傳遞給錯的人。

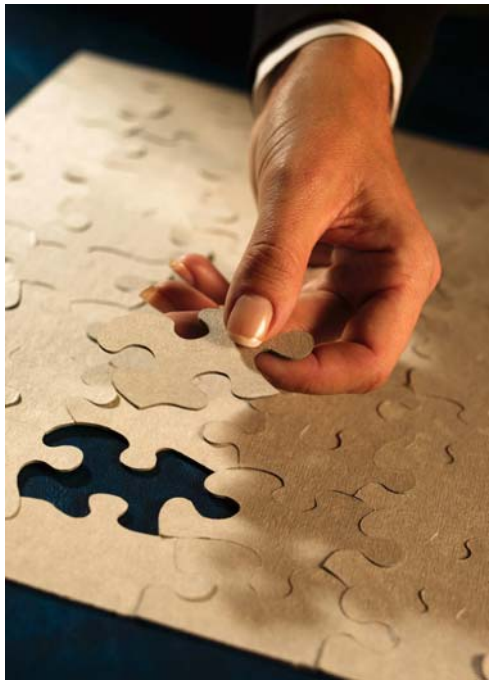
過度的聚焦於個人裝置造成資訊洩露的問題，但卻忽略了企業所擁有的裝置上也有相同的風險!

DLP(Data Loss Prevention)

- 極重要的資料遺失，對企業造成衝擊。
  - 對手會不會拿到?
  - 是否有無法公開的密秘?
  - 可能讓機關蒙羞?

- DLP的宗旨是??

我得不到的，你也別想要!!



DRM(Digital rights management)

資料在內外部開啟的方式是否相同?

能否管理到每個員工的行為?

是否能避免未經授權的洩露?

DRM的宗旨是??

只有主人才開得了!!

DLP V.S. DRM

兩者是相輔相成。

DLP並不等於DRM

對的鑰匙才能打開秘寶!!

DRM管理使用者的行為。

DLP避免資訊外洩時的衝擊。

天底下沒有解不開的鎖，鎖不是保護裝置

而是延遲開啟的時間!!

帳號密碼 + 驗證碼

帳號密碼 + 問題

帳號密碼 + OTP

帳號密碼+簡訊


facebook
Email or Phone
Password
Log In
Keep me logged in
Forgot your password?
14:14
8869115232665
訊息 (2)
8869115232665: You just activated Code Generator. If you change your mind or someone else activated Code Generator, you can remove this at [redacted]
2012 年 6 月 13 日, 週三, 16:07
8869115232665: 請使用這組安全碼 380558 確認你仍然握有你的手機，以啓用登入許可功能。
14:12
Select Sex:
Month:
Day:
Year:
Why do I need to provide my birthday?
Sign Up
中文(台灣)

帳號密碼 + 識別圖像

帳號密碼+SmartCard

2步驟證

應用程式專用密碼

某些不在瀏覽器中運作的應用程式還無法使用兩步驟驗證功能，因此無法要求提供驗證碼，例如：

- 較舊的 Android 智慧型手機
- Chrome 同步功能
- 郵件用戶端，例如 Microsoft Outlook
- 即時通訊用戶端，例如 Google Talk、AIM 等

如要使用這些應用程式，您需要先**產生應用程式專用密碼**。接下來，在應用程式的密碼欄位**輸入**應用程式專用密碼，而不是您慣用的密碼。您可以為每個需要應用程式專用密碼的應用程式產生新密碼。 瞭解詳情

觀看應用程式專用密碼的影片

步驟 2 之 1：產生新的應用程式專用密碼

輸入可以協助您記住應用程式用途的名稱：

名稱： 產生密碼

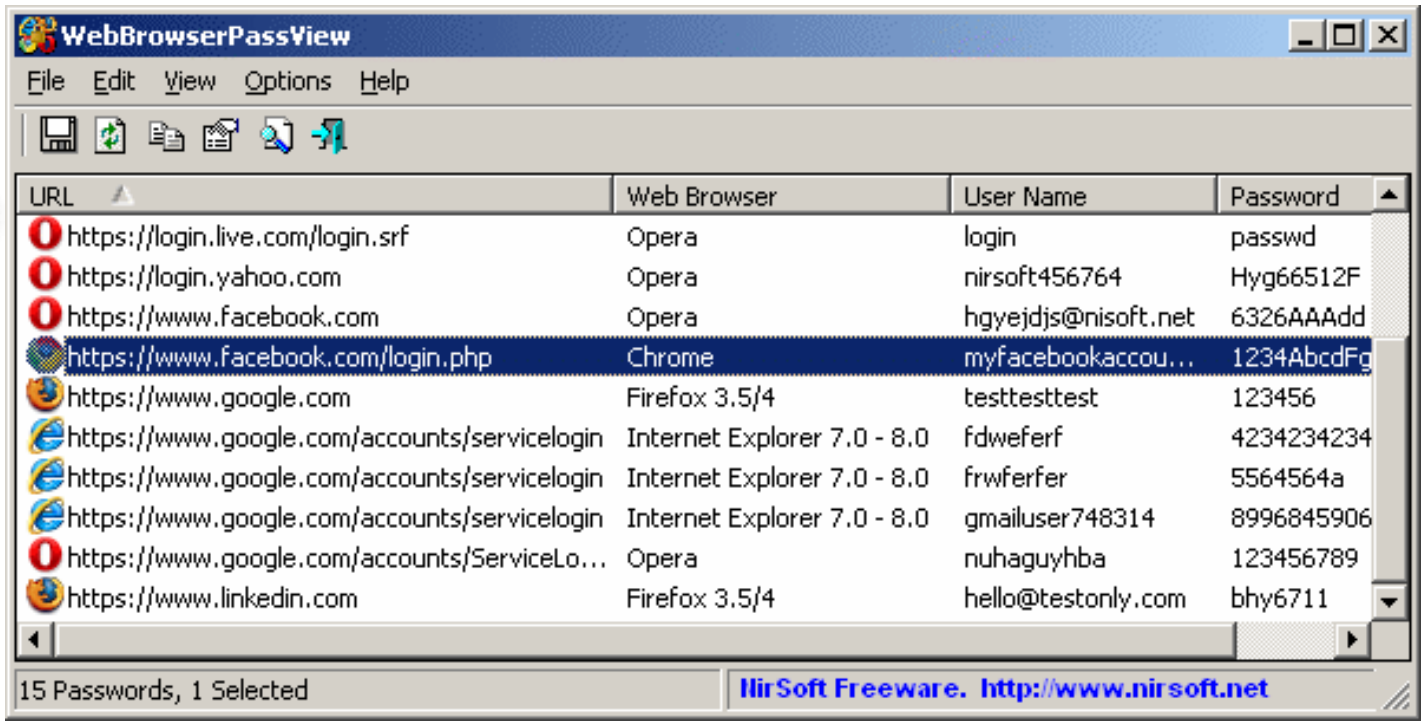
例如：「阿寶的 Android」、「我 iPhone 上的 Gmail」、「GoogleTalk」、「Outlook - 家用電腦」、「Thunderbird」

您的應用程式專用密碼	建立日期	上次使用時間	
HTC Desire HD	2012/8/10	2012/11/4	[撤銷]
Transformer	2012/8/10	2012/8/10	[撤銷]
HTC Wildfire	2012/8/10	2012/11/5	[撤銷]
HTC Incredible S	2012/8/10	2012/8/10	[撤銷]
Transformer2	2012/8/13	2012/11/7	[撤銷]
HTC Desire HD2	2012/8/18	2012/11/7	[撤銷]
Windows8	2012/10/17	2012/11/8	[撤銷]
GoogleTalker	2012/10/17	2012/11/7	[撤銷]
Windows8-Mail	2012/10/17	2012/10/28	[撤銷]
ViVoTabRT	2012/10/30	2012/11/8	[撤銷]

2步驗證真的安全?

- 不管是Microsoft或是Google，都有1.84467E+19 也就是16^16 (18,446,744,073,709,600,000)種組合
- 每增加一個裝置，就多一隻鴿子!
- Mail為基礎的服務，可多次猜密碼!

到底方便到誰



十五年來無解的資安問題

- 身份竊取分為:
  ①知道密碼(偷密碼、側錄密碼、keylog)
  ②不知道密碼(偷授權、側錄認證封包、重送攻擊)

- 針對NTLM v1而來的Pass-the-Hash; PtH attack
  - PtH是NTLM Hash的天生弱點
  - NTLM v1沒有做雜亂的程序(Part2 hash value=AAD3B435B51404EE)

- 針對Kerberos而來的Pass-the-Ticket; PtT attack
  - 當TGT向TGS要求Service ticket時沒有再做第二次驗證。

Mimikatz千面人攻擊工具

沒有非得要在AD環境，在AD環境只是方便了駭客。

Pass the Hash是NTLMv1的弱點。

- 拿的是你驗證過後的hash，在別台設備上再送一次
- 官方的解決方案是"請用NTLMv2"

Pass the ticket是Kerberos的弱點

- 拿的是你驗證過後的Ticket，在別台設備上再送一次
- 官方的解決方案是"請隔離敏感的主機"

由於接下來的畫面太過於血腥、暴力

若有IT部門主管身體不適

請自行就醫並隔離!!!

保密切結!

本人於今日課程中嚴守保密規定與國家相關法令對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播、應用於職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，並不造成第三方任何損害，講師已盡善意告知，並再三提醒，此後若有違者，為個人行為，不得陷害講師於不義，違者願負法律責任。

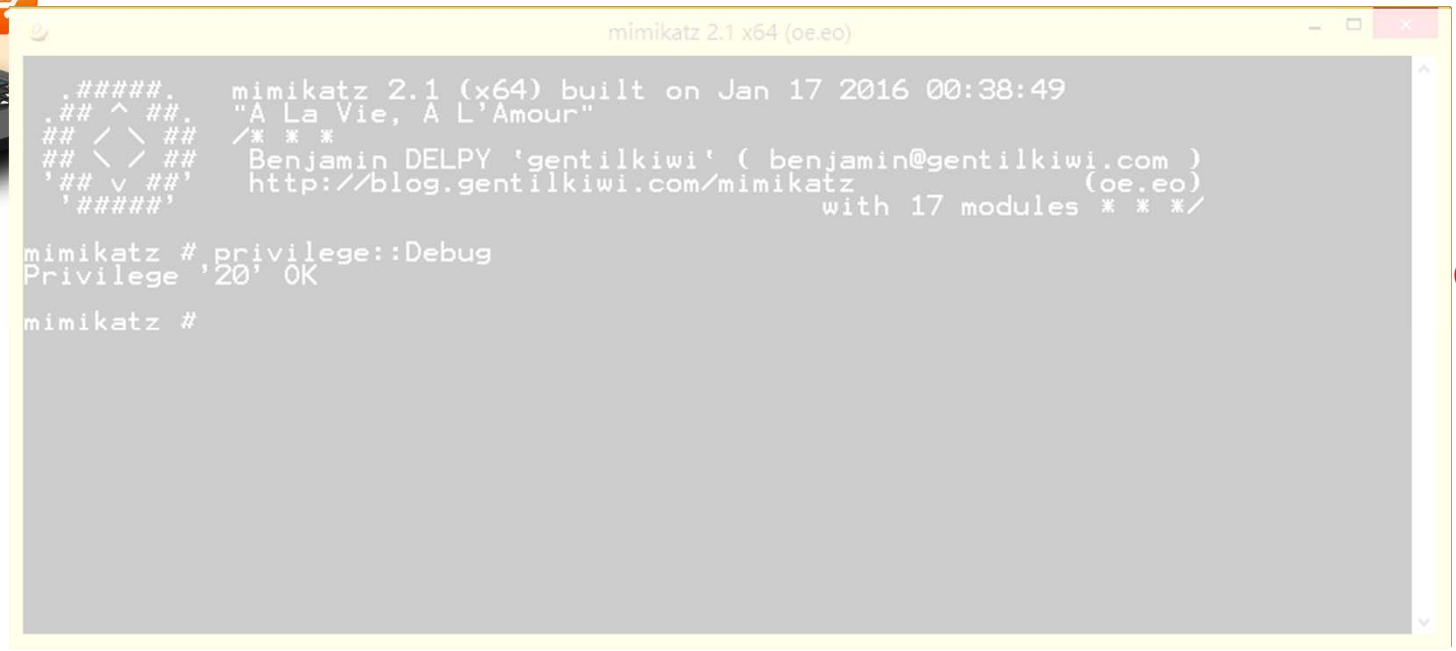
同意請示意!! 不同意請離席!!

情境說明

- 用戶端電腦均將主機使用者(Domain Users)設定為Administrators
- UAC是被關閉的!
- 所有的驗證機制僅仰賴著帳號及密碼
- 你擁有神兵利器級的工具!

模擬情境

主機存於有AD服務的環境



ege

Pass the Hash

- Hash是NTLM Hash，可以透過mimikatz內建的pth指令來達成：
  - Sekurlsa::msv
  - 找到相利用的帳號，再用下面的指令來送遞執行內容
  - "sekurlsa::pth /user:Administrator /domain:. /ntlm:'hash value' /run:"你想幹麻就幹麻"
- 近期來，我們看到非常多DC上都備有"Mimikatz"!!

如何找出內部攻擊來源

驗證、授權、稽核，3A架構把關

掌握驗證關卡，防堵權限提升

Target – 脆弱的身份系統被利用

"Target 駭客使用偷來的用戶名和密碼闖入網路，此用戶名和密碼專為公司維修其空調系統而創建。"

BRAIN KREBS（安全博主）

Target 信用卡被盜導致數百萬張信用卡出現在市場上

資料來源："目標攻擊中被盜的信用卡湧入地下市場，" KrebsOnSecurity.com，2013 年 12 月 20 日

洛克希德資訊洩露 – 前所未有的智慧財產權盜用

機密報告列出網路間諜洩露的美國武器系統設計

華盛頓郵報
2013 年 **5** 月 **27** 日

"現在，我們的防禦強大到足以應對威脅，很多攻擊者知道這一點，所以他們去追逐供應商。當然他們總是嘗試開發新的攻擊方式。"

linux安全不再 – 商用軟體的目標轉移

攻擊矛頭指向開放原始碼，Heartbleed與ShellShock可說是2014年兩大世紀安全漏洞，OpenSSL上的安全漏洞，駭客透過該漏洞攻擊竊取記憶體內容，ShellShock則是GNU作業系統殼層程式Bash Shell上的漏洞，駭客可藉由請求來執行惡意程式，進而掌控系統控制權。

隨著微軟Windows在安全上的改進與漏洞的逐漸減少

資料來源：“目標攻擊中被盜的信用卡湧入地下市場，” KrebsOnSecurity.com，2013 年 12 月 20 日

無法自已查詢的安全問題 – 劫持你的路由器

不安全的路由器駭客便能任意攔劫、檢測甚至修改任何裝置內送與外發的網路封包

"家用及商用路由器對駭客而言是個非常值得攻擊的目標，比起受感染的PC，遭劫持的路由器會更難以偵測察覺，絕大部分的路由器上沒有任何防毒或安全軟體
"

行動安全浮出枱面 –行動支付

Android平台上出現專門鎖定特定使用者Google Wallet帳號密碼的FakeID漏洞攻擊事件，被視安全無虞的iOS平台也開始出現安全威脅，蘋果用戶的WireLurker惡意程式。第一隻不需透過越獄，便可在進行USB連線同步化時感染iOS系統的惡意程式

行動支付安全勢將成為2015年最關鍵的行動安全議題

日漸普遍的APT與目標式攻擊–魚叉式釣魚郵件

APT與目標式攻擊(Targeted Attack)在新的一年裡將成為與一般網路犯罪一樣普遍的威脅。

這類攻擊仍以魚叉式釣魚郵件或水坑式攻擊做為起頭

2015年上半年遭到APT及目標式攻擊最多的地區是台灣(46%)，其次則為日本(20%)與美國(12%)。

APT演進過程

2000 – 2005年：暫時休息

– 在梅麗莎(Melissa)之後，巨集惡意軟體就變得沉靜起來。

2006年：巨集再次出現

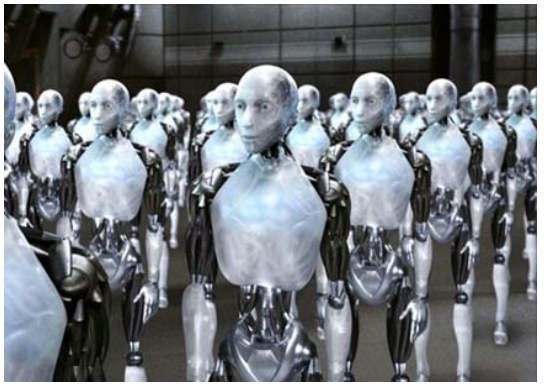
2014年：巨集惡意軟體最大化

2015年至今：巨集興起

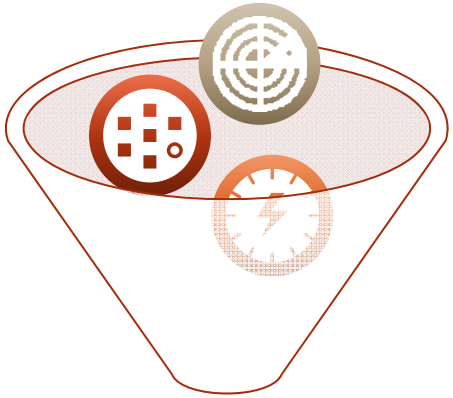
– 它們不僅被用來散播銀行惡意軟體，同時也被用在「進階持續性滲透攻擊」

有那些APT偵測解決方案

閘道硬體



終端安裝



Log分析

安全防護

- 實體層
  - 啟用TPM、SecureBoot開機前的啟動受到保護，
- 作業系統
  - Device Guard-杜絕了惡意程式越權執行的的行為
- 身份識別
  - Windows Hello-結合虹膜或指紋的辨識
  - Microsoft passport帳號登入結合雲端認證
  - Credential Guard保護內部帳號的認證安全。
- 資料
  - Azure RMS提供了Anywhere全面保護

多因子驗證

Knowledge (Something you know)

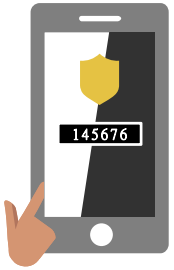
請輸入密碼：●●●●●●●●●

Ownership (Something you have)

Characteristics (Something you are)

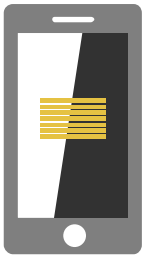
結合多因素驗證機制

登入應用程式



透過手機驗證

透過簡訊驗證



1.安全是要透過持續的更新知識。

2.正確的組態，才能真正的安全。

3.最小權限、僅知原則、職責切割。

4.解決根本原因才是真正的解決問題。

5.內部攻擊重點在於權限提升的把關！

- 淺談 (Pass the Hash) PtH 與 PtT (Pass the Ticket) 攻擊對企業的衝擊（下）
  - http://blogs.technet.com/b/technet_taiwan/archive/2016/03/29/pass-the-hash-pth-and-pass-the-ticket-ptt-01.aspx

- 淺談 (Pass the Hash) PtH 與 PtT (Pass the Ticket) 攻擊對企業的衝擊（上）
  - http://blogs.technet.com/b/technet_taiwan/archive/2016/03/29/pass-the-hash-pth-and-pass-the-ticket-ptt-02.aspx