勒索軟體與個人資安防護教育訓練

課程大綱

- 前言
- 勒索軟體的與起
- 散播的途徑
- 個人資安防護建議
- 問題與討論

前言

時事分享
Google宣佈Chrome將停止使用Flash

- 根據思科2015年年度安全報告，Java、PDF與Flash為駭客前三大攻擊途徑，並有資安研究人員建議使用者直接關閉Java與Fash功能
- Google及Firefox預計2016年底停止支援
- Facebook及資安業者呼籲停用flash

常見的資訊安全威脅

- 病毒
  - 是個不完整的程式，需要依附在執行檔中，藉由依附程式的執行而觸發
  - 執行後會造成電腦設備資料毀損、作業異常等惡意破壞行為。早期病毒不具備資訊網路通訊能力。
- 蠕蟲
  - 是個完整的程式，會透過網路、系統及應用程式進行自我執行、複製及散佈。
- 特洛伊木馬
  - 是個完整的程式，不會主動進行攻擊，主要目的為長期進駐目標設備，竊取資料或遠端操控目標設備

最終目的「植入後門程式

2017資安趨勢

- 勒索軟體的攻擊持續增加與擴大目標
  - 勒索軟體將會攻擊雲端
- 大規模的業務與作業中斷危機
  - 物聯網(IoT)DDoS攻擊
- 網路犯罪成為主流
- Apple漏洞倍增，零時差漏洞攻擊

資料來源：趨勢科技、Symantec、iSecurity

觀念與想法

資訊安全的強弱取決於您的觀念與想法

勒索軟體的興起

勒索軟體演進

1989
AIDS

2006
TROJ_CRYZIP

2012
Reveton

2013
CryptoLocker

2014~
TorrentLocker
Cryptowall
Chimera

2016~
KeRanger
WannaCry

案例分享
綁架勒贖-TorrentLocker

- TorrentLocker
  - *寄發偽裝信件(內含連結)，使用者開啟連結並下載惡意程式，惡意程式開始加密檔案(*.encrypted)並刪除主機的陰影複製檔案(無從復原)*

贖金：只接受以Bitcoin交付

利用Tor網路交付贖金

資料來源:http://blog.trendmicro.com.tw/

案例分享
綁架勒贖-CryptoLocker

- CryptoLocker
  - 將檔案用最嚴謹的演算法RSA-2048加密，威脅於時限內交付贖金，才解密

資料來源:http://blog.trendmicro.com.tw/

72小時之內，
支付300美元贖金

案例分享
綁架勒贖-SynoLocker

- SynoLocker
  - 將檔案用最嚴謹的演算法RSA-2048加密，威脅於時限內交付贖金，才解密

資料來源:http://blog.trendmicro.com.tw/

贖金：只接受以Bitcoin交付

勒索軟體訊息在地化

- 勒索軟體訊息在地化
- 過去勒索軟體的訊息大多以英文為主...
  - 中文的勒索訊息。(如：Cryptolocker)
  - 語音撥放勒索訊息。(如：_RANSON.Cerbera)

台灣本土最強勒索軟體

- 每年5月傳出災情

勒索軟體

- 勒索軟體(前身：假防毒軟體-Fake AV「假好心」)
  - 惡意軟體
  - 迫使受害者無法存取個人設備
- 攻擊型態
  - 加密型勒索軟體
    - DB加密、PC檔案加密
  - 限制系統運作型勒索軟體
    - 鎖住(綁架)PC
    - 類似模式：DNS綁架、首頁綁架

不幸中獎之後


Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 12/05/14 - 21:37 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR
Prior to increasing the amount left:
103h 37m 58s
Your system: Windows 7 (x64) First connect IP:
Total encrypted 56 files.
Refresh
Payment
FAQ
Decrypt 1 file for FREE
Support
We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?
bitcoin
1. You should register Bitcon wallet (click here for more information with pictures)
2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:

付不付贖金？


新聞夜視界
TVBS新聞台 HD
雲林
DOW
17726.20
32.01
全台上千電腦遭"綁票" 不付贖金資料毀
23:27
鎖售翻倍 網購迎戰雙11 倉儲人力增1.5倍趕出貨
0:01 / 1:19

或者來個討價還價

1.9萬砍到1.1千　殺價勒索病毒集團成功...他大讚有誠意！

▲台灣網友中勒索病毒，跟對方殺價成功的條件式，幫忙在台灣網站上寫文章。（圖／翻攝自mobile01）

資料來源：http://www.ettoday.net/news/20170514/924233.htm

加密檔案無法破解嗎？

- 目前CryptoLocker勒索軟體使用2048位元的RSA及AES加密技術
- 若金鑰是真正隨機產生的話，現代的超級電腦也要無窮歲月才能破解

資料價值>破解成本？

密碼長度	26 英文字母	26 英文字母 +10 數字	52大小寫 英文字母	96 可印出字元
4	0	0	1 分鐘	13分鐘
5	0	10分鐘	1 小時	22 小時
6	50分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21萬9000年
10	45 年	1159 年	45838 年	2100萬年

勒索軟體解密工具整理

勒索軟體	提供解密方式的網站	說明與介紹
CoinVault	https://goo.gl/CmsVJA	防毒廠商卡巴斯金與荷蘭警方合作，在2014年9月逮捕了相關勒索程式的作者， 讓受到CoinVault與Bitcryptor等勒索程式 挾持的用戶，能解開加密。
Bitcryptor	https://goo.gl/CmsVJA	Bitcryptor等勒索程式挾持的用戶，能解 開加密。
Linux.Encoder.1	http://goo.gl/rjepxA	Bitdefender發現，Linux.Encoder.1勒索 軟體中含有漏洞，可直接回復AES金鑰而 不必利用RSA來解鎖。
多種勒索軟體	http://sensorstechforum.com/cryptodrop- prevents-ransomware- encrypting-data/	由美國佛羅里達大學網絡安全研究團隊所設計的 CryptoDrop 系統，其特點在於會 主動ft擊，時刻監控電腦內的資料之餘， 一旦發現到有勒索軟件後並不會阻止它們 啟動，反而是去阻止它們完成任務。
多種勒索軟體	http://esupport.trendmicro.com/solution/zh	由趨勢提供之勒索軟體檔案解密工具

支付贖金

中了勒索軟體該怎麼辦？FBI回答：解密資料的最快方法就是花錢消災！

美國FBI探員Joseph Bonavolonta近日在波士頓舉行的網路安全高峰會上表示，雖然鼓勵受害者向FBI報案，但FBI無法替受害者取回加密的資料，最簡單的方式就是支付贖金。還說勒索軟體賺很多錢的原因就是絕大多數的人都選擇了支付贖金，而且可能因為這樣，駭客也不會要求太高的贖金，同時也會履行承諾幫受害者解密。

資料來源:iThome

何謂比特幣

- 比特幣(Bitcoin)，是一種電子貨幣，使用點對點網路追蹤和驗證交易。
- 是沒有中央發行機構的(該幣是由類似線上遊戲中的挖礦活動所得到的)，沒有監管單位，可於網路上當作現金使用。
- 比特幣匯率：1比特幣=18,631.8382新台幣

為什麼要使用比特幣付贖金

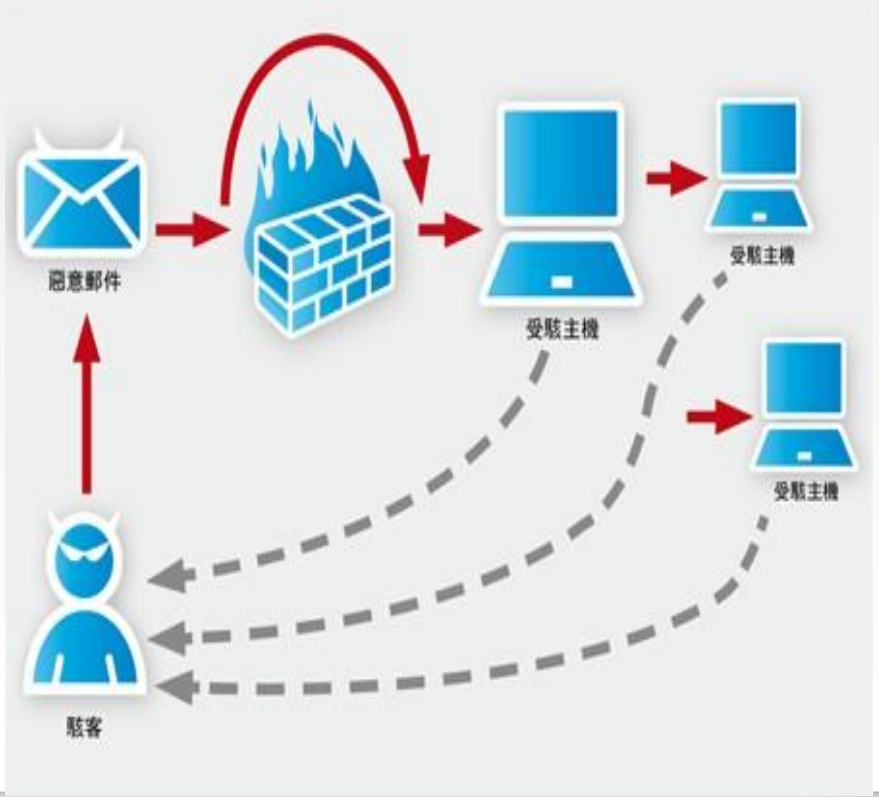
- 匿名性：比特幣的轉帳和交易都不需要附上真實姓名，有利駭客隱藏
  - 因為匿名特性，也讓駭客搞不清楚哪個受害者付了贖金
- 流通性：比特幣不受地域限制，便利全球化運作
  - 部分區域仍不流通比特幣
- 便利性：比特幣目前市佔率大、流通性佳，適合網路犯罪
  - 比特幣的操作仍不如其他幣值容易

散播的途徑

勒索病毒的散播途徑

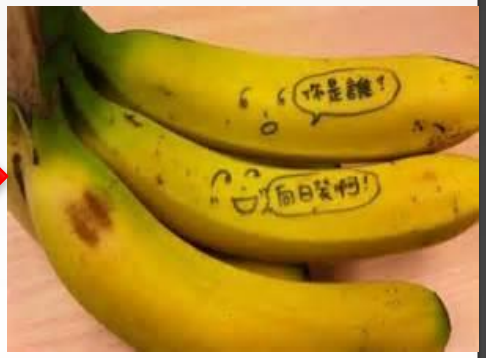
- 勒索病毒目前主要的攻擊途徑:
  - 惡意郵件
    - 釣魚連結和惡意夾檔
  - 網頁掛馬
    - 遭駭客入侵的網站
    - 惡意廣告
  - 弱點攻擊
    - IE browser
    - Java /Flash
    - Adobe

社交工程



Hacker的技倆

- 猜->破密分析(暴力、字典)
- 偷->植入惡意程式(spyware、key logger)
- 騙->社交工程
- 搶->Session Hijacking



你認為的社交工程

一般人的眼裡

老闆的眼裡

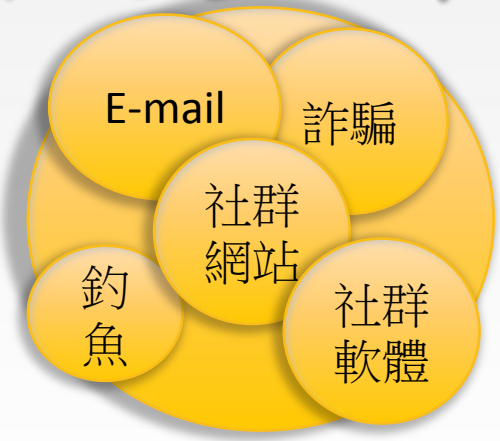
顧問的眼裡

詐騙集團的眼裡

駭客的眼裡

社交工程所扮演的角色
資安攻擊的基石

社交工程



社交工程所扮演的角色
資安攻擊的基石

社交工程所扮演的角色
給我一個支點我將舉起地球

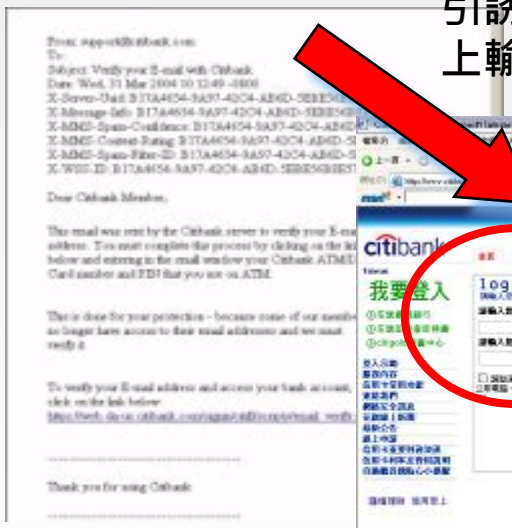
網路釣魚（Phishing）

- Phishing是個結合 Phone 和 Fishing 特殊的英文專有名詞
- 典型網路釣魚包含幾可亂真的電子郵件與詐騙網頁
  - 利用偽造的網頁作為誘餌，詐騙使用者洩漏如帳戶密碼等個人機密資料

網路釣魚網站攻擊方式示意

駭客

假冒銀行通知郵件



引誘使用者到假冒網站
上輸入帳號及密碼

花旗銀行-http://www.citybank.com.tw

駭客利用使用者
密碼登入真實網站

花旗銀行-http://www.citibank.com.tw

案例分享
您的快遞簽收單

詐騙訊息，上面寫著「**您的快遞簽收通知單，收件電子憑證 http://goo.gl/OOOO**」，如果亂點，訊息就會引導使用者下載並安裝病毒程式，請大家謹慎以對！

公司的防護有效嗎？

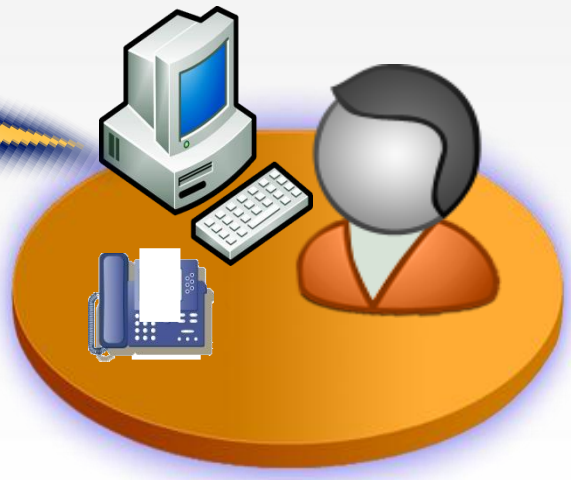
任何病毒都別想進來

合法掩護非法

釣魚網站

掛馬網頁

下載惡意軟體(勒索軟體)



有心人士

內部員工

合法掩護非法(續)

您的快遞簽收通知單，收件電子憑證

我的手機送修，麻煩替我收個簡訊好嗎

學運受傷學生急需醫藥費

社交工程有什麼影響

- 公司
  - 個資外洩
  - 違反個資法
  - 刑、民事責任
- 個人
  - 個資外洩
  - 個資遭盜用
  - 信用破產

案例分享
史上最嚴重，全台1.7億筆個資外洩

▼全台1億7000筆個資大外洩 2嫌聲押獲准

資料來源：東森新聞

電影：竊資達人

社交工程有什麼影響

- 勒索軟體
  - 資料遭加密
  - 系統(服務)停擺
  - 有形或無形損失
- 殭屍電腦
  - 個人電腦遭控制，隱私、機密全都露
  - 成為犯罪工具(共犯結構)-DDoS
  - 刑、民事責任

如果醫院被勒索了

TO PAY OR NOT TO PAY

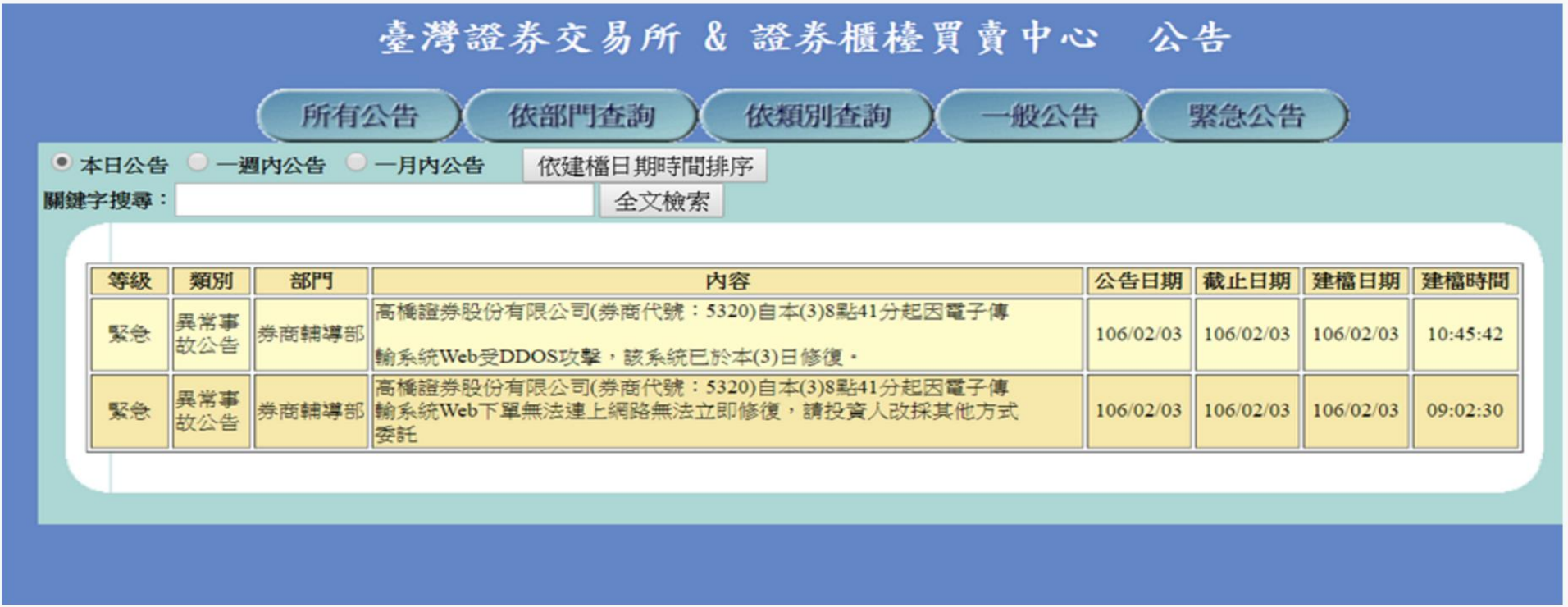
案例分享
駭客入侵醫院主機，挾病例勒索逾1億

駭客入侵醫院主機　挾病例勒索逾1億

美國洛杉磯好萊塢長老教會醫療中心（Hollywood Presbyterian Medical Center）驚傳主機遭到駭客入侵，被勒索9000比特幣（約1.1億元台幣）贖金。翻攝英國廣播公司

案例分享

多家券商證實遭DDoS攻擊，駭客揚言不付錢再打



臺灣證券交易所 & 證券櫃檯買賣中心　公告

所有公告 | 依部門查詢 | 依類別查詢 | 一般公告 | 緊急公告

本日公告　一週內公告　一月內公告　依建檔日期時間排序

關鍵字搜尋：　全文檢索

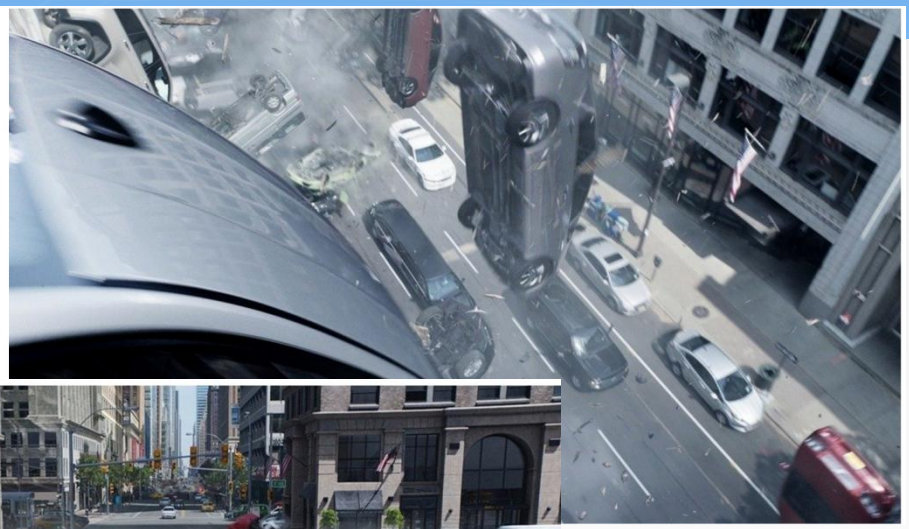
等級	類別	部門	內容	公告日期	截止日期	建檔日期	建檔時間
緊急	異常事故公告	券商輔導部	高橋證券股份有限公司(券商代號：5320)自本(3)8點41分起因電子傳輸系統Web受DDOS攻擊，該系統已於本(3)日修復。	106/02/03	106/02/03	106/02/03	10:45:42
緊急	異常事故公告	券商輔導部	高橋證券股份有限公司(券商代號：5320)自本(3)8點41分起因電子傳輸系統Web下單無法連上網路無法立即修復，請投資人改採其他方式委託	106/02/03	106/02/03	106/02/03	09:02:30

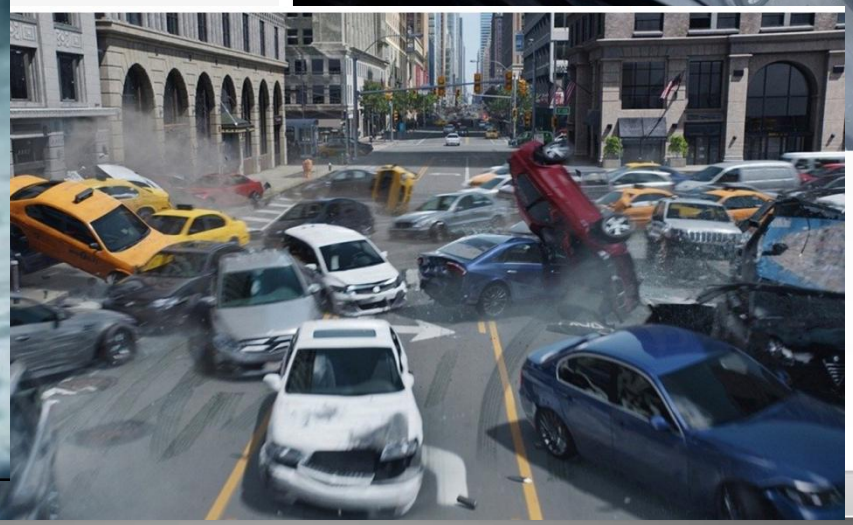
資料來源：iThome

案例分享
舊金山輕軌系統遭遇勒索軟體攻擊
但他們寧可讓乘客免費搭乘也不願付贖金

舊金山輕軌系統是在週五晚上被證實遭到駭客入侵，一直到週六當天乘客搭乘輕軌系統時還沒有解決。在 MUNI 車站的顯示螢幕上，顯示著這樣的訊息：
你的系統已經遭駭，所有資料已被加密。請聯繫（cryptom27@yandex.com）ID:681 。

電影：玩命關頭8-殭屍車隊





資料來源：噓星聞

案例分享
手機APP遙控汽車

資料來源：車訊網

案例分享
除了車之外，其實飛機也可以

「德國之翼」班機墜毀失事，第二具黑盒子也就是飛航資料紀錄器，日前找到經過判讀，證實副機師故意把客機降到一百英呎的高度低飛，並且多次微調自動駕駛功能，讓飛機撞山墜毀。飛安專家認為，如果有軟體，可以把機師的致命指令，整個覆蓋掉，然後把飛機帶往安全的地方降落，那麼也許這起悲劇，就不會發生。

機師波頓，如果有越來越多人知道，覆蓋軟體的存在，那也許壞人會利用這項軟體搞破壞，這將會是一件很糟糕的事，飛行員也擔心，如果飛機被植入這套軟體，要是被駭客惡意操控，那後果更加不堪設想，這恐怕也是當初空巴，決定放棄研究覆蓋軟體的原因之一，究竟機上乘客的命運，該放在電腦還是人腦上，兩派專家各持己見。

個人資安防護建議

勒索軟體防護措施

- 軟體更新
  - 作業系統(Windows、OS X)、應用軟體(Java、Frish、防毒軟體)
- 資料備份
  - 備份頻率(每週、每月、每季)
  - 備份媒體(隨身碟、外接式硬碟、雲端)

緊急處理加密勒索軟體威脅7原則

- 緊急處理加密勒索軟體威脅7原則
  - 中斷網路連線
  - 即刻發現，應立即關機(10分鐘內還有資料可救回-端看電腦速度)
  - 緊急宣導、清查不可少
  - 評估災情
  - 系統重灌，但軟體防護要更注意
  - 保存現場狀況，請求支援
  - 沒有辦法中的辦法：付贖金
- 搶救只是權宜之計，預防更加重要

資料來源：http://www.ithome.com.tw/tech/101366

社交工程防護

個人資訊勿隨意登錄於不明網站

* E-mail 管理
  - 區分公司及個人使用之信箱
  - 在外登錄註冊之信箱，容易收到許多垃圾郵件，使用時務必小心
  - 不回覆來源不明之郵件
* 定期安檢作業
  - 即時更新軟體修補程式
  - 即時更新防毒軟體及病毒碼
  - 經常對系統進行檢測
* 實體隔離
  - 機敏資料應於實體隔離主機上作業

社交工程防護(續)

* 停—使用任何電子郵件軟體前，須先確認以下設定
  * 是否已安裝防毒軟體並確實更新病毒碼
  * 取消郵件預覽功能(outlook express/檢視/版面配置/預覽窗格，不要勾選顯示預覽窗格的設定)
  * 儘量使用純文字模式開啟信件(outlook express/工具/選項/讀取/讀取郵件，☑在純文字中讀取所有郵件)
* 看—收到信件後必須注意
  * 信件主旨是否與本身業務相關
  * 開啟信件前須先確認信件來源，否則建議刪除
* 聽—若懷疑信件來源必須進行確認
  * 透過電話或電子郵件向寄件人確認信件真偽

社交工程防護(續)

- 不要瀏覽非工作相關或不信任的網站
- 不要下載安裝未經認可的軟體或程式
- 隨時更新作業系統與應用程式
- 安裝必要的防護軟體
- 不要開啟可疑或非工作相關的信件附檔
- 對任何提到”緊急”或”個人金融”保持懷疑態度
- 對信件有任何一點疑慮千萬不要點選Email裡的超連結
- 不要填寫Email裡有關個人金融資料的表格
- 在網站上輸入信用卡號或個人資料時先確認該網站安全性

社交工程防護(續)

- 不將Email留在任何公開的網頁上
- 不開啟來歷不明之信件
- 不轉寄非必要之信件
- 不回應任何未知的信件
- 安裝防止網路釣魚詐騙的工具軟體
- 經常或定期登入你的網路帳號
- 定期確認你的銀行帳戶、信用卡的交易狀態都正確無異常
- 確認你的瀏覽器、收信軟體、文書軟體及其他程式是最新版本，而且都已更新修補程式
- 自助互助，告知相關單位你發現的網路釣魚事件

結論

- 預防重於治療
- 隨時注意更新
- 正確的觀念

Q&A 問題討論