資訊安全講習-4

- 資 訊 科 技 與 競 爭 優 勢 -

李政峰 (James Lee)
經濟部工業局-能源管理系統輔導顧問
教育機構驗證中心ISCB個資講習顧問
Line：bear1858

- ISO 27001 主導稽核員
- ISO 20000 主導稽核員
- ISO 9001 內部稽核員
- BS 25999 主導稽核員
- BS 10012 主導稽核員
- SSCP 合格完訓
- CISSP合格完訓

Agenda

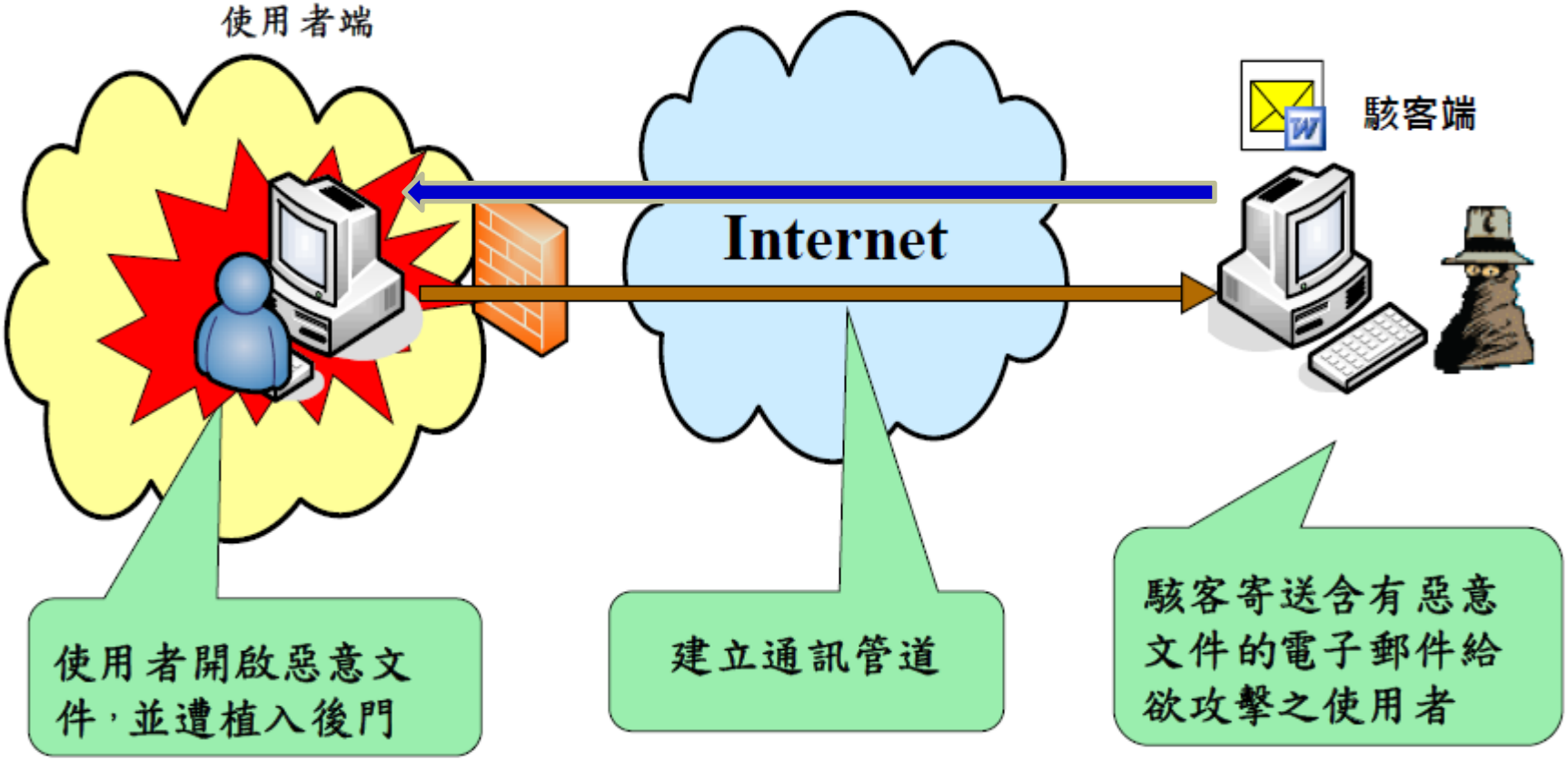
- 電子郵件社交工程
- 商務電子郵件詐騙
- 防止隨身碟病毒的保護方法
- 好習慣掌握行動裝置安全
- 資訊安全案例分享
- 課後評量

電子郵件社交工程

- 資 訊 科 技 與 競 爭 優 勢 -

社交工程攻擊模式

主要利用電子郵件攻擊



電子郵件的社交工程類型

- 假冒寄件者
- 使用讓人感興趣的主旨與內文
- 含有惡意程式的附件檔案
- 利用0_DAY攻擊

躲在正常網站後的惡意網站

駭客熟知你我的操作習慣

台視全球資訊網 www.ttv.com.tw TTV ·設為首頁·

| 台灣台 | 家庭台 | 財經台 | 國際台 | 會員 | 購物 | 新聞 | 影音 | 遊戲 | BLOG | 討論

台視新聞

政治 | 財經 | 社會 | 醫藥 | 國際 | 科技 | 文化 | 體育 | 娛樂 | 綜合 | 照片 | 氣象

TTV》新聞》

網路劫標客 相仿帳號發信騙錢
數字1小寫L 肉眼難辨成漏洞

報導記者：郭于中 941206

Print Email

網路拍賣詐騙手法又翻新，一位民眾在網路上向取名flora的賣家購買手機，沒想到，收到的得標信，卻是署名f一ora，由於一跟英文字母小寫的L，實在太過相近，被害人沒發現，就把錢給轉出去，對於類似的詐騙手法，連網路拍賣業者都說還沒聽說過。

網路上琳瑯滿目的拍賣

BEC 商務電子郵件詐騙

- 資 訊 科 技 與 競 爭 優 勢 -

BEC 商務電子郵件詐騙

BEC 商務電子郵件詐騙

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- 在這些年來，駭客最容易賺錢的方法之一是勒索病毒攻擊。這些攻擊利用強有力的加密技術來讓受害者無法使用自己的檔案和資料 – 然後攻擊者再出售解密金鑰來換取無法追踪的比特幣贖金。
- 但是現在又有另一種高獲利的攻擊手法出現，特別是針對了企業。

防止隨身碟病毒的保護方法

- 資 訊 科 技 與 競 爭 優 勢 -

防止隨身碟病毒的保護方法

保護自己，也保護別人，大家一起來。

如何知道您的隨身碟有沒有中毒?

- 在隨身碟建立 AUTORUN.INF資料夾，使病毒無法建立 AUTORUN.INF檔案。
- 若看到隨身碟中已有autorun.inf 和奇怪的****.exe 檔存在，則表示可能已中毒。

清除隨身碟autorun. inf等病毒檔

- 結束隨身碟防毒設定，也可比照設定C、D等槽，加入〈autorun.inf〉資料夾避免autorun.inf 侵入C、D等槽。

清除隨身碟autorun. inf等病毒檔

- autorun.inf 目錄（資料夾）的屬性必需記得設定為【唯讀】與【隱藏】，在 autorun.inf 資料夾按「右鍵」，選（內容），再設定即可。

好習慣掌握行動裝置安全

- 資 訊 科 技 與 競 爭 優 勢 -

LINE安全性

常見詐騙訊息內容

這是過年時候大家聚會的照片，好珍貴的留影，你快看看吧
地址： “http://URL.CN/EZS4UT”

您的民事賠償訴訟通知單[高雄地院]
“http://9xm.cn/qs5”

尊敬的客戶，您的手機正在申請6800元的網路支付，如非本人請立即回報 “http://103.42.15.183/10086.apk”

親愛的會員，您所購買的商品已送達超商門市，取件資訊為
“http://shengri.cn/c？11685606”

LINE安全性

朋友請我回撥 沒關係吧?

2017起未來3年重大資安事件

- 資 訊 科 技 與 競 爭 優 勢 -

1. 破解電子鎖竊盜

資料來源：iThome 文/黃泓瑜 | 2017-03-15

大部分公司、家庭和汽車逐漸拋棄過去傳統門鎖，轉而使用電子鎖來管理門禁。但是，駭客一旦破解了其中一個電子鎖，就可能會同時破解內部其它電子鎖，形成門戶大開的情形，駭客之後再利用機器來竊取物品。這種偷竊方式，不但可以直接在遠端遙控，偷盜效率更高、時間縮短，還難以讓警方查到犯罪者的身份。

最近美國地下論壇，駭客已經公開徵求會寫電子鎖程式的駭客來破解電子鎖，共同策劃在夜間入侵某企業內部的竊盜計畫，並且還拍了各種電子鎖照片，詳細說明電子鎖按鈕形狀、感測距離等，所以2018年會開始出現這類科技竊盜的案件，甚至今年就會發生。

2. 無人車自行解體、綁架

資料來源：iThome 文/黃泓瑜 | 2017-03-15

預計在2019年會有很多駭客跟無人車結合的竊盜事件，他舉出，未來駭客只要鎖定大量汽車的內部系統來發動攻擊，然後破解車庫電子鎖來打開車庫門，之後遠端操控這些汽車到回收廠，並且下達解體車體的指令，汽車就會自行解體變成一堆汽車零件，駭客就能夠高價販賣這些零件來獲取利益。

他認為未來自動駕駛技術會開始盛行，汽車駕駛系統、安全系統和車門系統都可由遠端來操控，駭客不僅可以利用自動駕駛系統來竊盜，還能夠利用車門系統來關閉汽車門鎖，或是操控駕駛系統引導自動駕駛車到荒郊野外，來綁架特定人士。

3. 東京奧運遭勒索攻擊

資料來源：iThome 文/黃泓瑜 | 2017-03-15

2020年奧運在東京舉辦，日本政府已經宣稱東京奧運要全面自動化、IoT化，包括運動員身上會配戴各種偵測裝置、無人車會載觀眾或是貴賓到指定旅館入住，以及利用IoT裝置操控飯店設備等。張裕敏預測，駭客可以鎖定這些自動化裝置、偵測裝置和IoT裝置發動勒索攻擊，要求奧運主辦單位勒索比特幣，否則就癱瘓這些裝置，干擾奧運活動的進行。

資訊安全案例分享

- 資 訊 科 技 與 競 爭 優 勢 -

驚！臉書系統漏洞遭駭 恐影響約5,000萬用戶

資料來源：聯合新聞網 聯合線上2018年9月29日

臉書發生系統出現漏洞遭入侵事件，影響將近5,000萬個帳戶。 路透社

驚！臉書系統漏洞遭駭 恐影響約5,000萬用戶

資料來源：聯合新聞網 聯合線上2018年9月29日

- 全球社群網站龍頭臉書（Facebook）29日表示，本周稍早發現一起系統出現漏洞、遭入侵事件，影響將近5,000萬個帳戶。該公司已修正漏洞，並已知會執法當局。臉書股價29日盤中應聲重挫3.5%。
- 臉書發布聲明表示，本周稍早發現其名為「View As」的功能程式碼有漏洞，駭客能藉此漏洞接管用戶的帳戶，目前已修正漏洞，並已知會執法官員。超過9,000萬名臉書用戶29日也被迫登出帳戶，這是帳戶被駭知後的常見安全措施。
- 臉書表示，還不知道駭客的來源或身分，也仍無法完全評估整起攻擊的規模，該公司的調查仍在起步階段，還待確認這些帳戶是否遭濫用或是否有資訊遭不當取得。

臉書史上最大資安危機？

資料來源：科技報橘 2018年9月29日

駭客利用「零時漏洞」入侵臉書，影響上千萬帳號

- 此次事件可說是臉書史上最大規模的資安漏洞，連官方都喊罕見的發布了安全公告，主動說明了此次的事情。
- 根據臉書的公告與其他媒體的報導，駭客透過了「檢視角度（View as）」功能中的漏洞，取得了「存取權杖（Access Token）」資料，並可能藉此進入受影響者帳號查看相關個人資訊。
- 「檢視角度（View as）」的功能，是臉書過去推出的一個隱私工具，它可以讓使用者透過其他用戶的角度查看自己帳號呈現在特定用戶前的樣貌，讓用戶確認自己的那些資訊是否有被公開給特定對象。
- 臉書認為另外一個上傳生日祝賀影片的功能，也包含了類似的漏洞，一樣可以讓駭客取得權限，查看受影響者的帳號內容。

臉書史上最大資安危機？

資料來源：科技報橘2018年9月29日

相關漏洞存在超過一年才被發現，臉書：無法估計損害程度

- 但這次事件最令人擔憂的點，在於漏洞存在的時間，以及臉書對於入侵程度的把握。
- 據調查，此次事件中駭客採用的漏洞，早在 2017 年 7 月就已存在，然而臉書直至 2018 年 9 月 25 日才發現相關漏洞，雖然展開了緊急修補作業，卻仍遲至 27 日才將相關問題修復完成，並在 28 日採其他應對措施。
- 除此之外，臉書在官方報告中坦言，由於他們才剛展開調查，目 前他們無法確認駭客入侵的程度、帳號受影響的狀態，駭客的攻擊目的、攻擊者的身分等關鍵資訊 ，若他們在後續調查中有任何發現，他們也將會第一時間發布更新資訊告知用戶。

課後評量

- 資 訊 科 技 與 競 爭 優 勢 -

感謝您的聆聽！