網路手機的資訊安全案例分享

劉得民
Diamond Liu
0932-212-913
dmliu99999@hotmail.com

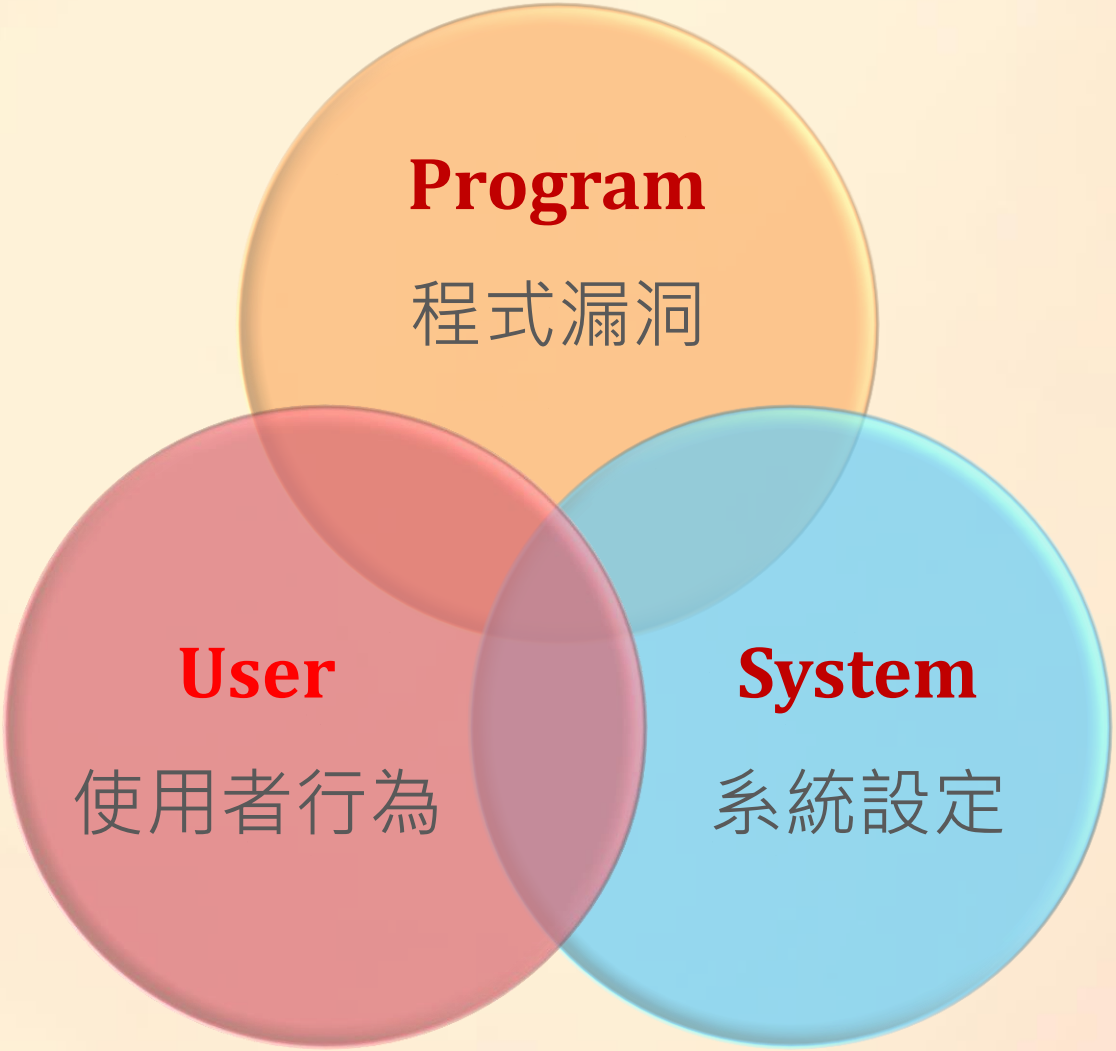
網路手機的資訊安全案例分享

- 資訊安全之基本說明
- 無線存取點欺騙與防範
- 手機安全與個資防護
- 檔案加密勒索與防範
- 電郵社交工程與防範
- Q&A

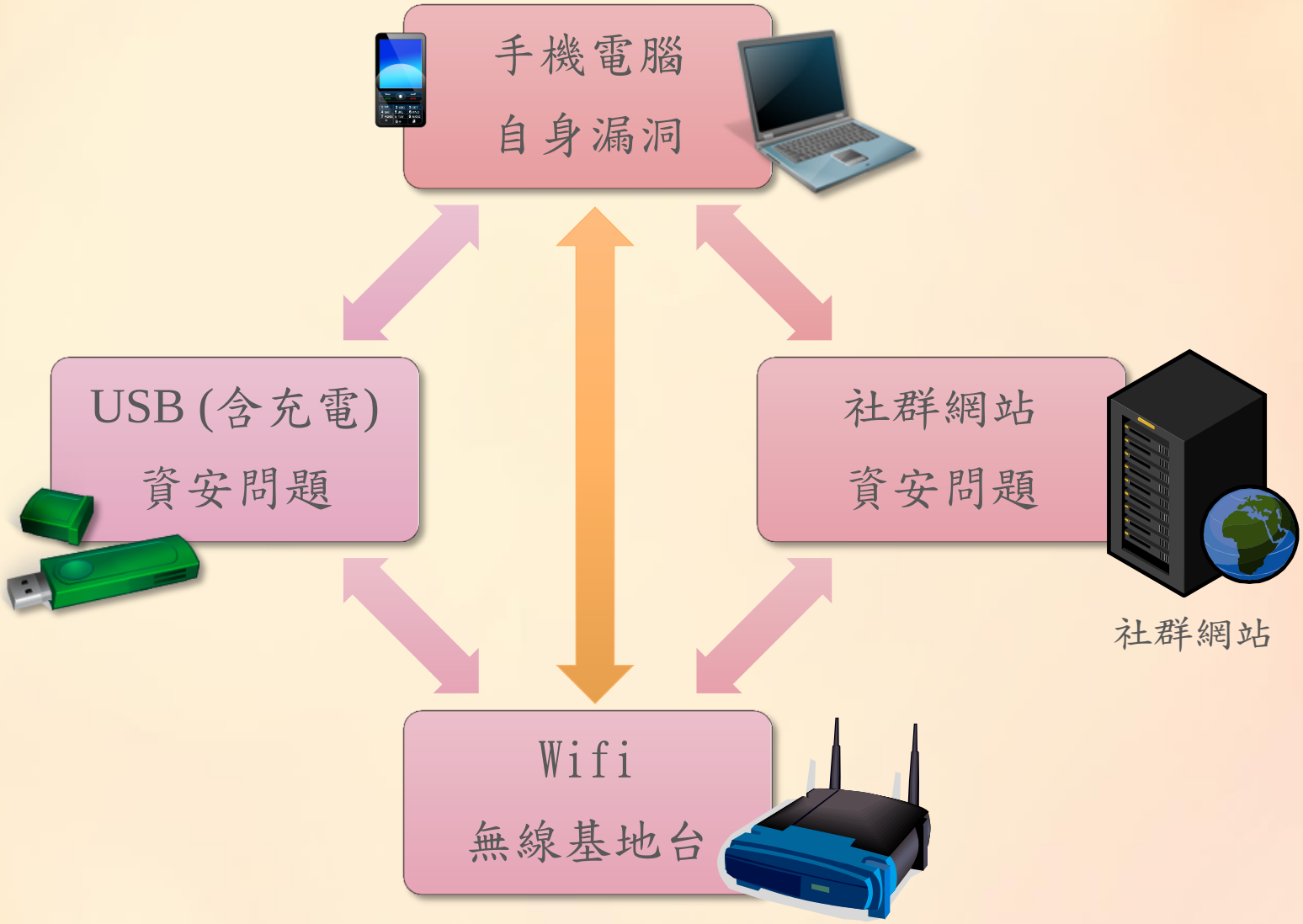
資訊安全之基本說明

劉得民
Diamond Liu
dmliu99999@hotmail.com

網路駭客攻擊的主要途徑



常見資安防範基本知識



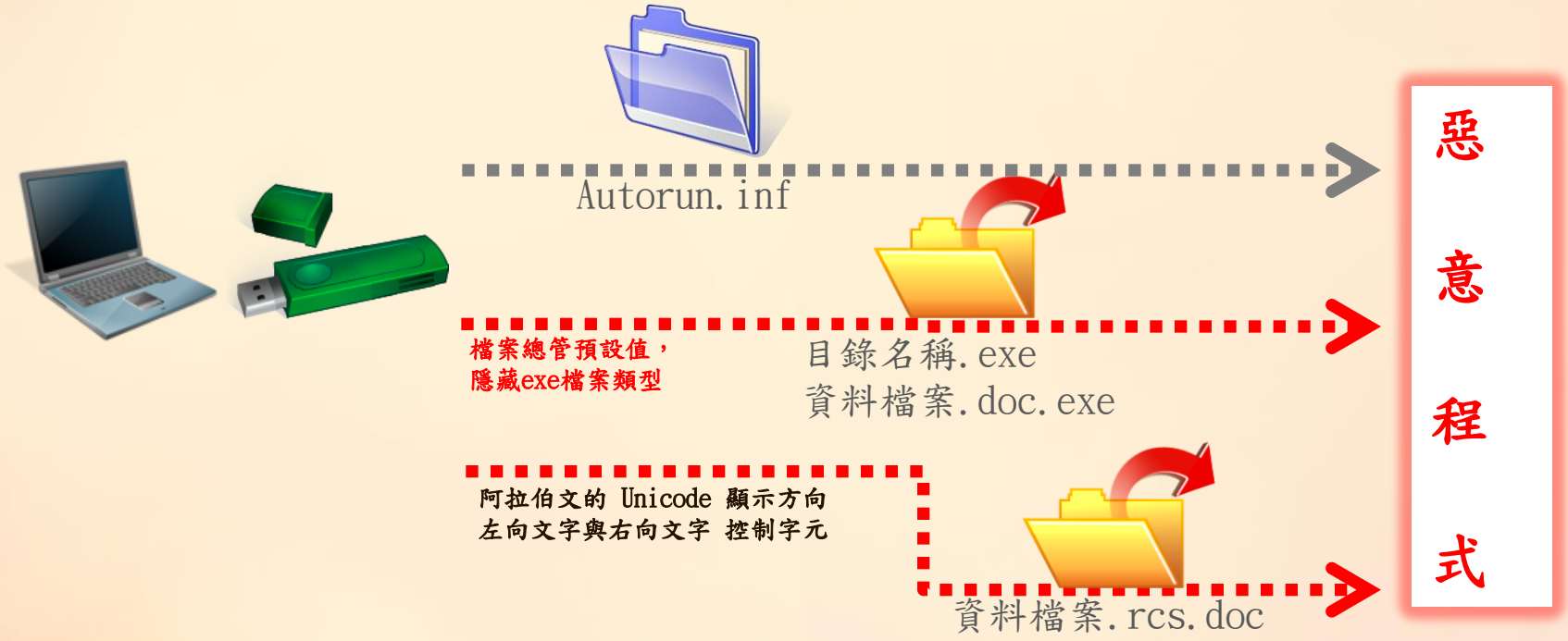
USB 隨身碟的資安防範

常見USB儲存設備病毒種類

A. 自動執行方式　惡意程式隱藏於 Autorun.inf（比較少見）

B. 隱藏文件方式　惡意程式儲存於**正式文件.doc.exe**、**目錄名稱.exe**、**檔案目錄捷徑.lnk**

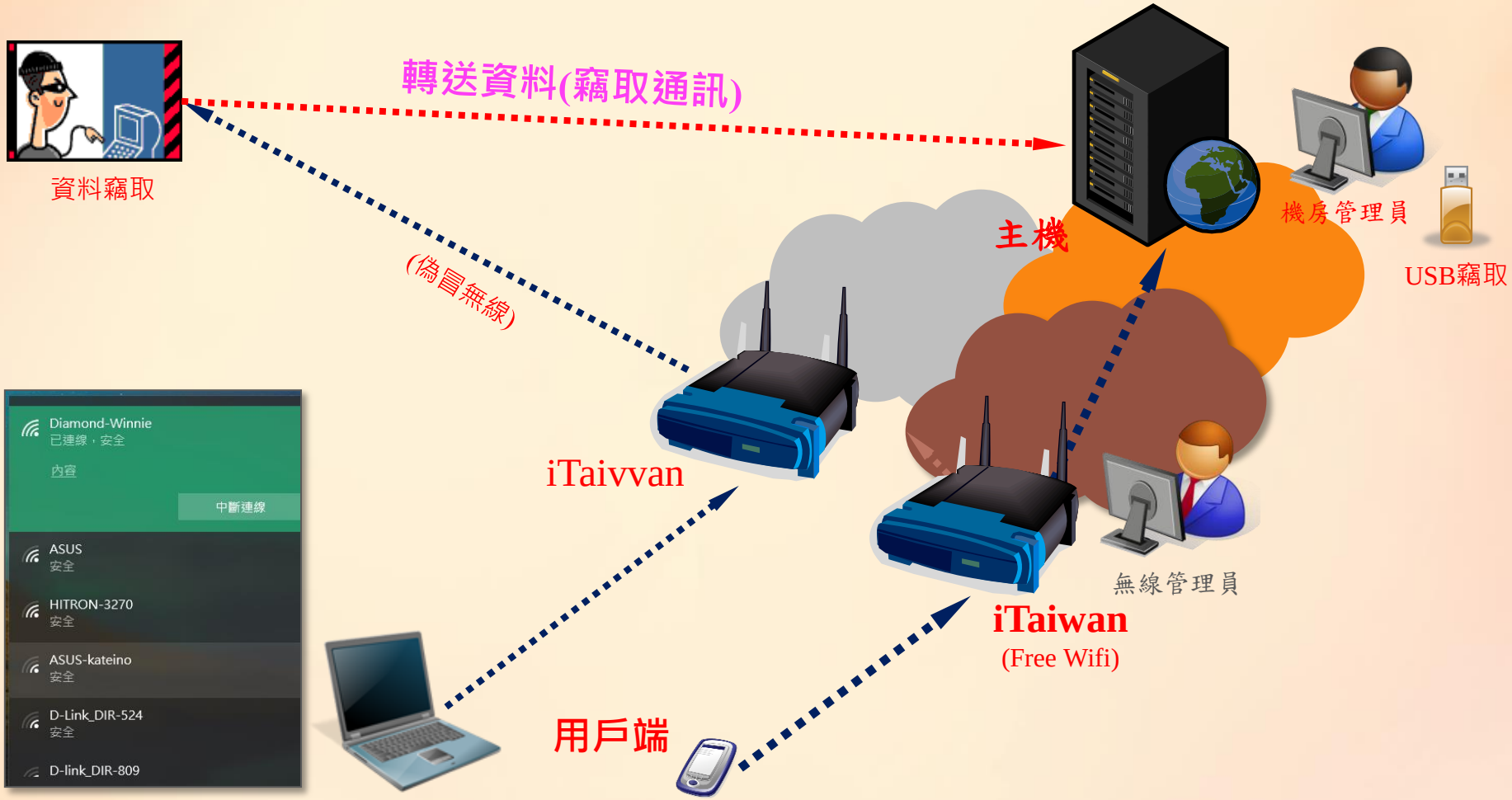
惡意程式的部分檔案名稱，採用『右向文字』顯示



無線存取點欺騙與防範

劉得民
Diamond Liu
dmliu99999@hotmail.com

無線網路Wifi的資安問題



Wifi 的WPA2資安漏洞

WPA2 加密機制爆漏洞, 五招自保以防Wi-Fi 上網遭偷窺| 資安趨勢部落格
https://blog.trendmicro.com.tw › 資安小百科 › WiFi ▾
2017年10月19日 - 最近，Wi-Fi 無線網路加密協定WPA2 被揭露多項安全漏洞，據稱可能讓Wi-Fi 無線裝置遭到所謂的「金鑰重新安裝攻擊」(Key Reinstallation AttaCK，簡稱KRACK)，是一種針對WPA2 加密機制漏洞的概念驗證攻擊。KRACK 採用的是「篡改並重送加密交握訊息」的手法，也就是從系統和裝置在彼此通訊之前交換參數的 ...

【Wi-Fi加密大崩壞】超詳細WPA2協定弱點廠商修補進度大整理(11/6更...
https://www.ithome.com.tw/news/117532 ▾
2017年10月17日 - https://support.apple.com/en-us/HT208222WPA2漏洞的曝光，讓全球Wi-Fi加密連線面臨高風險，不只微軟、Google、蘋果都展開因應，網通、作業系統等超過40個廠牌業者也緊急提出因應對策，不論是先公布受影響產品，或緊急釋出更新，都詳細整理在這裡。清單最近更新時間：2017/11/26 12:00.

14年來最大威脅，WPA2加密協定安全拉警報| iThome
https://www.ithome.com.tw/news/117600 ▾
2017年10月20日 - ... 網通廠商、作業系統業者的夢魘，全球數十億上網裝置Wi-Fi加密傳輸也恐面臨高風險，不論是Android手機、iOS裝置，或Windows電腦、Linux設備都有可能遭殃，甚至連使用WPA2加密傳輸的相機或Wi-Fi記憶卡，都可能面臨資料曝光的風險。14年來沒有出現弱點的WPA2加密協定，竟然出現了高風險的資安漏洞。

【Wi-Fi加密大崩壞】WPA2為何不再安全？剖析KRACKs攻擊原理| iThome
https://www.ithome.com.tw/news/117583 ▾
2017年10月20日 - 無線網路加密通訊協定WPA2弱點被揭露，不同於過去破解方式，而是在終端裝置剛接入Wi-Fi時，建立初始連線的四向交握階段，以密鑰重裝方式攻擊。因此，攻擊者靠近有漏洞的無線AP網路訊號範圍內，等終端裝置要接入時就可發動攻擊。

【Wi-Fi加密大崩壞】WPA2爆重大漏洞恐外洩加密資料，危及所有Wi-Fi ...

Wi-Fi使用WPA2加密遭惡意入侵，Android用戶問題最嚴重 | 數位時代

https://www.bnext.com.tw/article/46565/wifi-found-vulnerability-on-wpa2 ▼

2017年10月17日 - 人人都在使用的無線網路Wi-Fi被發現漏洞，只要使用WPA2加密方式連網的用戶，都可能受到影響。包含微軟、Apple等公司，都出面表示已釋出系統 ...

【WPA2漏洞】微軟已推安全更新蘋果OS與Android還需數週- UNWIRE.HK

https://unwire.hk/2017/10/17/wpa2krackpatch/tech-secure/ ▼

2017年10月17日 - Wi-Fi 用到的加密技術WPA2（Wi-Fi Protected Access II）被發現存在漏洞，能受到「KRACK」攻擊，在資訊保安界成為一大炸彈。而Wi-Fi 規格標準化 ...

美國政府證實：Wi-Fi「WPA2」協定爆漏洞，Android 修復速度最慢 ...

3c.ltn.com.tw/news/31694 ▼

2017年10月17日 - 據了解，由於WPA2 能加密用戶在網路中傳輸的資料，讓傳輸的內容即使被攔截，惡意駭客也無法得知用戶在做哪些事，不過一旦WPA2 協定被破解， ...

【Wi-Fi加密大崩壞】全球數10億裝置遭殃！14個QA了解WPA2新漏洞 ...

https://www.ithome.com.tw/news/117511 ▼

2017年10月17日 - 包括Windows、Linux，iOS和Android平臺的裝置全部受影響. ... KRACKs（Key Reinstallation AttaCKs）是一系列WPA2協定漏洞的總稱。WPA2是 ...

Wi-Fi WPA2 security cracked: Android & Linux most vulnerable, but ...

https://9to5mac.com/2017/10/16/wifi-wpa2-hacked/ ▼ 翻譯這個網頁

2017年10月16日 - Update: Apple says the security vulnerability has been fixed in the beta versions of

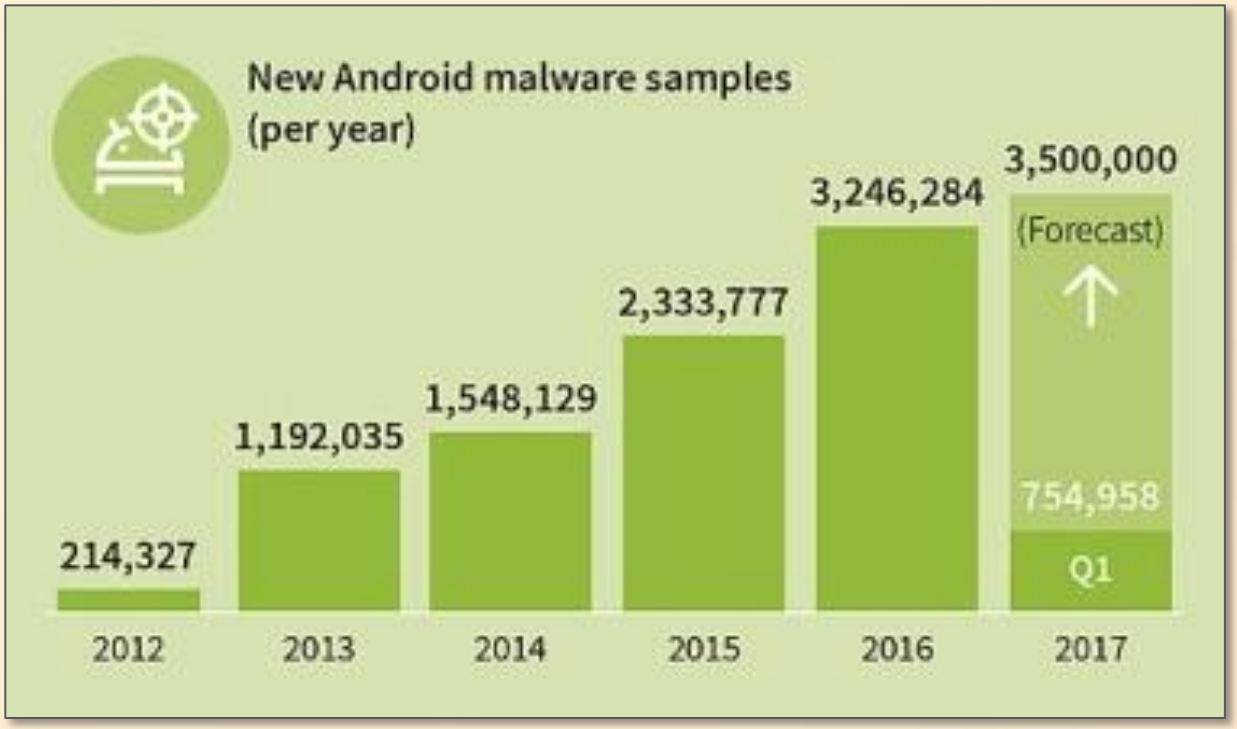
案例學習重點

- **免費無線網路，要仔細判斷**
  - 偽裝免費無線網路服的方式，非常簡單
  - 手機與電腦的資料，可以透過偽冒無線基地台擷取。
- **無線網路的WPA服務有嚴重漏洞:**
  - 所有的無線網路WPA2協定，有嚴重漏洞，要立刻修補!!!
  - 家裡的無線基地台，可以被駭客從遠端偷資料(WPA2漏洞)
  - 筆電盡可能使用有線網路, 手機平板則盡可能使用3G/4G/5G服務!!
- **無線網路，要採用HTTPS網路服務**

手機安全與個資防護

劉得民
Diamond Liu
dmliu99999@hotmail.com

Android手機，最容易被攻擊



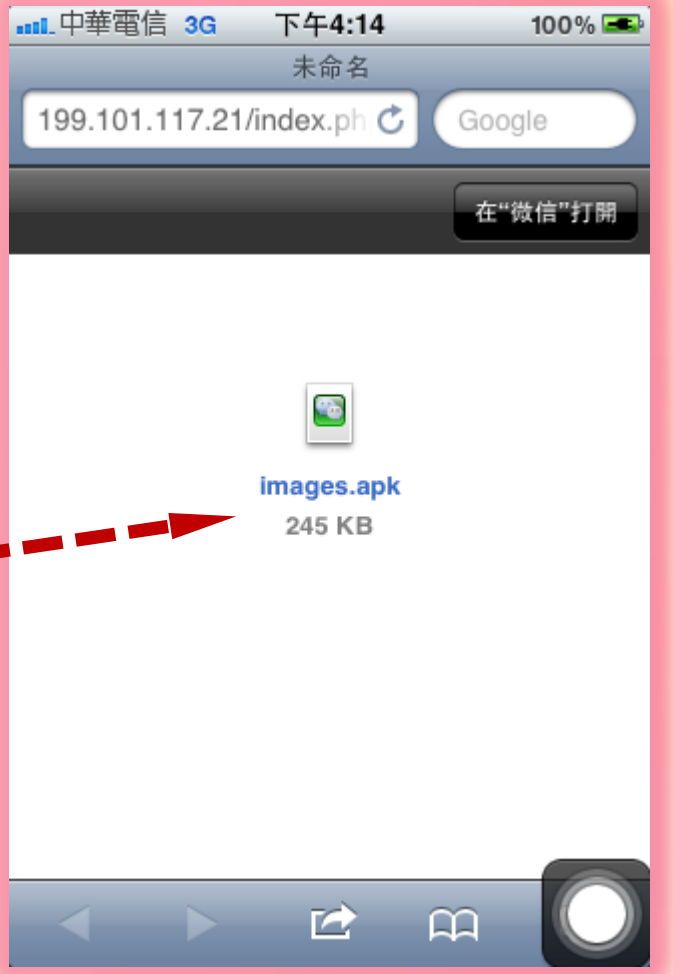
舊型Android系統，容易被駭

- 每 10 秒鐘就會發現一款新的 Android 惡意應用程式。
- 2017年5月的統計資料
  - 全球只有4.9%的Android裝置升級Android 7.0，而該系統已經發佈了8個多月。
  - 升級到Android 6.0的手機，31.2%。
  - 將近32%的手機使用Android 5.0 (漏洞很多)。
  - 20%執行Android 4.4以下的版本 (容易感染病毒)。
- 沒有更新到最新的Android版本，主要因素
  - **手機製造 OEM 廠商不提供舊裝置的Android系統更新。**
- 大部分手機惡意應用程式，主要出現在非Google官方的第三方應用商店。

Android 病毒入侵百萬個 Google 帳戶！

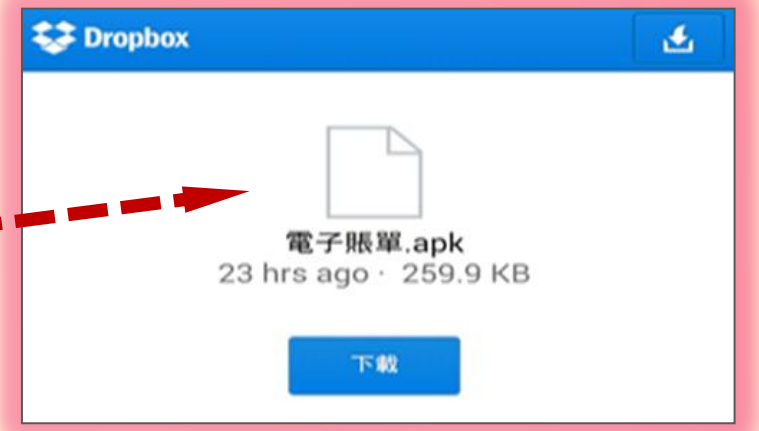
- 該惡意軟體主要的感染途徑，仍是第三方來源的 App 安裝進入用戶電腦，也就是非 Google Play 以外的安裝管道。受到感染後，除了會被竊取手機內資料，同時還會獲取手機 Root 權限、竊取用戶的 Email 位置，以及認證權限（authentication tokens）。
- 透過這個認證權限，駭客得以進入用戶的 Google 帳戶，竊取郵件、相片、文件等私人檔案。更糟的是，該惡意軟體還會感染 Google Play，下載其他受感染的應用到用戶手機內，並且在手機內展示大量的廣告。
- 這個 Android 惡意軟體特別需要用戶關注，原因在於他會感染多種 Google 原生 App，包含 Google 相簿、Google 雲端硬碟、Google 文件等，藉此偷取裡面的資料。

Android手機 的 可執行檔案 APK



手機 各種詐騙方式

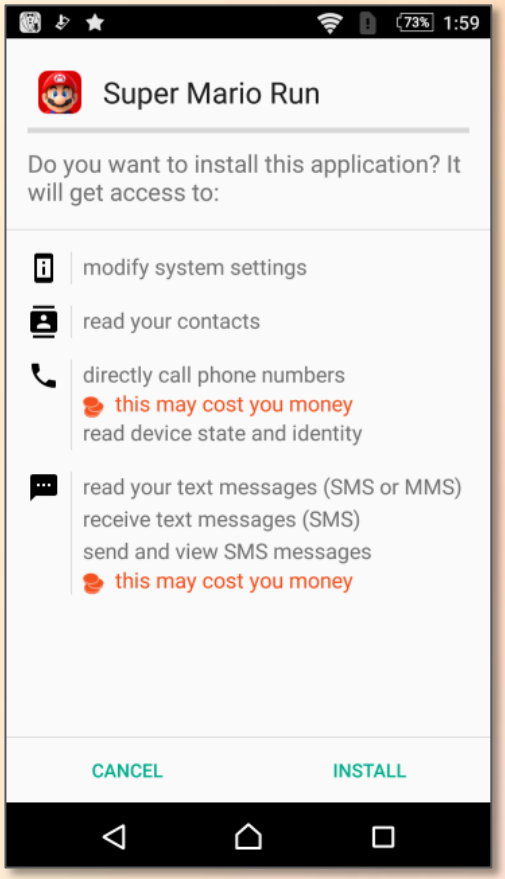
- 手機接獲訊息（內含網址URL連結）
  - 費用帳單、快遞資訊、好友訊息 …
  - 「上次聚餐照片，你不在好可惜！」 、 「被偷拍的是你嗎？」、「取消網路支付電費」、「快遞簽收單」…



用手機-聽音樂, 結果...

假借遊戲程式，竊取手機資訊

- 假《超級瑪利歐酷跑》偷走信用卡資訊!
  - 在用戶安裝手機遊戲時，它會要求包括**聯絡人、手機號碼及文字簡訊存取權**，藉此蒐集敏感資訊。
  - 要求裝置管理員權限，能讓它隱藏自己真正的圖示，也使得用戶想要卸除它更為困難。
  - 用戶安裝完成時，會跳出貌似Google Play的輸入對話框，要求用戶輸入信用卡號碼，而且無法繞過。它還能做到驗證信用卡，包括辨識信用卡(Visa或Mastercard)，並使用Luhn演算法檢查信用卡號碼真偽。
  - 如果輸入無效信用卡，它還會顯示錯誤訊息。



安裝手機App軟體的權限問題

安裝手機App軟體的權限問題

安裝手機App軟體的權限問題

手機 App 疑問?!

安裝修圖軟體、美肌軟體、照相軟體、影片軟體、遊戲軟體... 需要這麼多資訊嗎?

包括我們的應用程式紀錄、使用者身份、通訊資訊...

2016-中國大陸-網路安全法

BloombergTechnology | China Adopts Cybersecurity Law Despite Foreign Opposition

China Adopts Cybersecurity Law Despite Foreign Opposition

Bloomberg News

2016年11月7日 下午 01:33 TST *Updated on* 2016年11月7日 下午 04:56 TST

- Law takes effect in 2017 and imposes certification requirement
- Foreign tech firms worry it will shut them out of the market

China has green-lit a sweeping and controversial law that may grant Beijing unprecedented access to foreign companies' technology and hamstring their operations in the world's second-largest economy.

2016-中國大陸-網路安全法

BloombergTechnology ▼ | China Adopts Cybersecurity Law Despite Foreign Opposition

The requirement on certification could mean technology companies will be asked to provide source code, encryption or other critical intellectual property for review by security authorities. This is something Microsoft already does with its software, under controlled conditions.

The law also requires business info and data on Chinese citizens gathered within the country to be kept on domestic servers and not be transferred abroad without permission. That last condition hampers the operations of multinationals accustomed to a global Internet computing environment.

"A number of IT companies have really serious concerns. We don't want to see barriers put up," U.S. Deputy Secretary of Commerce Bruce Andrews told reporters during an October visit to Beijing. "Cross-border data flow has become increasingly important to trade and to companies in the way they operate every day."

案例學習重點

1. APK檔案，是Android的可執行檔案之一。點選 APK或apk檔案，是危險的手機行為。
2. 不要安裝來路不明的遊戲程式，或是遊戲破解軟體。
3. 舊型Android手機(5.0以前的版本)，容易造成駭客入侵。
4. 重要資料備份，至少每2個月進行一次。
5. 某些App，疑似預藏惡意行為程式(過多的操作權限)。
6. **中國大陸政府，2017已經通過網路安全法，加強網路監控。**

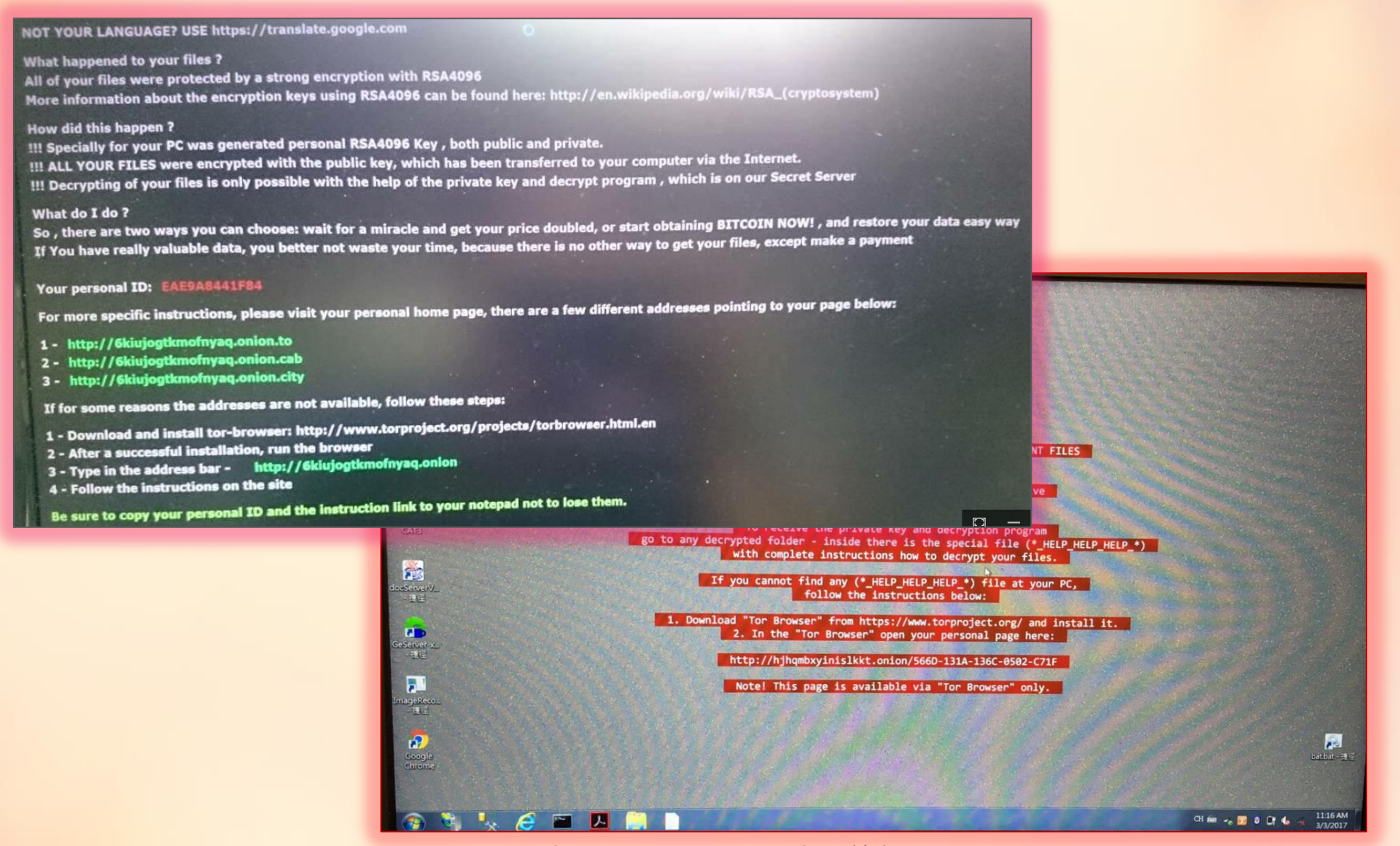
檔案加密勒索與防範

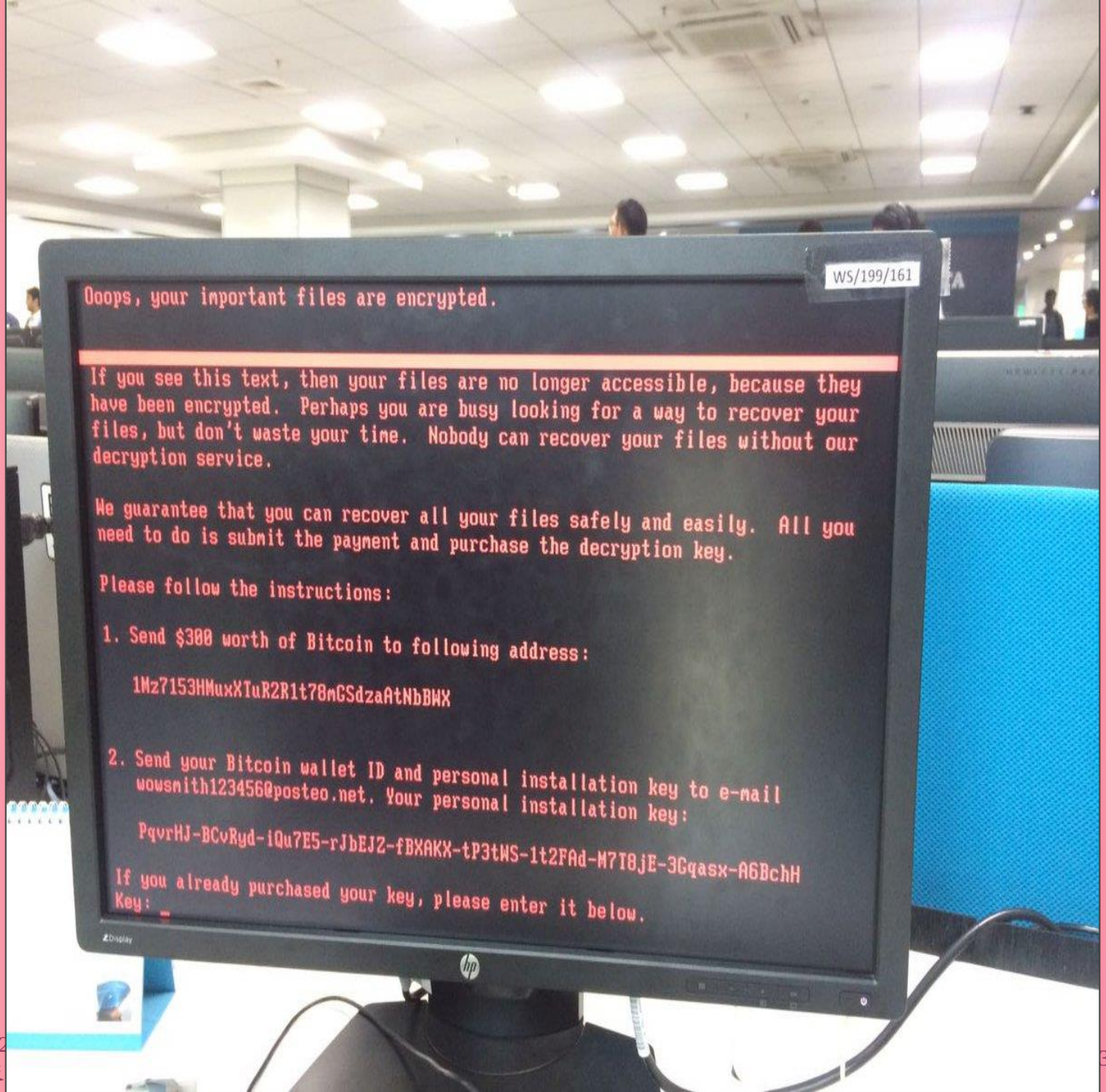
劉得民
Diamond Liu
dmliu99999@hotmail.com

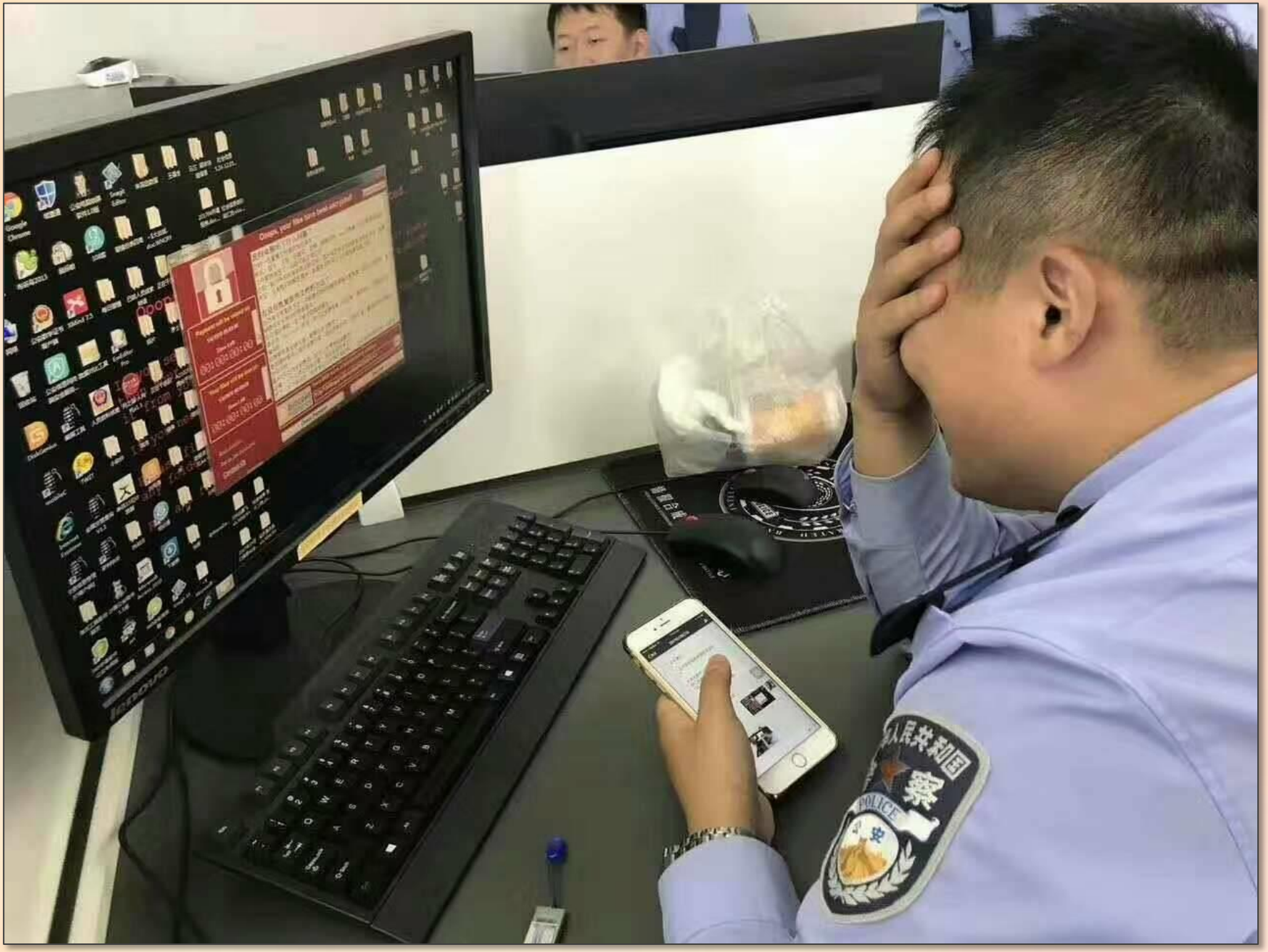
Android勒索軟體DoubleLocker現身，不僅加密還會變更你的手機密碼

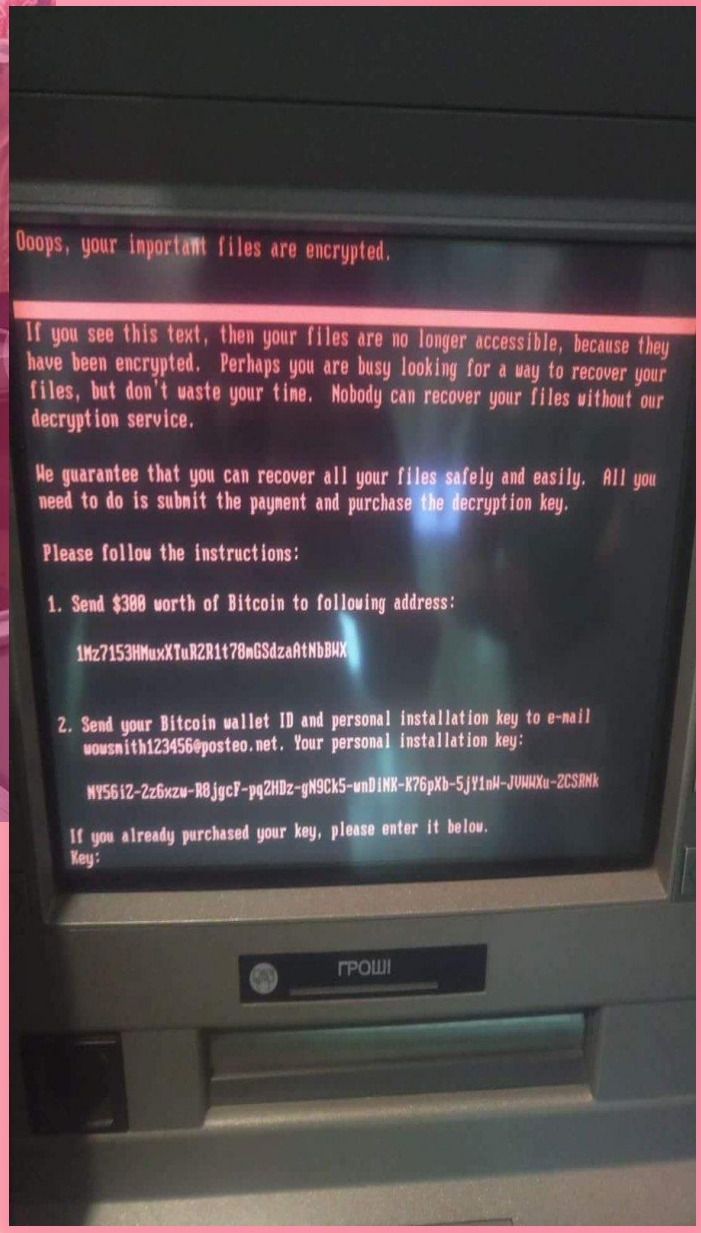
ESET指出DoubleLocker會使用了兩種方法鎖住Android裝置。除了以AES加密檔案，還會變更裝置的PIN碼，新PIN碼為隨機設定，只有攻擊者可遠端重設PIN碼。是第一次出現擁有兩種封鎖技倆的惡意程式。

瀏覽網頁，電腦檔案被加密勒索




WS/199/161
Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
PqvrHJ-BCvRyd-iQu7E5-rJbEJ2-fBXAKX-tP3tWS-1t2FAd-M7I8jE-3Gqasx-A6BchH
If you already purchased your key, please enter it below.
Key:

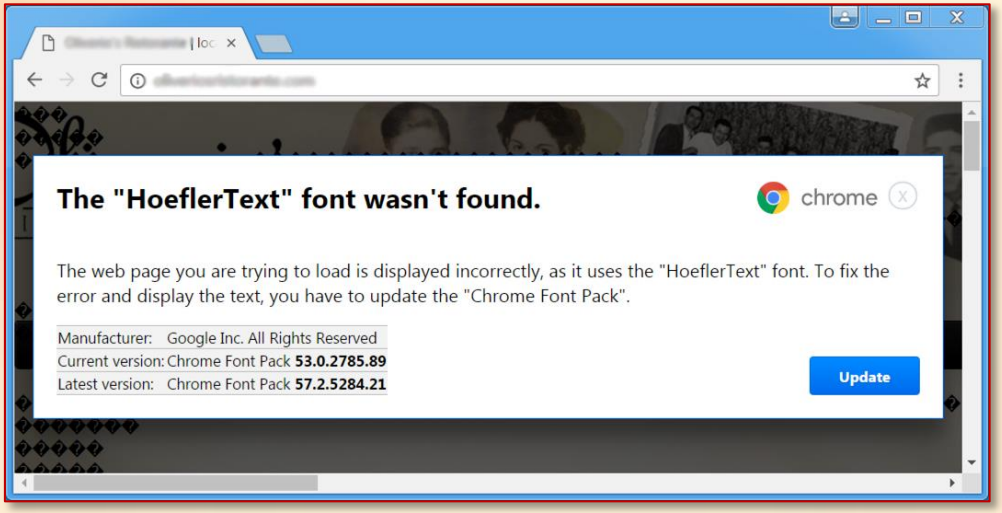


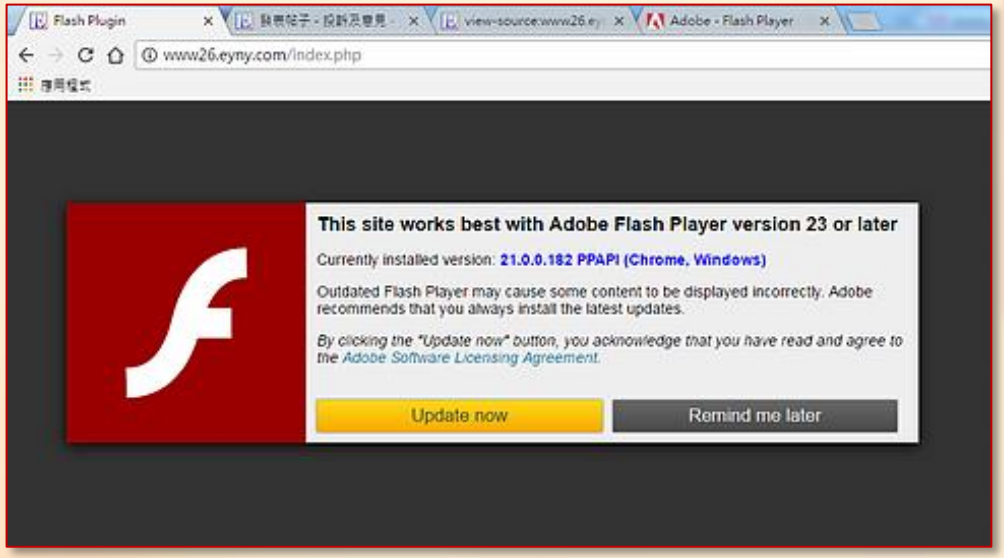


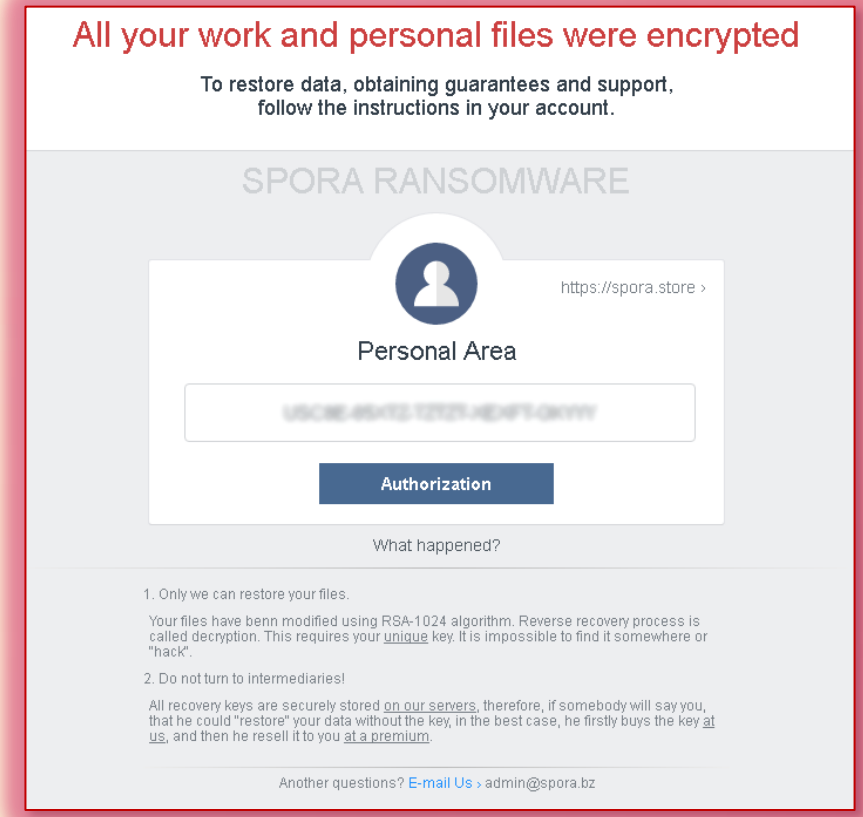
勒索病毒曾經使用的網路釣魚

1. iPhone中獎通知
2. 應徵者求職信(偽裝履歷表壓縮檔)
3. 金融機構的電子帳單郵件
4. 假冒 Chrome, Facebook 和 PayPal 電子郵件
5. 假冒 Microsoft, Adobe, Java 的更新通知
6. 瀏覽網頁，要求安裝字型

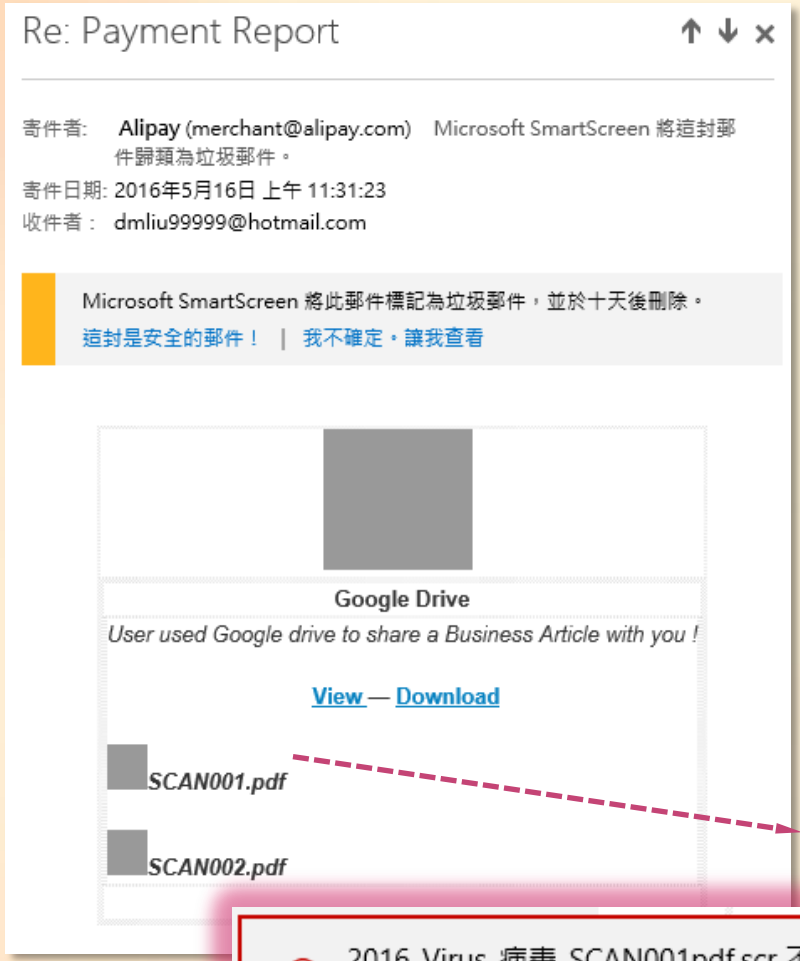
論壇網站遭入侵(網頁掛馬,假訊息)



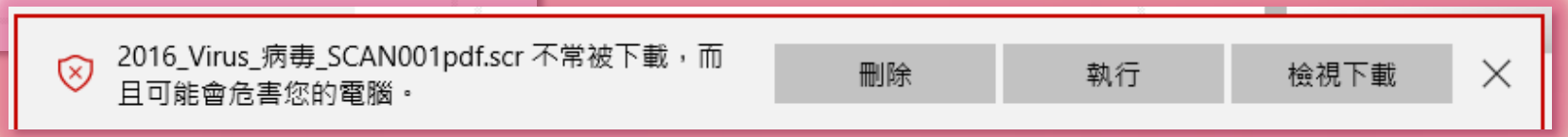




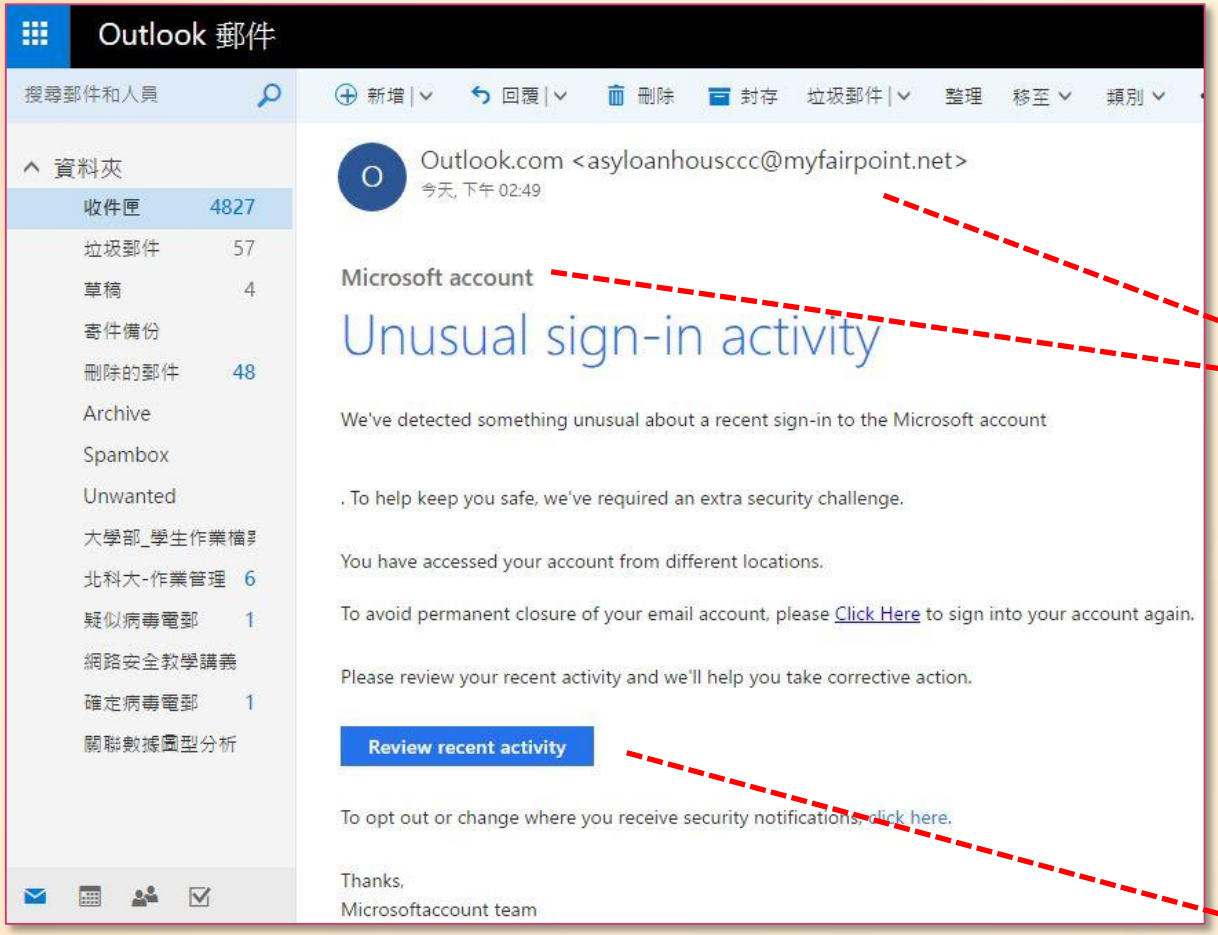
開啟電郵，電腦檔案被加密勒索



電子郵件，金融對帳單，提醒瀏覽(下載)
(這是惡意程式)



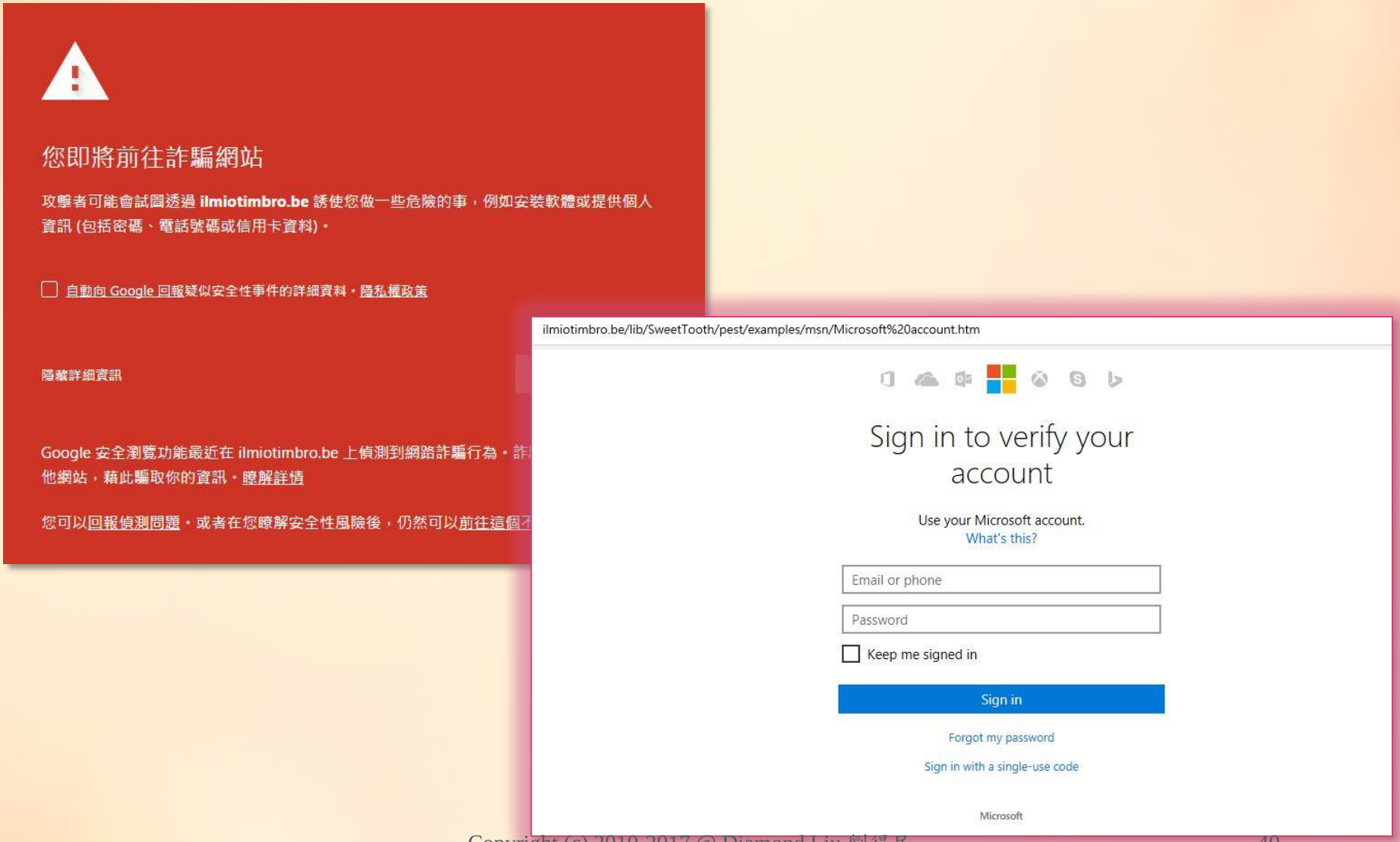
開啟電郵，電腦檔案被加密勒索



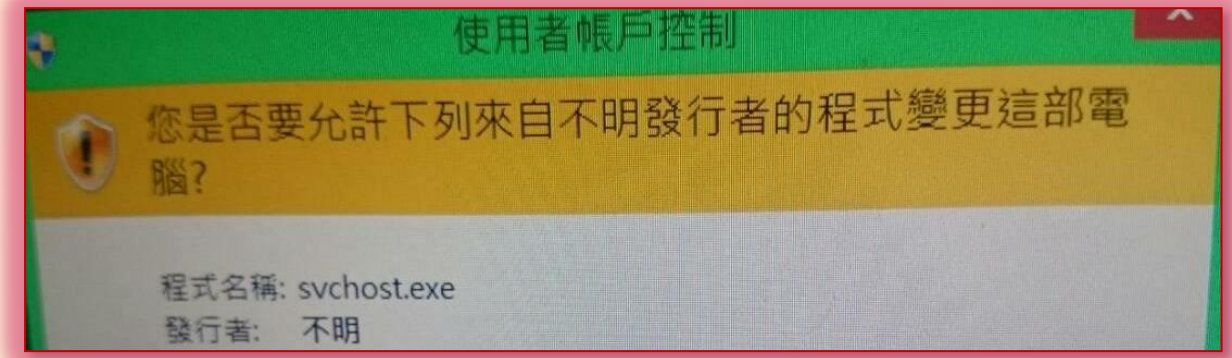
寄件人資訊，怪怪的！

駭客寄送的惡意程式

開啟電郵，電腦檔案被加密勒索



瀏覽網頁，需要特殊權限?



小心!! 這是駭客放置的加密勒索病毒

案例學習重點

- 加密勒索常見偽冒方式
  - **偽冒網址**, 利用英數字的相近 (O與0, l與1, W與VV, m與rn, C與G …)
  - **偽冒網站**, 利用網址的管轄差異(.com.tw 與 .com.cn)
  - **免費更新**, 利用被害人 (貪小便宜、好奇心 …)
  - **電子郵件**, 利用操作疏失(點選 郵件 URL附件 下載)
  - **舊版漏洞**, 利用系統未安裝更新版本

webmail.tku.edu.tw	webmail.tku.eud.tw	大學電郵
www.chinatrust.com.tw	www.chinatnust.com.tw	金融銀行
TW.BID.YAHOO.COM	TW.BlD.YAHO0.COM	拍賣網站
www.landbank.com.tw	www.1andbank.com.tw	金融銀行
www.china-airline.com.tw	www.china-air1ine.com.tw	航空公司
www.google.com.tw	www.goog1e.com.tw	網路服務
www.outlook.com	www.0utlook.com	電郵服務
www.microsoft.com	www.micoosoft.com 或 www.rnicrosoft.com	

臉書與網路詐騙之案例討論

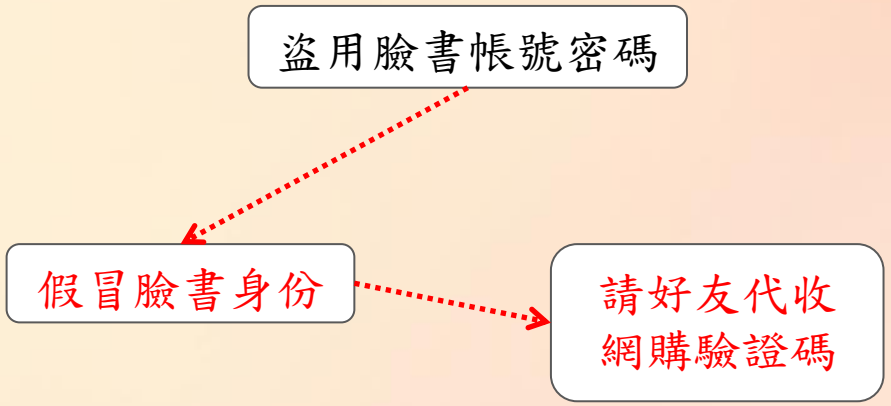
劉得民
Diamond Liu
dmliu99999@hotmail.com

社群網站資料防護的漏洞

1、你或家人的生日日期
2、你的感情狀態
3、你目前的所在位置
4、你的個人習慣
5、小朋友的私人資訊

智慧手機-臉書-Line之詐騙分析

1. 假網頁、真詐騙
2. 盜用帳號，進行詐騙
   - 駭客結合臉書與Line
   - 網購詐騙 -> 驗證碼
   - 誘騙臉書好友代收



臉書-Line之詐騙分析

臉書-Line之詐騙分析

臉書-Line之詐騙分析

臉書-Line之詐騙分析

臉書-Line之詐騙分析

透過臉書/Line的低價購物

Facebook 親友電郵遭駭　真實案例

假藉Facebook名義 入侵電腦

熱門的社群交友機制,Facebook, 許多人都有在其中種菜養魚的經驗，最近有電子郵件假借Facebook帳號通知的名義，該電郵信件內容(中英文皆有)：為了確保帳號安全，要求用戶重新設定Facebook帳號。

若是使用者若想要知道其重新設定的帳號，就必須先開啟郵件中的附件檔案，來誘使Facebook使用者開啟郵件中夾帶檔案。而實際上這個附件檔中隱藏了一個名為「Trojan Bredolab」的木馬程式。


The Facebook Team
To:
Facebook_Password_7a343.zip (23.8 KB)
Facebook Password Reset Confirmation.
Hey ,
Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.
Thanks,
The Facebook Team
The message comes with a .zip file containing a malici
as Trojan.Bredolab.
This variant of Bredolab connects to a Russian domain and the infect
botnet.

Facebook 親友電郵遭駭　真實案例

假藉Facebook名義 入侵電腦

熱門的社群交友機制,Facebook, 許多人都有在其中種菜養魚的經驗，最近有電子郵件假借Facebook帳號通知的名義，該電郵信件內容(中英文皆
設定Facebook帳號。

若是使用者若想要知
中的附件檔案，來誘
而實際上這個附件檔
的木馬程式。


The Facebook Team
To:
Facebook_Password_7a343.zip (23.8 KB)

Facebook Password Reset Confirmation.

Hey ,

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

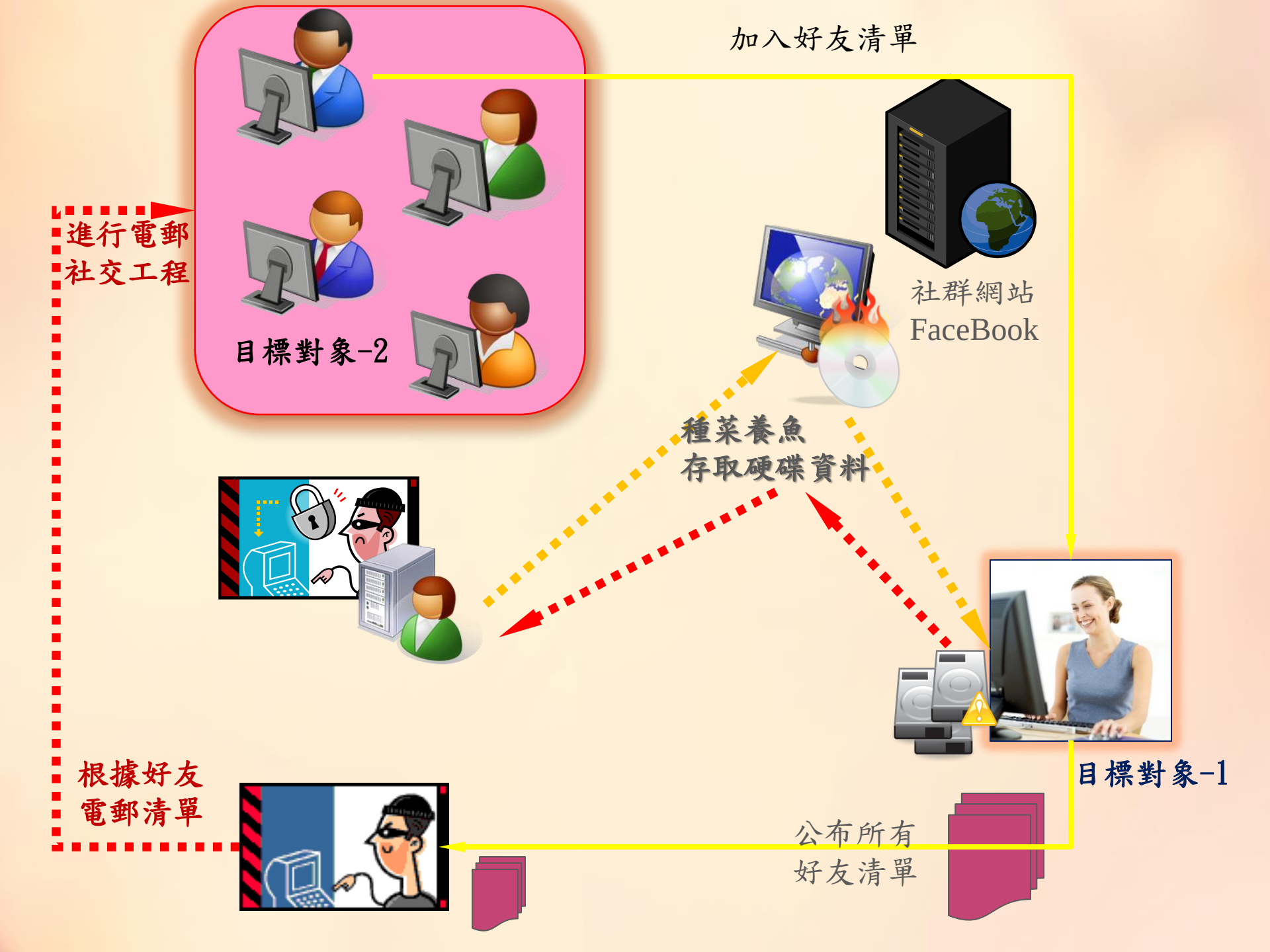
Thanks,
The Facebook Team

假借服務電郵，詐騙帳號密碼

臉書社群的駭客攻擊分析

- **社交工程問題**: 透漏親戚朋友的通訊電郵資料。
- **遊戲程式問題**: 內建遊戲程式可以存取電腦資料。
- **惡意轉接問題**: 連接詐騙假網站， 安裝惡意程式。
- **身分偽造問題**: 社群網站無身分驗證，假冒親友。
- **洩漏行蹤問題**: 透過資料分析，洩漏工作內容。
- **網購詐騙問題**: Facebook 親友要求代接手機驗證碼。

- 過去，檔案P2P分享軟體很方便，資安問題也很多!
- 現在，社群網站機制很熱門，資安問題誰來提醒？！


加入好友清單
進行電郵
社交工程
目標對象-2
社群網站
FaceBook
種菜養魚
存取硬碟資料
目標對象-1
根據好友
電郵清單
公布所有
好友清單

社群網站的遊戲程式問題

“开心水

14:11 , Qi

历时2个月

游戏地址:

简介: 这

如而神奇

接下来还有

吸引力的新颖:

> **引用**
>
> 北京双鱼互动招聘美术设计/flash工程师/java_web工程师
> 双鱼互动是一个专业从事scoial game开发的创业公司.如果你对这个行业有兴趣，欢迎你加入
>
> 我们现在需要如下:
>
> 学历要求：不限
> 薪资待遇：6K-8K 税后

联系我们

北京智明星通科技有限公司

客服邮箱: support@elex-tech.com
商务邮箱: biz@elex-tech.com
公司电话: +8610-82800116 +86-186-1156-2829
公司地址: 北京市海淀区中关村大街19号新中关大厦写字楼A座9层

合肥智明星通软件科技有限公司

客服邮箱: kfzp@elex-tech.com
商务邮箱: biz@elex-tech.com
公司邮箱: hf-hr@elex-tech.com
公司电话: 0551-4663787
公司地址: 合肥市高新区动漫和服务外包产业发展基地B3楼四层

同意 不允許

確定要按下『同意』嗎？

臉書社群的駭客攻擊分析

- **開心農民、開心農場、陽光牧場的軟體發展公司**
  - 北京、上海、合肥...
  - 智明星通、五分鐘軟體公司、熱酷傳媒...

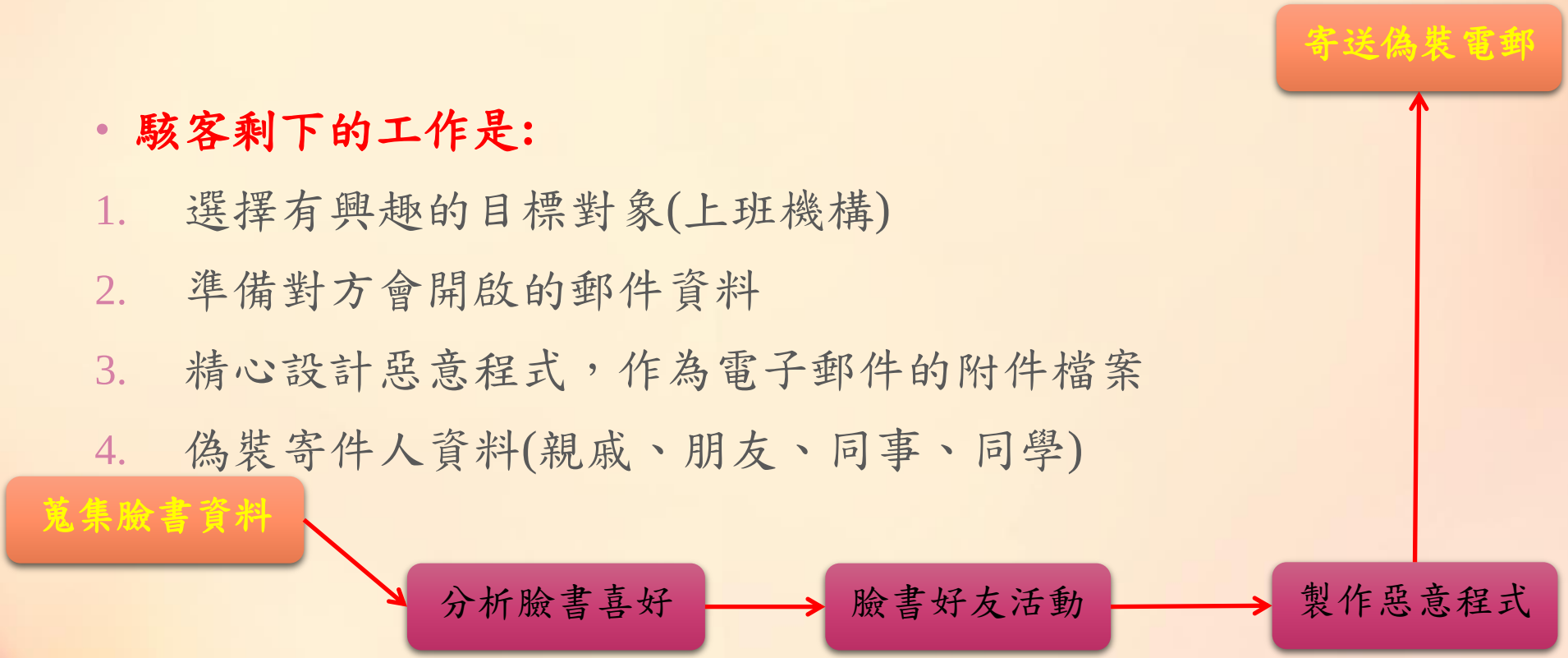
- **令人驚奇的疑問是??**
  - 中國大陸使用金盾工程(GFW)過濾對外網際網路通訊。
  - 中國大陸自2009/07開始，因為擔心『網路茉莉花革命』效應，因此禁止全中國大陸使用Facebook！
  - Facebook的遊戲發展公司，如何除錯? 如何連線?
  - 這些軟體公司與中國大陸官方幕後的關聯與影響是什麼?

臉書社群的社交工程

- 透露親友聯絡資料(親戚、朋友、同事、同學)
- 顯示自身完整記錄(學校、工作、喜好、活動)
- 親友完整聯絡紀錄(活動、照片、內容)
- 私人電子郵件信箱(gmail, hotmail, yahoo.mail)

- **駭客剩下的工作是:**

1. 選擇有興趣的目標對象(上班機構)
2. 準備對方會開啟的郵件資料
3. 精心設計惡意程式，作為電子郵件的附件檔案
4. 偽裝寄件人資料(親戚、朋友、同事、同學)



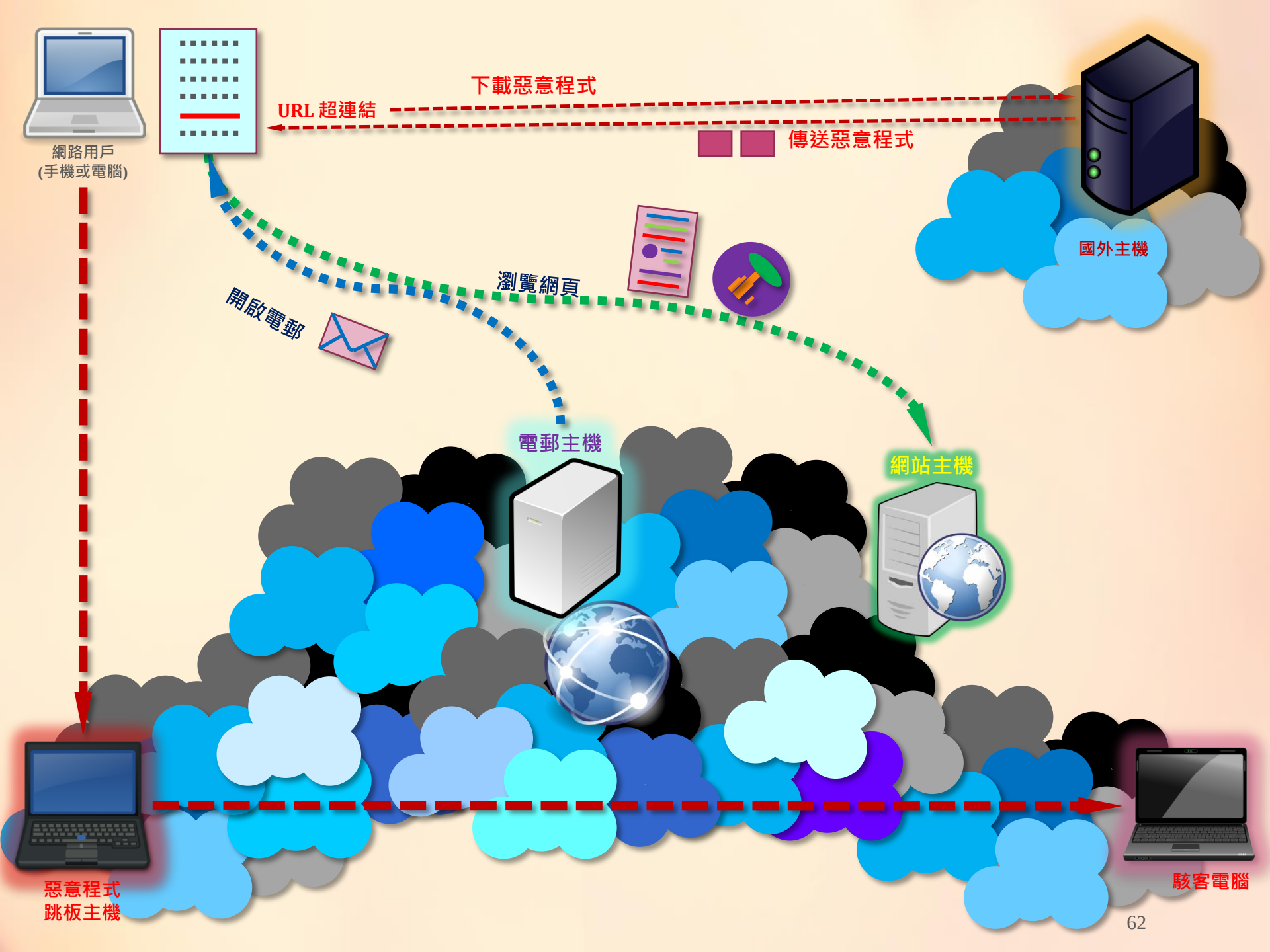
網路社交工程 案例討論

劉得民
Diamond Liu
dmliu99999@hotmail.com

網路社交工程
犯罪模式發展

- 網路社交工程: 加害人經過某種偽裝，取得被害人信任後，進行欺騙的網路攻擊行為。透過電子郵件的方式，稱為「電子郵件社交工程」

- 網路社交工程，可能的攻擊方式
  - 電子郵件夾帶附件檔案(開啟附件)
  - **郵件內容要求點選URL超連接網址(下載檔案)**
  - 郵件隱含可執行程式碼(JavScript)
  - **瀏覽影片網站或是手機瀏覽影片圖片**
  - **從非官方網站下載檔案(偽裝真網站)**

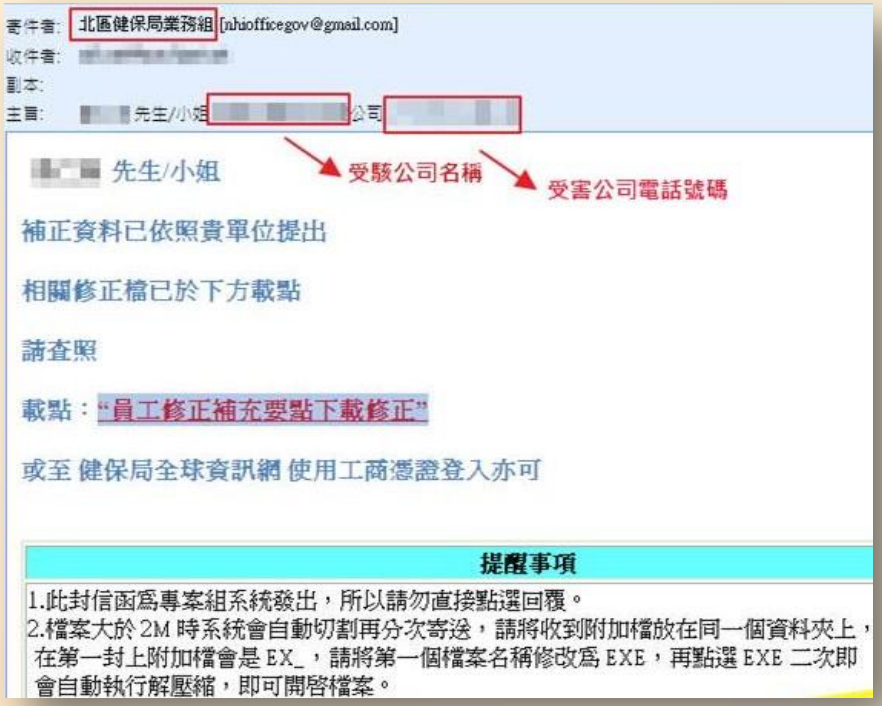

網路用戶
(手機或電腦)
下載惡意程式
URL 超連結
傳送惡意程式
國外主機
瀏覽網頁
開啟電郵
電郵主機
網站主機
惡意程式
跳板主機
駭客電腦

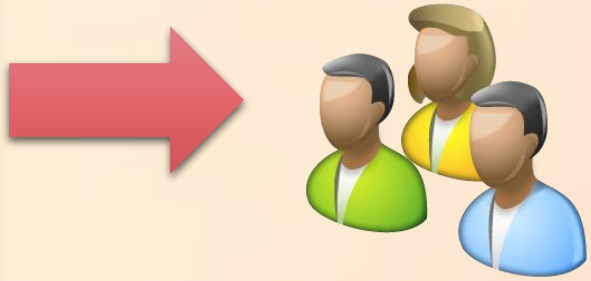
偽冒健保局寄發惡意電子郵件

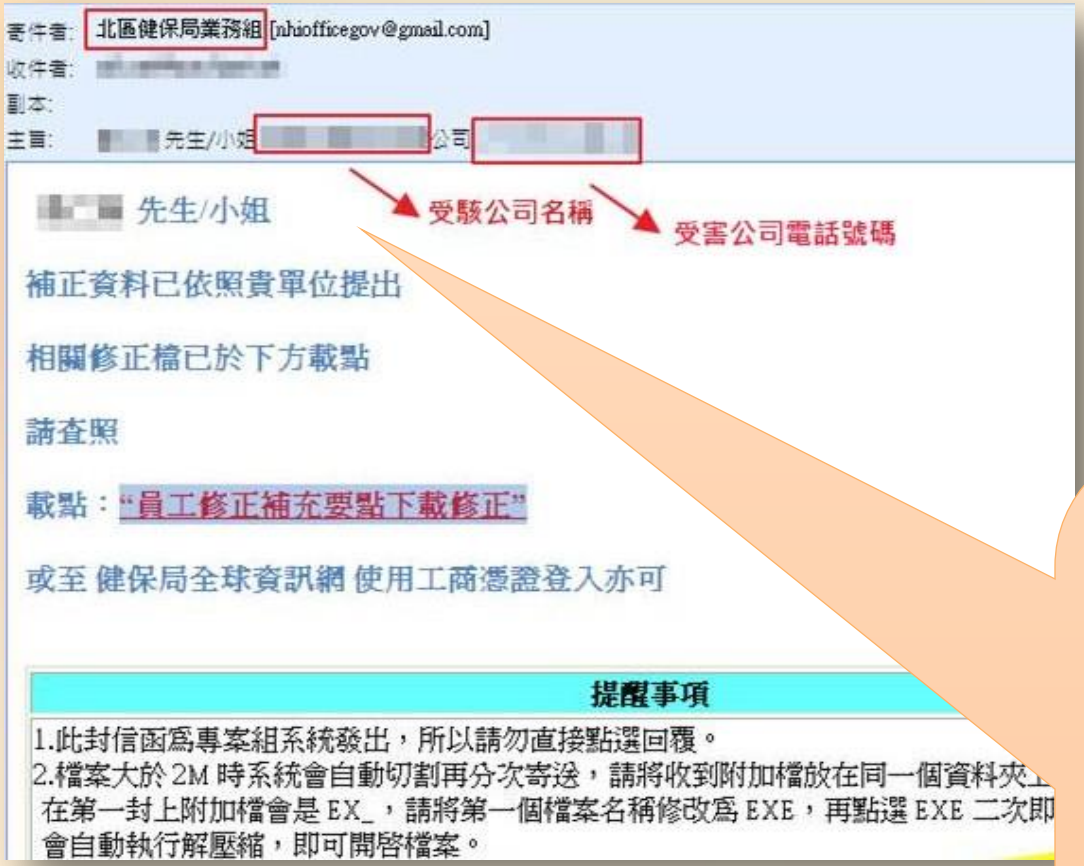
(一)時間：102年4月。

(二)案由：健保局於4月26日發現有不法份子冒用健保局北區業務組名義寄發惡意郵件，被害人電腦中毒後，駭客就能遠端監看、盜取被害人電腦內所有個資。

(三)手法：以APT寄送電子郵件手法散布(鬼網Gh0st)惡意程式。







嫌犯被逮捕後表示當初從網路上搜尋取得或他人指定之中小企業公司會計部門或負責人寄送含惡意程式之電子郵件，由於電子郵件主動出現對方姓名，多半不疑有他點選惡意程式並注入後門程式成功!

http://contagiodump.blogspot.tw/search?updated-min=2010-01-01T00:00:00-05:00&updated-max=2011-01-01

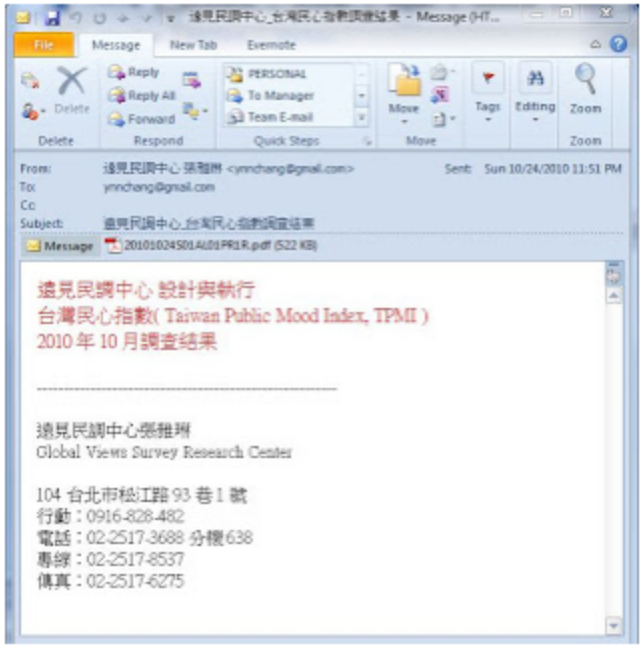
contagio

SUNDAY, OCTOBER 24, 2010

Oct 24 CVE-2010-2883 PDF Vision Poll Center from ynnchang@gmail.com

CVE-2010-2883 Stack-based buffer overflow in CoolType.dll in Adobe Reader and Acrobat 9.3.4 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a PDF document with a long field in a Smart INdependent Glyphlets (SING) table in a TTF font, as exploited in the wild in September 2010. NOTE: some of these details are obtained from third party information

Download 20101024S01AL01PR1R.pdf as a password protected archive (contact me if you need the password)



遠見民調中心 設計與執行
台灣民心指數(Taiwan Public Mood Index, TPMI)
2010 年 10 月調查結果

遠見民調中心張雅琳
Global Views Survey Research Center

104 台北市松江路 93 巷 1 號
行動：0916-828-482
電話：02-2517-3688 分機 638
專線：02-2517-8537
傳真：02-2517-6275

From: 遠見民調中心 張雅琳 [mailto:ynnchang@gmail.com]
Sent: Sunday, October 24, 2010 11:51 PM
To: ynnchang@gmail.com
Subject: 遠見民調中心_台灣民心指數調查結果

遠見民調中心 設計與執行
台灣民心指數(Taiwan Public Mood Index, TPMI)
2010年10月調查結果

遠見民調中心 張雅琳
Global Views Survey Research Center
104 台北市松江路93巷1號
行動：0916-828-482
電話：02-2517-3688分機638
專線：02-2517-8537
傳真：02-2517-6275

Chinese to English translation

From: Vision polling centers Zhang Yalin [mailto: ynnchang@gmail.com]

http://contagiodump.blogspot.tw/search?updated-min=2009-01-01T00:00:00-05:00&updated-max=2010-01-01 contagio

MONDAY, DECEMBER 28, 2009

Dec. 28 CVE-2009-4324 Adobe 0-day "consumer welfare table" from gwsm01@gwsm.gov.tw Mon, 28 Dec 2009 22:08:05 +0800

- CVE-2009-4324 Use-after-free vulnerability in the Doc.media.newPlayer method in Adobe Reader and Acrobat 8.0 through 9.2, and possibly earlier versions, allows remote attackers to execute arbitrary code using ZLib compressed streams, as exploited in the wild in December 2009.

Download CVE-2009-4324 samples (Password protected archives. Use the same password you used on the samples above or contact me for the password)

Download dropped binaries ((Password protected archives. Use the same password you used on the samples above or contact me for the password)

Details: 99年(春節)消費者福利表.pdf - c61c231d93d3bd690dd04b6de7350abb

From: 國防部福利總處
[mailto:gwsm01@gwsm.gov.tw]
Sent: 2009-12-28 8:03 AM
To: xxxxxx
Subject: 檢送國防部福利總處99年(春節)消費者福利表文件乙份,請查照!

詳情登陸國防部福利總處
http://www.gwsm.gov.tw/

服務專線： (02)2392-2377
地址：臺北市信義路一段3號
郵政信箱：台北郵政90036號信箱
網頁維護：綜合資訊組 分機：709

http://contagiodump.blogspot.tw/search?updated-min=2009-01-01T00:00:00-05:00&updated-max=2010-01-01 contagio

Dec. 21 Adobe 0 Day CVE-2009-4324 PDF Attack of the Day SEF preparatory discussions list 陸委會轉寄 海基會、海協會協商代表團預備性磋商名單 from macnews@mac.gov.tw Mon, 21 Dec 2009 20:37:15 +0800

- CVE-2009-4324 Use-after-free vulnerability in the Doc.media.newPlayer method in Adobe Reader and Acrobat 8.0 through 9.2, and possibly earlier versions, allows remote attackers to execute arbitrary code using ZLib compressed streams, as exploited in the wild in December 2009.

Download infected pdf *海基會協商代表團預備性磋商名單.pdf as SEFdiscussionsm.zip*. Password protected, please use the same as on other CVE-2009-4324 files or contact me for the password

Yawn. Here is one more.

From: macnews [mailto:macnews@mac.gov.tw]
Sent: Monday, December 21, 2009 7:37 AM
To: XXXXXXXXXXXX
Subject: 陸委會轉寄 海基會、海協會協商代表團預備性磋商名單

您好，附件為本次協商海基會、海協會代表團預備性磋商名單，提供給您參考，謝謝。

_____ Information from ESET NOD32 Antivirus, version of virus signature database 4707 (20091221) _____The message was checked by ESET NOD32 Antivirus.
http://www.eset.com

Here is a terrible machine translation but it is easy to understand that the mailing is fueled by the recent news, namely, the talks between the ARATS (Association for Relations Across the Taiwan Straits) and SEF (Straits Exchange Foundation) in Taichung tomorrow, December 22, 2009.

案例學習重點

- **瀏覽網頁時，不要點選視窗UAC項目!**
  - 加密勒索病毒會偽裝成為各種網頁需求, 安裝軟體、更新程式、增加字型 ...
  - 因XP已經不再更新/修補系統，所以XP無法從系統這部分抵禦病毒入侵。
- **常見被感染電腦的特徵:**
  - 舊版Java 。
  - 舊版Adobe PDF Reader, 或是 舊版Adobe Flash Player 。
  - 沒有 Windows Update更新
- **至少每2個月，電腦檔案要備份(異地備份, 另外一個地方)。**
- **3-2-1 備份原則：**
  - 3 份 備份檔案 (1份, 存成 3 份)
  - 2 種 不同儲存媒體 (雲端備份, USB備份, 光碟備份, ...)
  - 1 個 不同的存放地點 (辦公室, 家裡,...)

案例學習重點

1. 駭客會假冒政府機構，寄送惡意電子郵件。
2. 自稱政府機構的郵件，不一定是安全乾淨的。
3. 2017-2022年, 預估會有更多的加密勒索病毒(手機)
4. Wifi 基地台有漏洞(WPA-2)導致手機通訊資料外洩
5. 假冒無線基地台，騙取無辜使用者的資料
6. 網路購物要非常小心，自稱銀行人員或網站客服，請特別小心。

Q&A

Diamond 資訊安全規則

1.絕對不在自己的電腦上，做任何危險的電腦操作。

2.當防毒軟體表示該檔案有「毒」，它一定是惡意程式。而防毒軟體表示沒有「毒」的時候，只代表沒有掃到病毒，並不表示該檔案是乾淨的無毒檔案！

3.做好資訊安全工作，不用花大錢，只要養成電腦網路的好習慣！

- Name : Diamond Liu (劉得民) 0932-212-913, 0985-604-145
- Email : dmliu99999@hotmail.com

God is not on the side of the big battalions, but on the side of those who shoot best.

Voltaire, French author, wit, and philosopher