



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



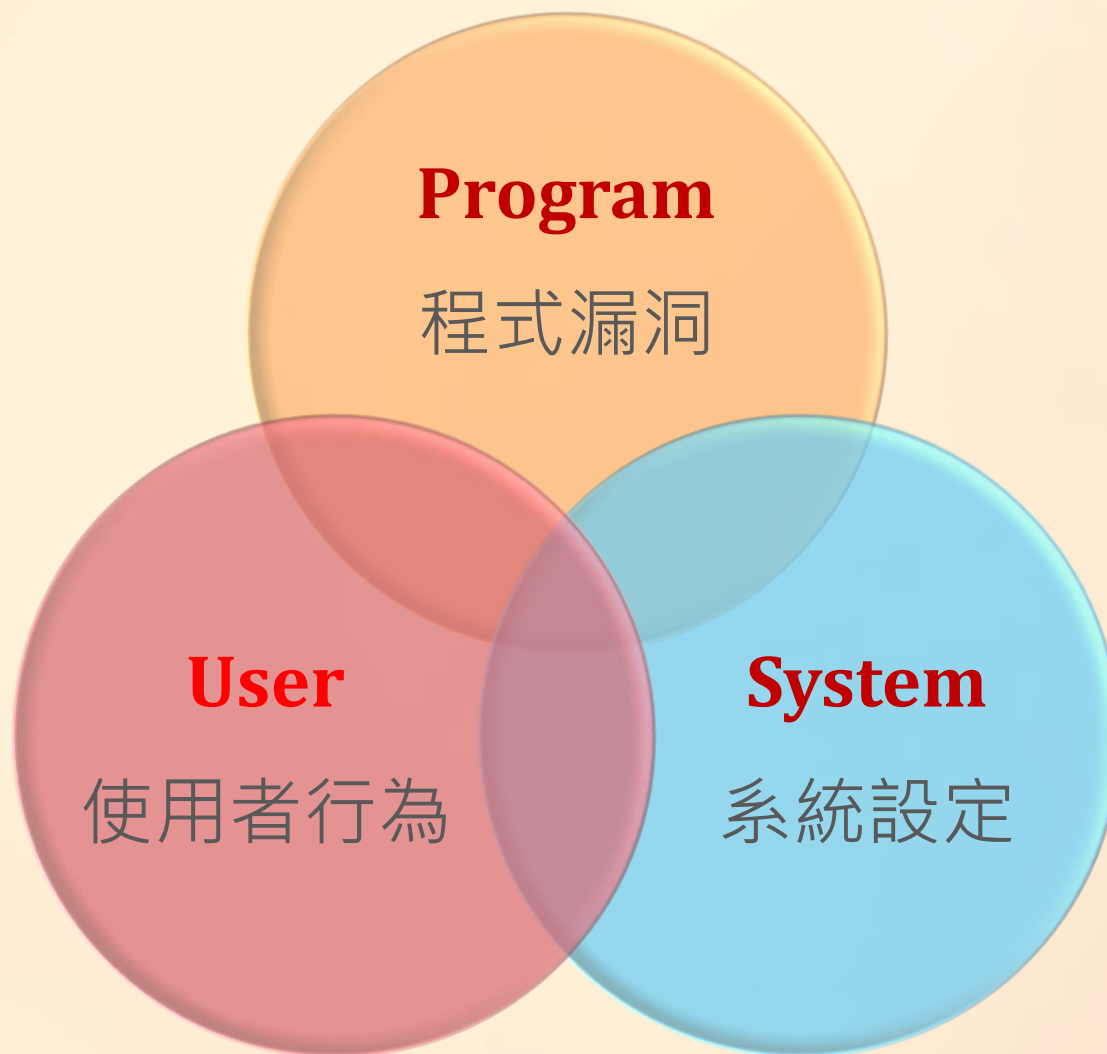
資訊安全之基本說明

劉得民

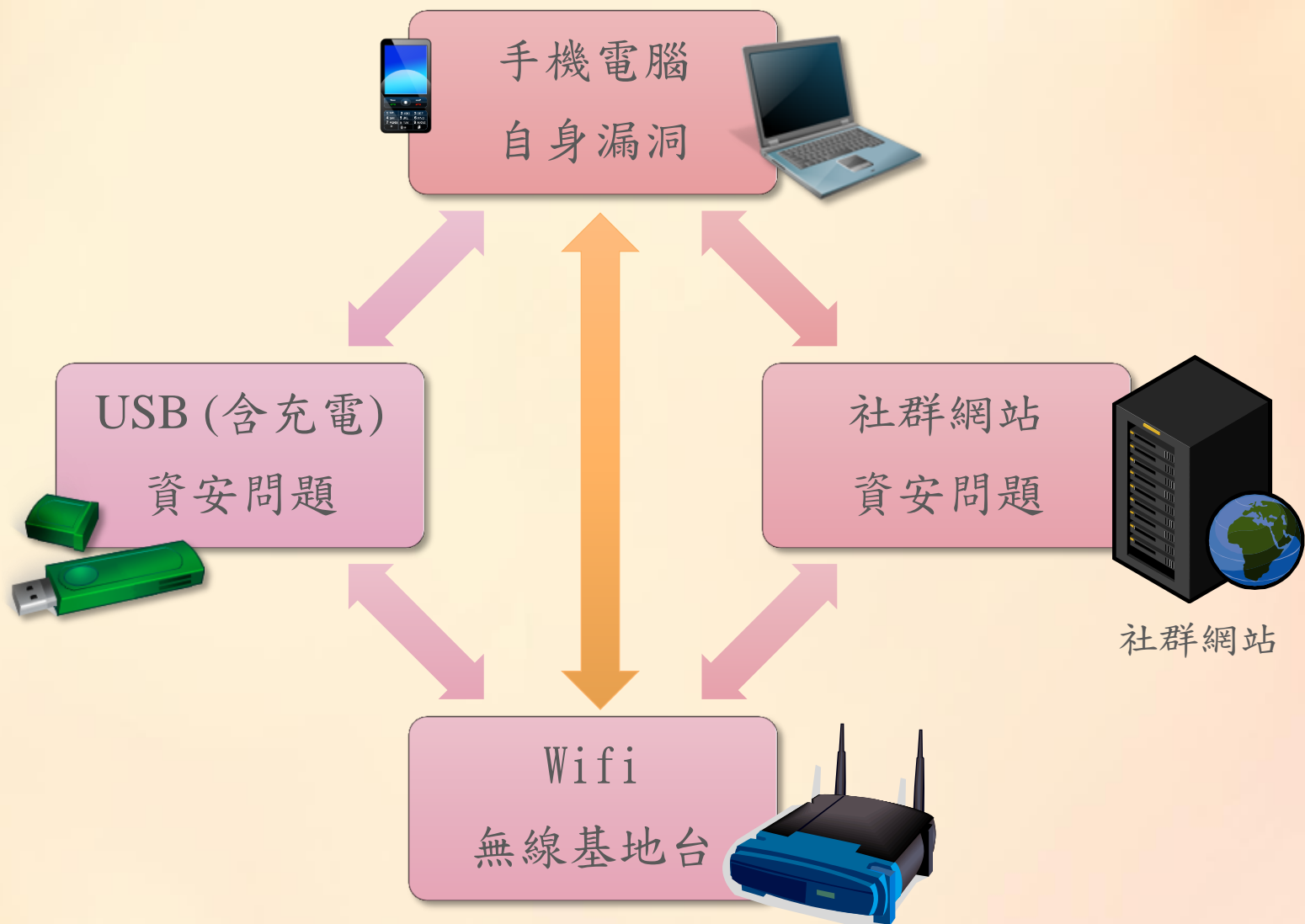
Diamond Liu

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





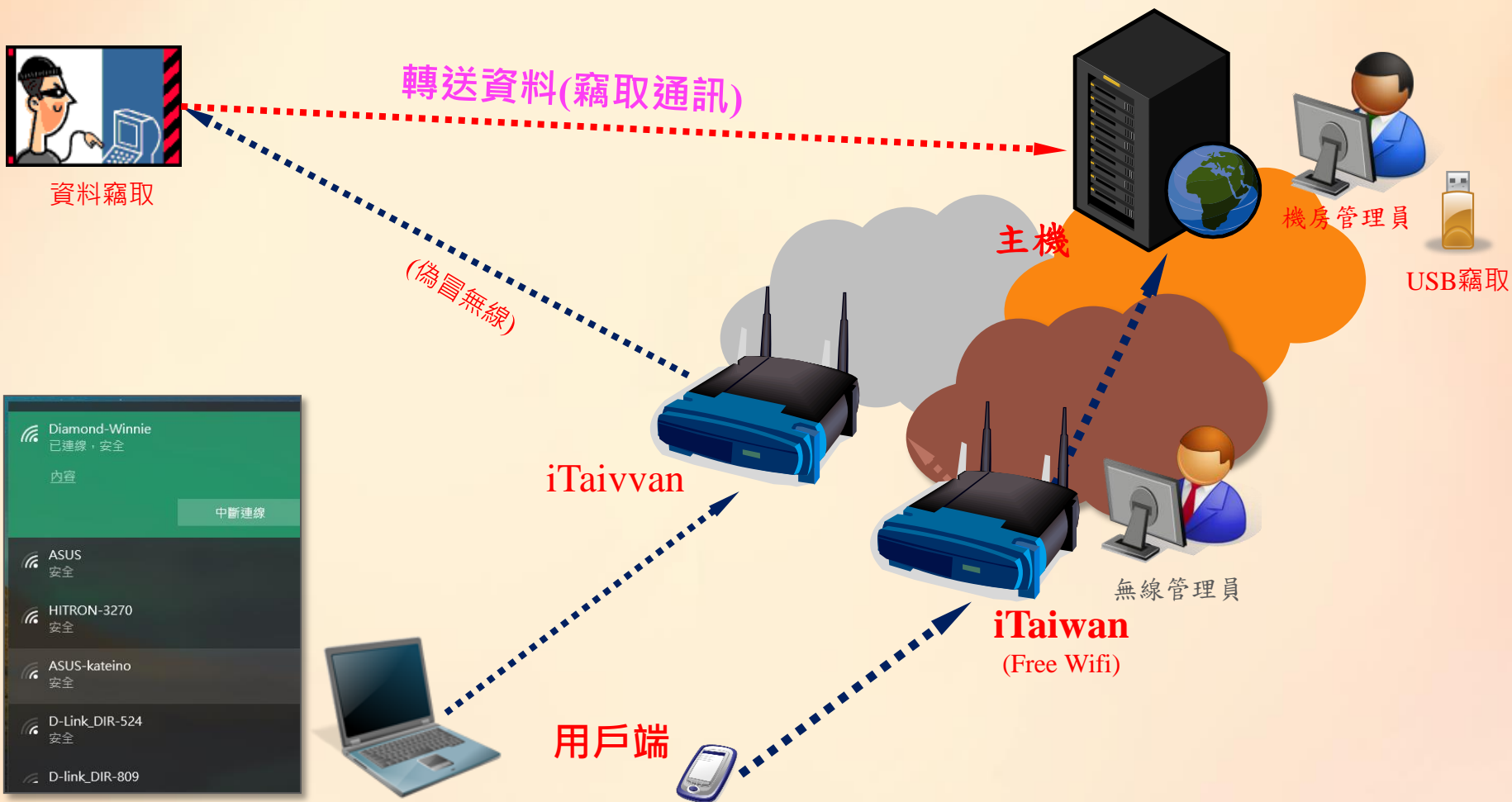
無線存取點欺騙與防範

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「篡改並重送加密交換訊息」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/HT208222>WPA2**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換階段, 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.itn.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**



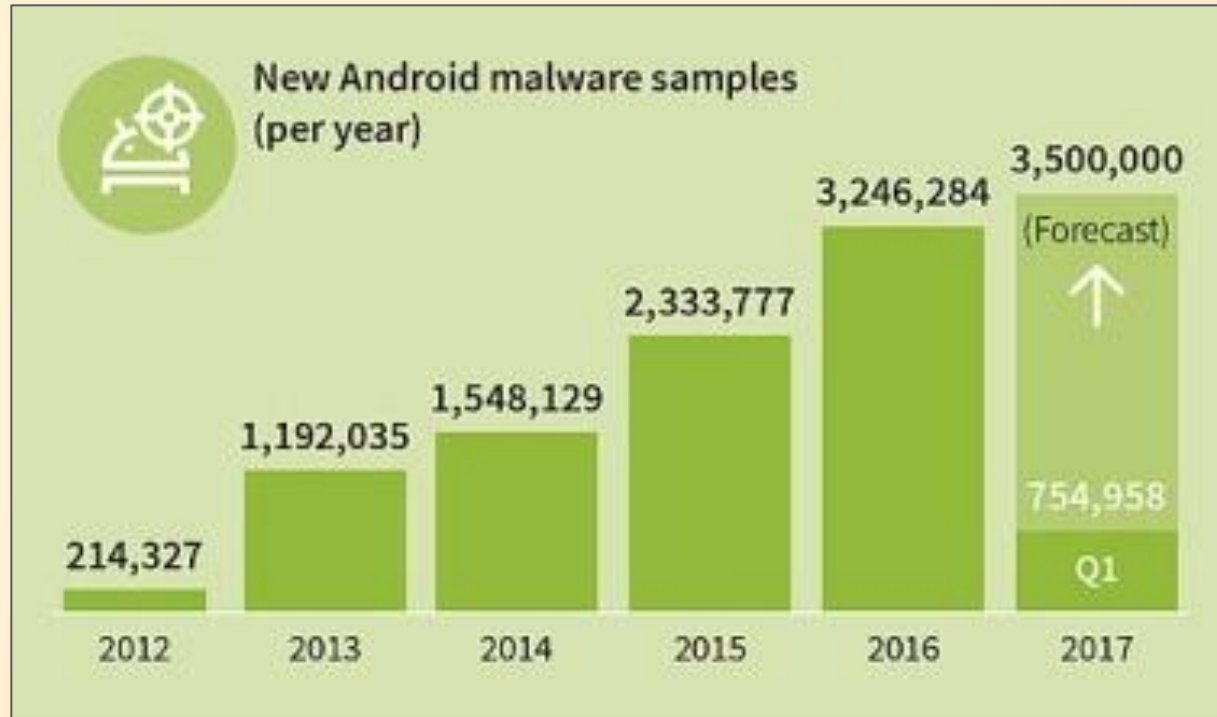
手機安全與個資防護

劉得民

Diamond Liu

dmliu99999@hotmail.com

Android手機，最容易被攻擊



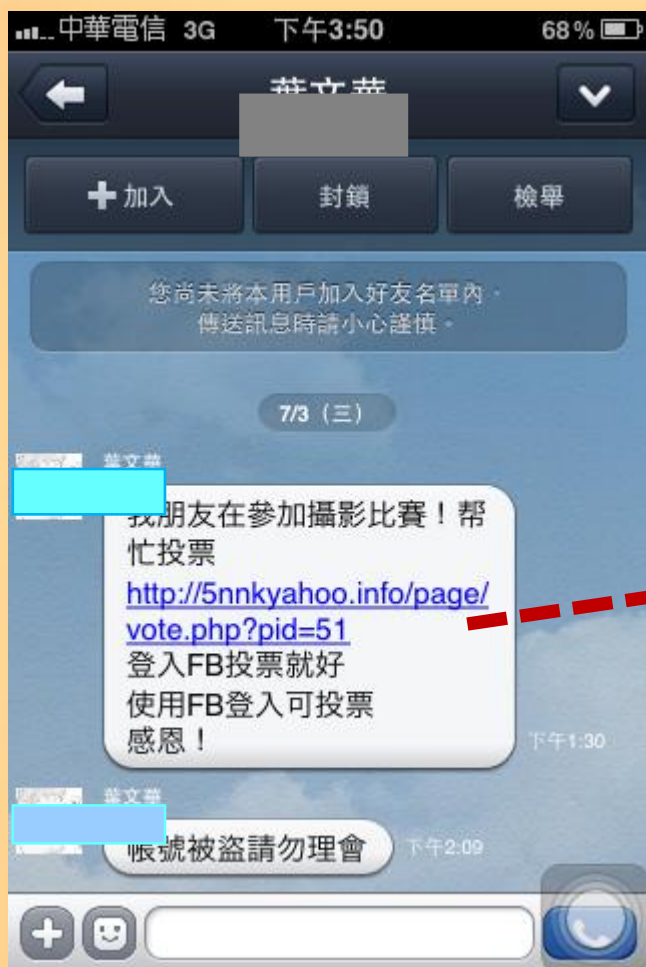
舊型Android系統，容易被駭

- 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...

AIOMP3

Search Mp3

玩命關頭7片尾曲、see You Again Free Mp3 Download

Mobile Content Download

4:00 Duration 陳傑瑞 - See You Again 中文版演唱【玩命關頭 7 片尾曲】 陳傑瑞 - 再見 original by Wiz Khalifa (JERIC CHINESE COVER)

▶ Play Mp3 Download

4:01 Duration Wiz Khalifa - See You Again ft. Charlie Puth 《玩命關頭7 Furious 7》片尾曲 「See You Again 來日再見」 中英文字幕

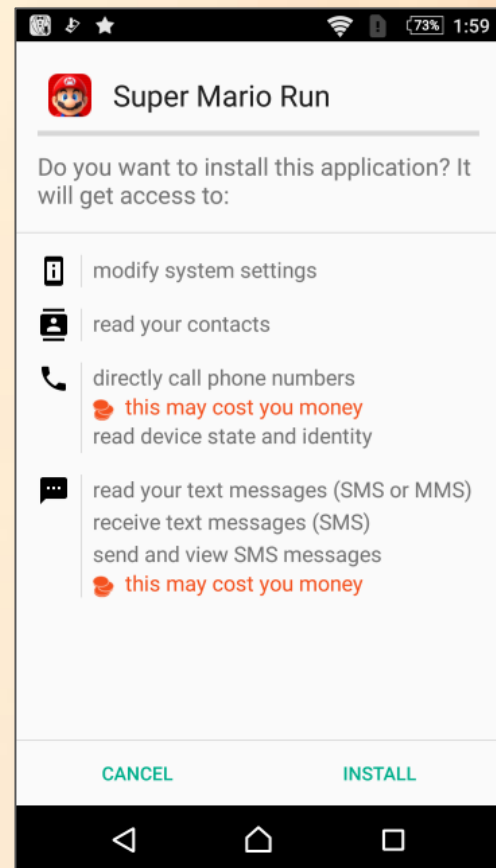
▶ Play Mp3 Download

⚠ 這種類型的檔案可能會損害您的裝置，您要保留 14659798513256.apk 嗎？

取消 確定

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



Photo Editor – InstaMag

需要下列項目的存取權



相片/多媒體/檔案



Google Play

接受



PIP Camera Effect

需要下列項目的存取權



相片/多媒體/檔案



相機



Wi-Fi 連線資訊



Google Play

接受


安裝手機App軟體的權限問題



拼立得 - 讓你的照片一秒變海報



需要下列項目的存取權



 身分識別 

 位置 

 相片/多媒體/檔案 

 相機 

 Wi-Fi 連線資訊 

 裝置 ID 和通話資訊 

Google Play

接受





PIP Collage Maker



需要下列項目的存取權

 身分識別 

 相片/多媒體/檔案 

 相機 

 Wi-Fi 連線資訊 

 裝置 ID 和通話資訊 

Google Play

接受

安裝手機App軟體的權限問題



小影:最強大影片剪輯/
幻燈片免費程式 自拍/貼
圖/字幕/音樂

需要下列項目的存取權

💰 應用程式內購

🕒 裝置和應用程式紀錄

📍 位置

🖼️ 相片/多媒體/檔案

📷 相機

🎤 麥克風

📶 Wi-Fi 連線資訊

📱 裝置 ID 和通話資訊

Google Play

接受

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

NOT YOUR LANGUAGE? USE <https://translate.google.com>

What happened to your files ?
All of your files were protected by a strong encryption with RSA4096
More information about the encryption keys using RSA4096 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

How did this happen ?
!!! Specially for your PC was generated personal RSA4096 Key , both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

What do I do ?
So , there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW! , and restore your data easy way
If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment

Your personal ID: **EAE9A8441F84**

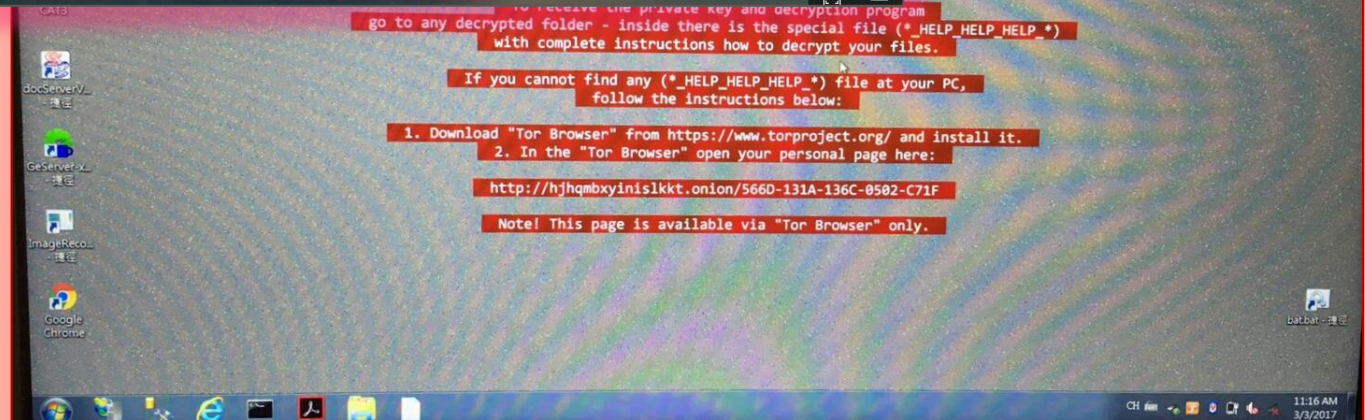
For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

- 1 - <http://6kiujogtkmofnyaq.onion.to>
- 2 - <http://6kiujogtkmofnyaq.onion.cab>
- 3 - <http://6kiujogtkmofnyaq.onion.city>

If for some reasons the addresses are not available, follow these steps:

- 1 - Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
- 2 - After a successful installation, run the browser
- 3 - Type in the address bar - <http://6kiujogtkmofnyaq.onion>
- 4 - Follow the instructions on the site

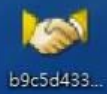
Be sure to copy your personal ID and the instruction link to your notepad not to lose them.



Windows Update 選擇要安裝的更新

Windows 7 (5)

- 2017-05 適用於 Windows 7 的更新
- KB2840631 : x64 系統更新
- KB2987107 : Internet Explorer 11 更新
- KB890830 : Windows 7 安全更新
- May, 2017 Security and Quality Rollup



Oops, your files have been encrypted!

Payment will be required to decrypt your files.

5/13/2017 16:47:55
Time Left: 00:00:00

Your files will be encrypted.

5/13/2017 16:47:55
Time Left: 00:00:00

Send \$600 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Check Payment Decrypt

Load PerfMon Counters 已經停止運作

Windows 可以在下次您上線時，線上檢查是否有問題的解決方案。

- 稍後線上檢查是否有解決方案並關閉程式
- 關閉程式

檢視問題詳細資料



WS/199/161

Oops, 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:

1Mz7153HMuxXTuR2R1t78mCSdzaAtNbBNX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsnith123456@posteo.net. Your personal installation key:

PqvrHJ-BCvRyd-iQu7E5-rJbEJZ-fBXAKX-tP3tWS-1t2FAd-M7T8jE-3Gqasx-A6BchH

If you already purchased your key, please enter it below.
Key: _





Oops, 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 \$388 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsnith123456@posteo.net. Your personal installation key:

NY56i2-2z6xzu-B8JgcF-pq2HDz-gM9Ck5-wnDINX-K76pXb-5jY1nM-JUWxXu-2CSRNk

If you already purchased your key, please enter it below.
Key:



Ooops, your files have been encrypted!

Chinese (traditions)

我的電腦出了什麼問題？

您的一些重要文件被我加密保存了。照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。

有沒有恢復這些文檔的方法？

當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。但這是收費的，也不能無限期的推遲。請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。但想要恢復全部文檔，需要付款點費用。是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。最好3天之內付款費用，過了三天費用就會翻倍。還有，一個禮拜之內未付款，將會永遠恢復不了。對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪

Payment will be raised on

1/4/1970 08:00:00

Time Left

00:00:00:00

Your files will be lost on

1/8/1970 08:00:00

Time Left

00:00:00:00

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$600 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

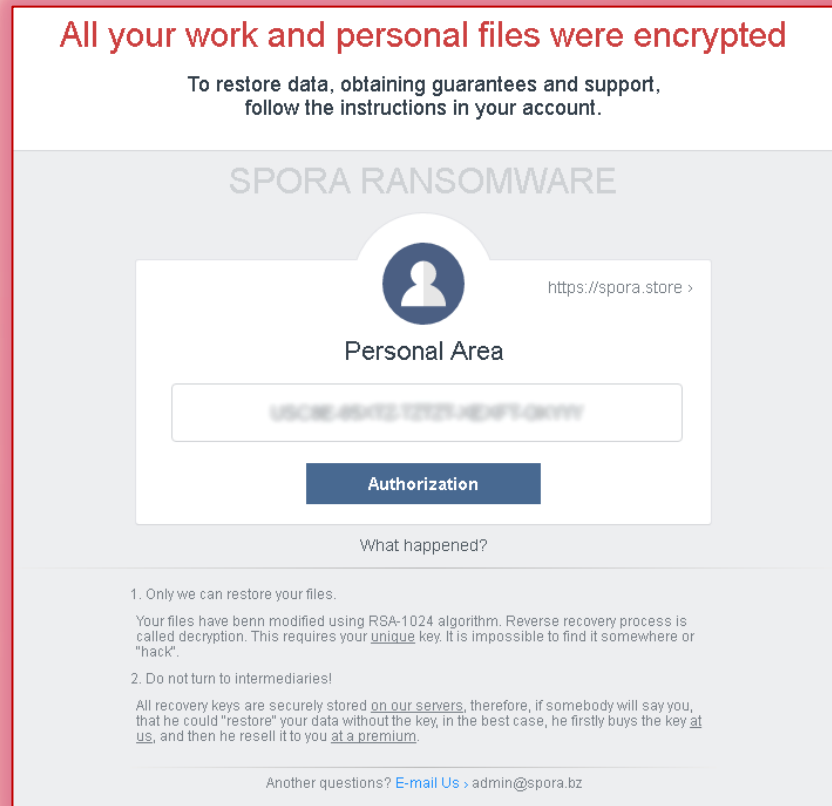
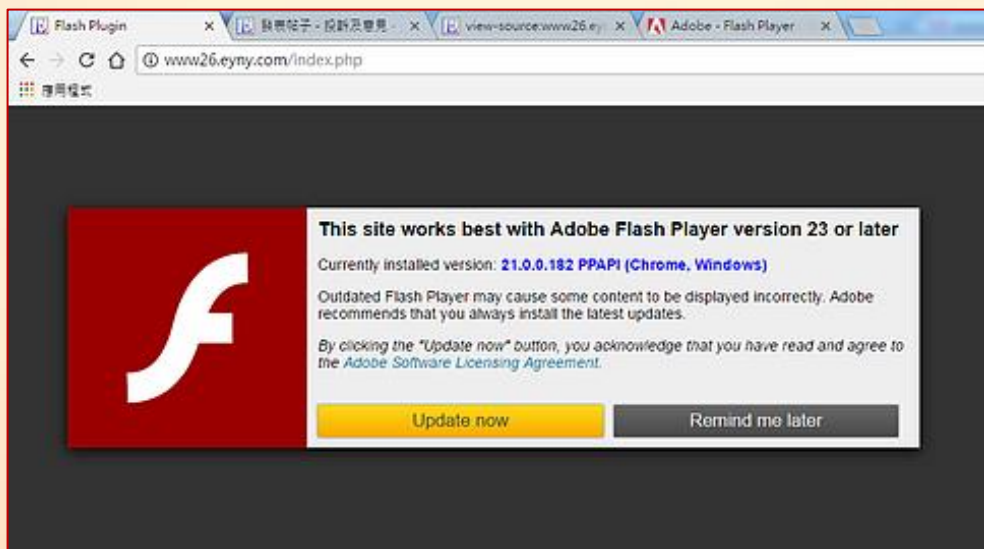
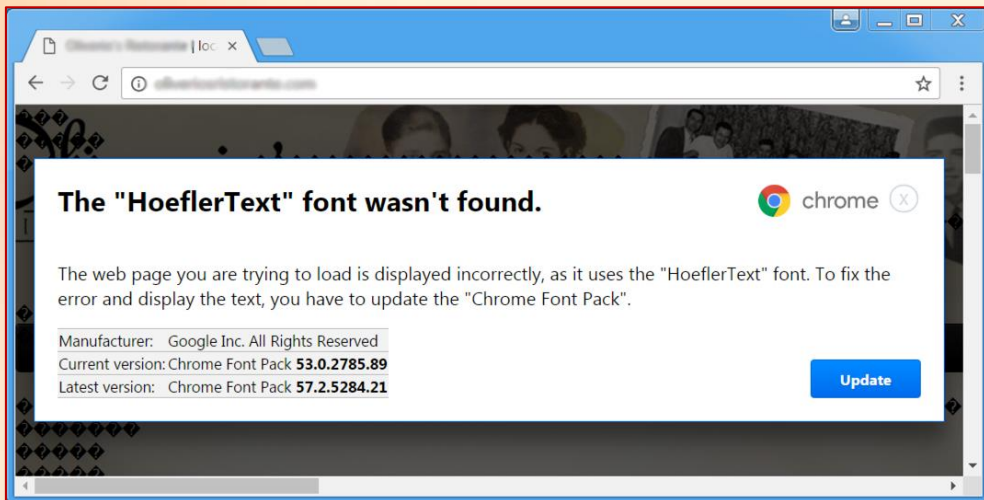
Decrypt



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

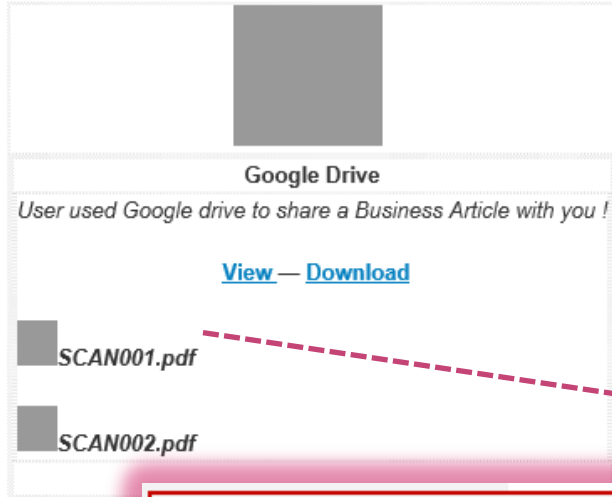
Re: Payment Report ↑ ↓ ×

寄件者: **Alipay** (merchant@alipay.com) Microsoft SmartScreen 將這封郵件歸類為垃圾郵件。

寄件日期: 2016年5月16日 上午 11:31:23

收件者: dmliu99999@hotmail.com

Microsoft SmartScreen 將此郵件標記為垃圾郵件，並於十天後刪除。
這封是安全的郵件！ | [我不確定](#) · [讓我查看](#)



電子郵件，金融對帳單，提醒瀏覽(下載)
(這是惡意程式)



2016_Virus_病毒_SCAN001pdf.scr 不常被下載，而且可能會危害您的電腦。

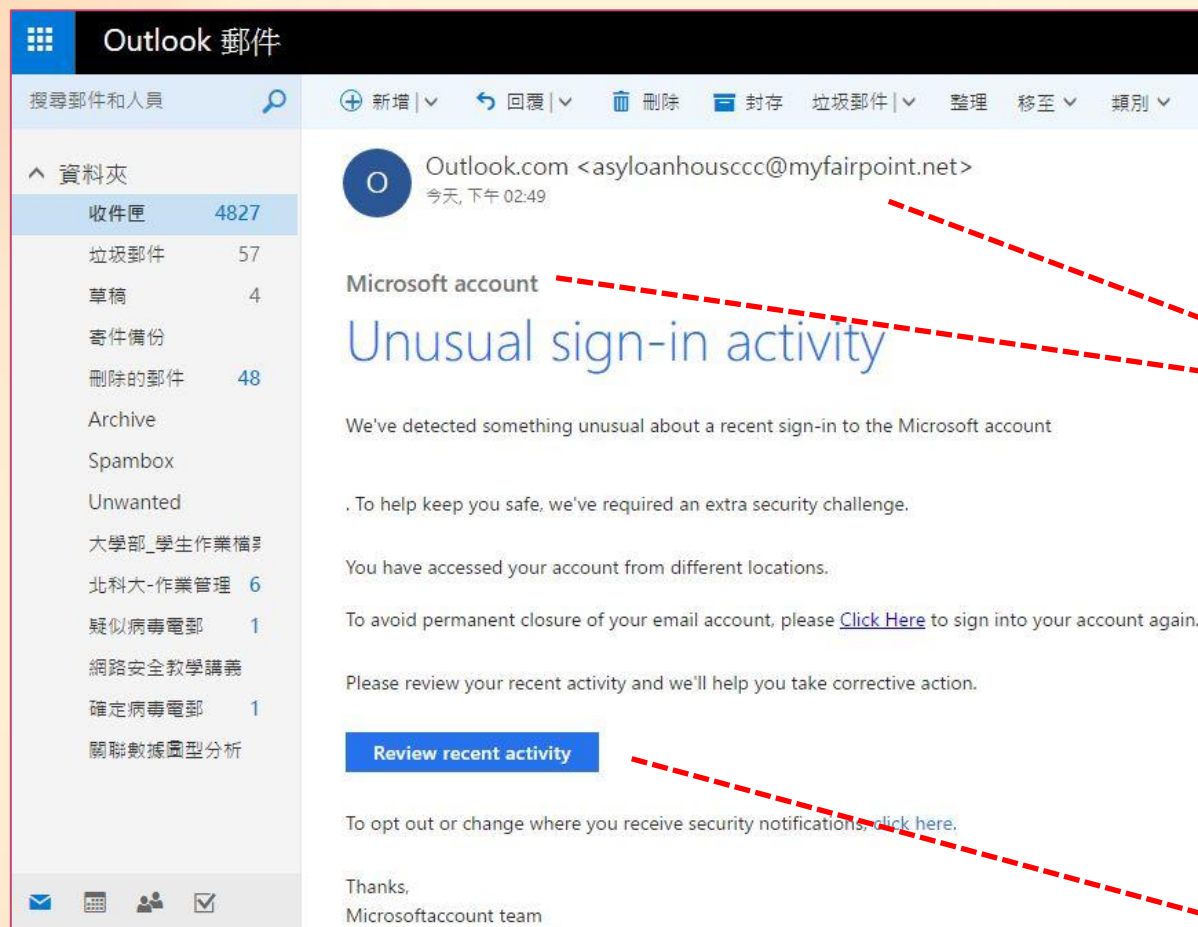
刪除

執行

檢視下載



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



您即將前往詐騙網站

攻擊者可能會試圖透過 **ilmiotimbro.be** 誘使您做一些危險的事，例如安裝軟體或提供個人資訊 (包括密碼、電話號碼或信用卡資料)。

自動向 Google 回報疑似安全性事件的詳細資料。隱私權政策

隱藏詳細資訊

Google 安全瀏覽功能最近在 **ilmiotimbro.be** 上偵測到網路詐騙行為。詐騙者利用這個網站，藉此騙取你的資訊。瞭解詳情

您可以回報偵測問題。或者在您瞭解安全性風險後，仍然可以前往這個不安全的網站。

ilmiotimbro.be/lib/SweetTooth/pest/examples/msn/Microsoft%20account.htm

Sign in to verify your account

Use your Microsoft account.
[What's this?](#)

Email or phone

Password

Keep me signed in

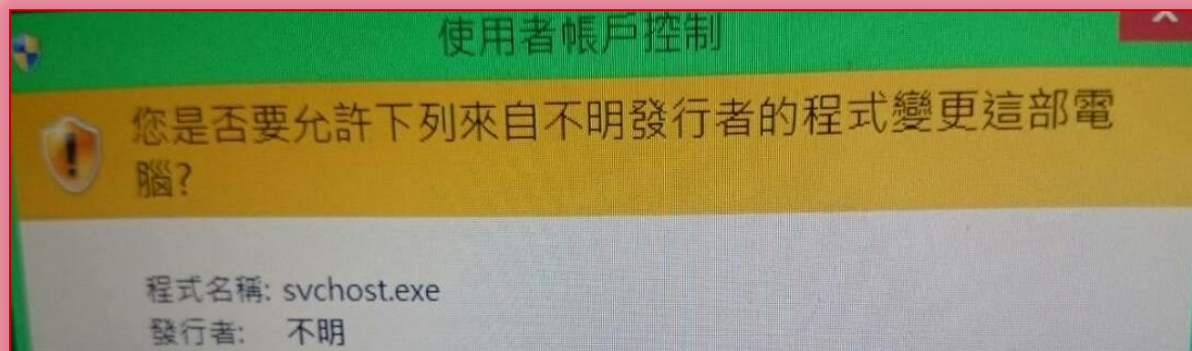
Sign in

[Forgot my password](#)

[Sign in with a single-use code](#)

Microsoft

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.chinatrust.com.tw | 金融銀行 |
| • TW.BID.YAHOO.COM | • TW.BID.YAHOO.COM | 拍賣網站 |
| • www.landbank.com.tw | • www.landbank.com.tw | 金融銀行 |
| • www.china-airline.com.tw | • www.china-airline.com.tw | 航空公司 |
| • www.google.com.tw | • www.google.com.tw | 網路服務 |
| • www.outlook.com | • www.Outlook.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

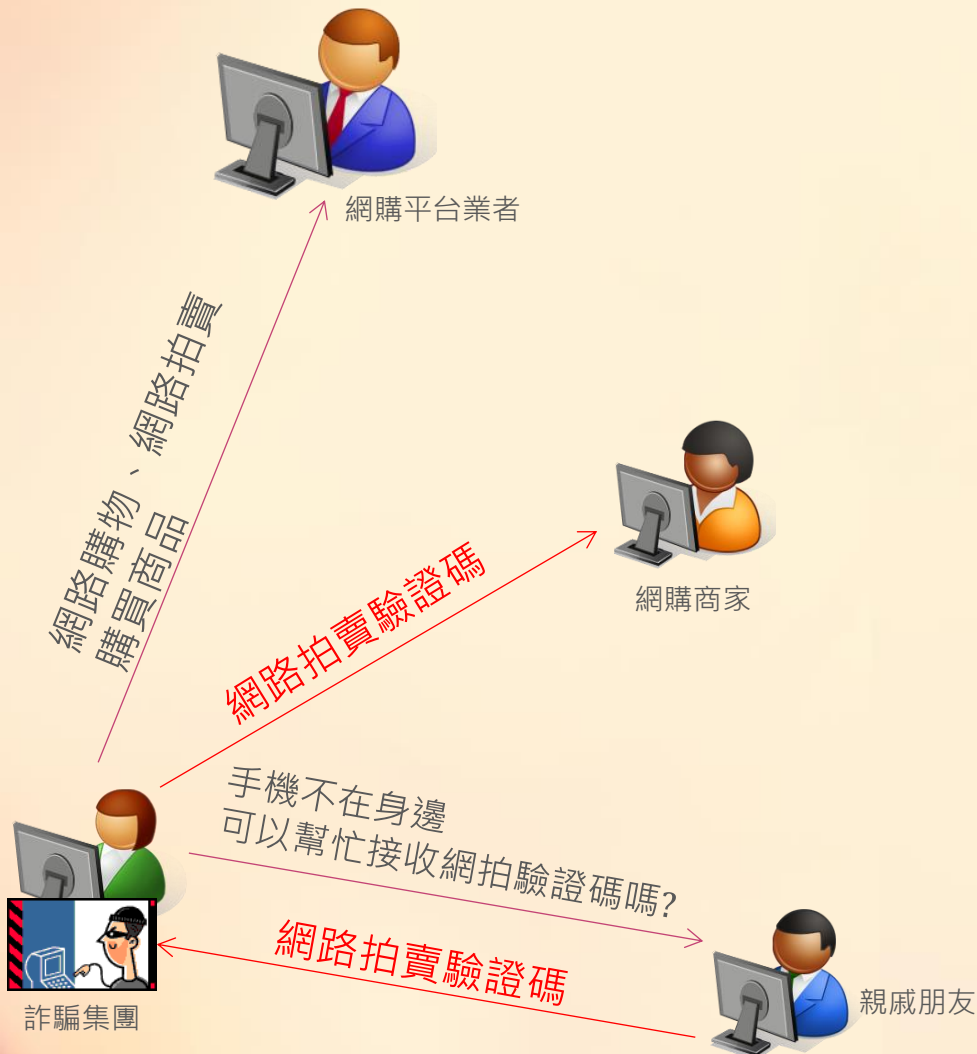
社群網站資料防護的漏洞

- 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



盜用臉書帳號密碼

假冒臉書身份

請好友代收
網購驗證碼

臉書-Line之詐騙分析



高風險賣場排名

第一名：蝦皮拍賣	【被害59件】
第二名：露天拍賣	【被害42件】
第三名：SHOPPING99	【被害38件】
第四名：HITO本舖	【被害29件】
第五名：奇摩拍賣	【被害12件】
第五名：巴黎草莓國民時尚美妝	【被害10件】

統計日期：105年12月19日至105年12月25日



1. 上述數據包含「假網拍」（匯款後未收到物品或商品顯不相符）☹️及「ATM解除分期付款」（假冒賣場客服來電稱訂單錯誤，要求操作ATM解除設定詐騙）☹️。
2. 網購應選擇信譽良好且有完善資安防護的優良商家，切勿透過FACEBOOK、LINE等方式私下聯繫匯款，若賣場或購物平臺無法保障您的個資，您購買前應三思而後行。

>>

0

>>

1

>>

2

>>

3

>>

4

>>

臉書-Line之詐騙分析

民眾通報高風險賣場（平臺）

賣場名稱	被害件數
EZ訂（電影票券）、蝦皮拍賣	被害21件
露天拍賣	被害16件
可樂旅遊	被害13件
讀冊生活	被害10件



統計區間：106年5月15日至5月21日

臉書-Line之詐騙分析

民眾通報高風險賣場（平臺）

一訂OK網

被害38件

雄獅旅行社、蝦皮拍賣

被害26件

露天拍賣

被害15件

JOYCE-SHOP

被害11件

旋轉拍賣

被害10件

統計日期：106年6月5日至106年6月11日

誤設成分期付款

將扣款12次

要操作ATM解除

就是

騙



快透過以下管道，取得最新防詐資訊

165官網：搜尋「警政署165反詐騙」

165臉書：搜尋「165反詐騙宣導」，有刑事Bear才是官方版

165 APP：iTunes Store或Google Play搜尋「165反詐騙」

165 LINE：@tw165



臉書-Line之詐騙分析



EZ訂 (電影票券)

被害45件

饗食天堂

被害40件

雄獅旅行社

被害29件

露天拍賣

被害15件

Viva美好購物網

被害14件

統計日期：106年6月19日至106年6月25日

1. 誤設成分期付款、VIP、團購、多筆訂單
2. 將重複扣款
3. 要操作ATM解除
4. 要加LINE聯繫

騙

※近期詐騙集團多鎖定「旅行社」、「電影票券」及「餐飲業」作為假冒對象，請提高警覺。

※透過臉書FB、LINE購物詐騙多（如演唱會門票），應選擇商譽良好及有完整客服的商家，較有保障。

165官網：搜尋「警政署165反詐騙」165APP：iTunes Store或Google Play搜尋「165反詐騙」

165 LINE：@tw165

165臉書：搜尋「165反詐騙宣導」，有刑事Bear才是官方版

臉書-Line之詐騙分析

民眾通報高風險賣場（解除分期付款）

賣場名稱	被害件數
OB嚴選	21
首爾妹	20
DEVILCASE	17
明洞國際	15
威秀影城	13
美麗華影城	13
雄獅旅行社	12

統計日期
106年11月13日至106年11月19日

ATM解除分期詐騙 2階段轉接手法

1線 假冒電商業者客服



謊稱民眾
訂單或會
員等級設
定錯誤，
造成重覆
扣款。

要求民眾
唸出提款
卡或信用
卡上的客
服電話，
表示會協
助聯絡處
理。



2線 假冒銀行或郵局客服

竄改來電
顯示號碼
為銀行電
話，要求
民眾至AT
M操作。

先提供錯
誤帳號讓
民眾操作
失敗，解
除民眾防
備心。

要求民眾
輸入訂單
號碼跟解
除代碼(其
實是匯出
帳號跟匯
出金額)，
誘使民眾
匯款。

謊稱民眾
操作不當
造成帳戶
異常，需
把戶內餘
額領出，
以ATM現
金存款方
式存入指
定「安全
帳戶」。

165 反詐騙 APP



iOS 系統 Android 系統

165 反詐騙官網



165 反詐騙宣導海報



165 反詐騙宣導 LINE



透過臉書/Line的低價購物

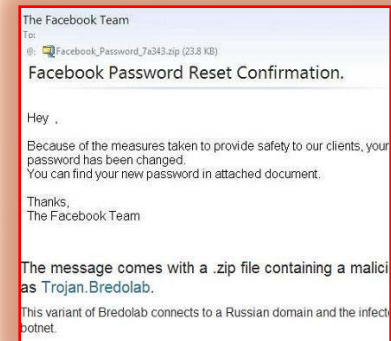


Facebook 親友電郵遭駭 真實案例

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, 該電子郵件內容(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。



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, 誘騙郵件內容(中英文皆)設定Facebook帳號。

若是使用者若想要知道這件郵件中的附件檔案, 來誘使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



目標對象-2

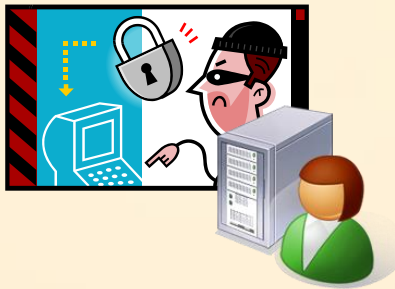
進行電郵
社交工程



社群網站
FaceBook



種菜養魚
存取硬碟資料

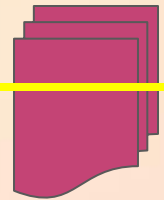


目標對象-1

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

授權請求

「開心農場」需要你的授權以執行以下事項：



允許此程式取得我的基本資料

包括姓名、個人檔案、性別、人際網路、用戶 ID、好友清單，和其他設定為「公開」的資訊



發送電郵給我

「開心農場」可以直接寄電子郵件給我在 yuling_0825@hotmail.com 的信箱 · [更改](#)



以我的名義發表

這個應用程式可以用我的名義貼文，包括你的最高分數及更多。



開心農場

在你繼續下一步安裝此應用程式時，即表示你同意開心農場的[服務條款與隱私權政策](#) · [舉發應用程式](#)

Logged in as Yuling Chou · [登出](#)

同意

不允許

“开心水”

14:11, Q

联系我们



历时2个月
 游戏地址:
 简介: 这
 知而神奇
 接下来还有
 吸引力的新剧:

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

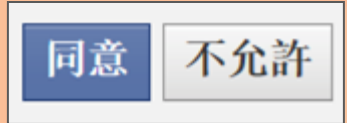
合肥智明星通软件科技有限公司
 客服邮箱: kfzp@elex-tech.com
 商务邮箱: biz@elex-tech.com
 公司邮箱: hf-hr@elex-tech.com
 公司电话: 0551-4663787
 公司地址: 合肥市高新区动漫和服务外包产业发展基地B3楼四层

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social 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



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)

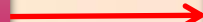
蒐集臉書資料

分析臉書喜好

臉書好友活動

製作惡意程式

寄送偽裝電郵





網路社交工程 案例討論

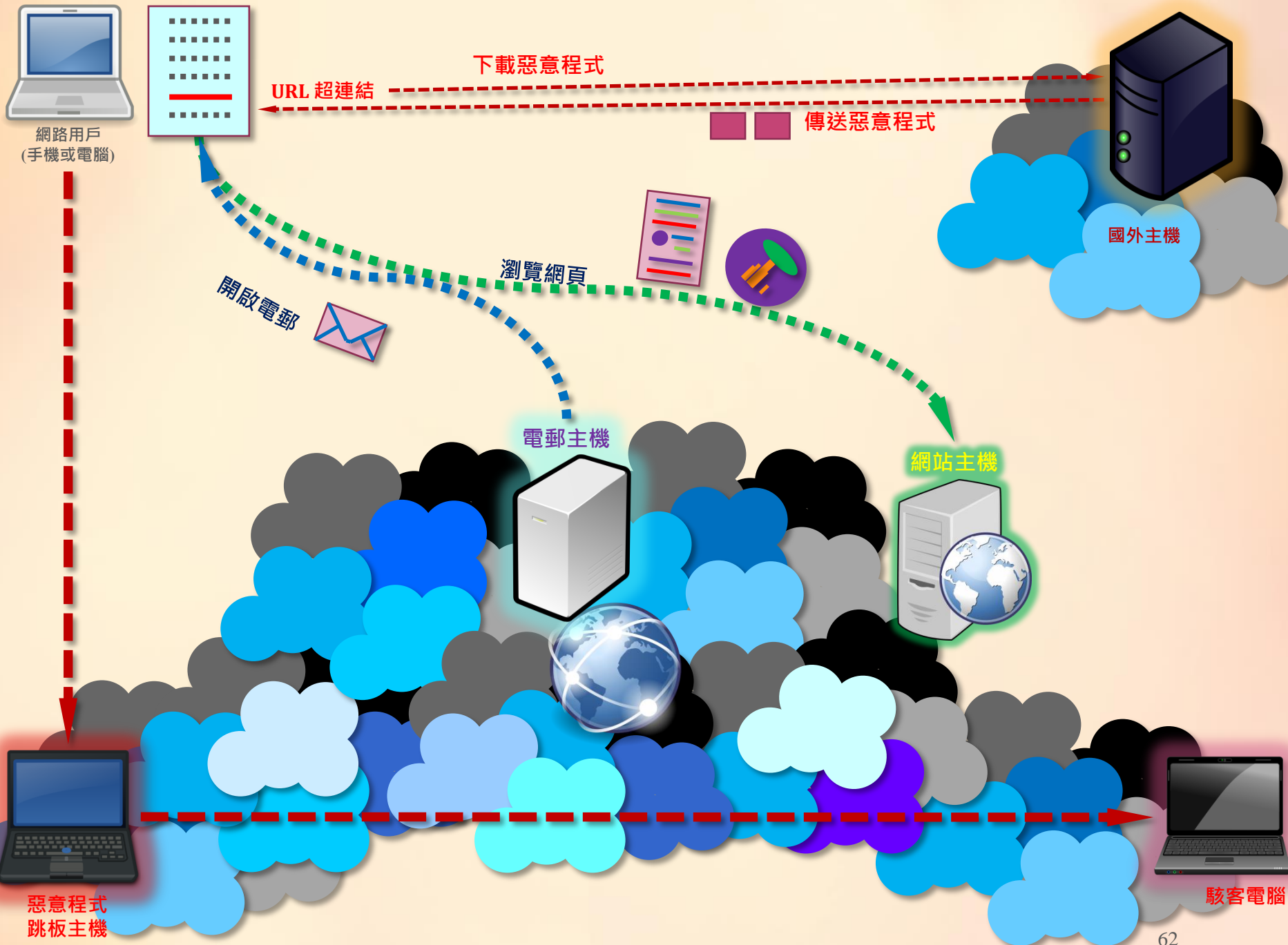
劉得民

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)**
 - 郵件隱含可執程式碼(Javascript)
 - **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)**

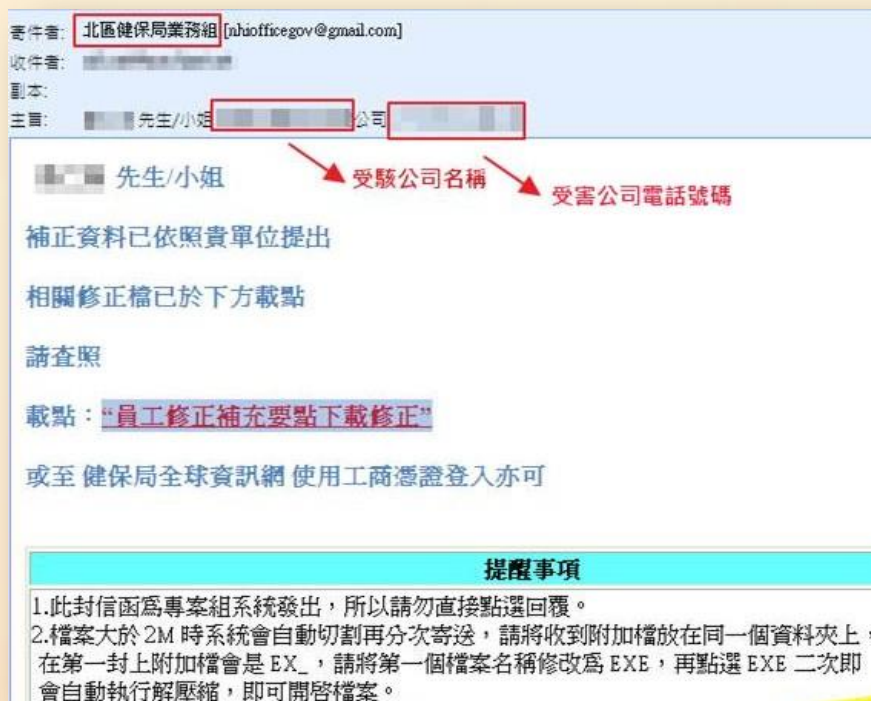


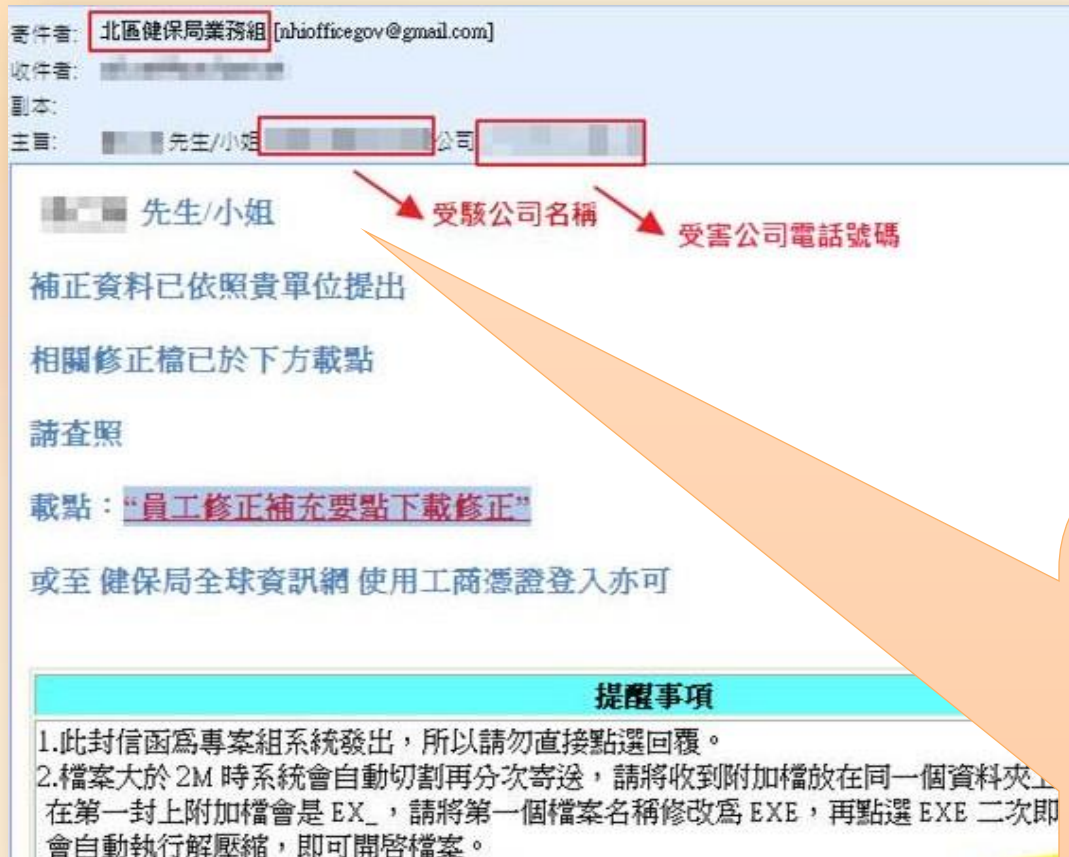
偽冒健保局寄發惡意電子郵件

(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！

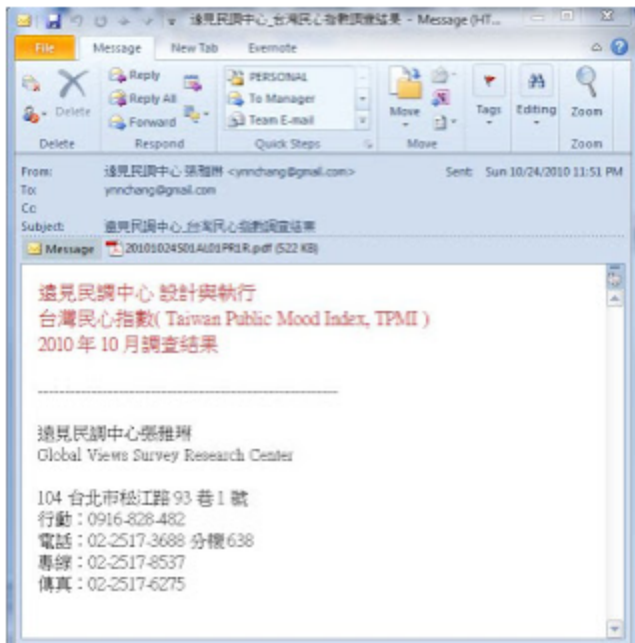
SUNDAY, OCTOBER 24, 2010

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)



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]

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

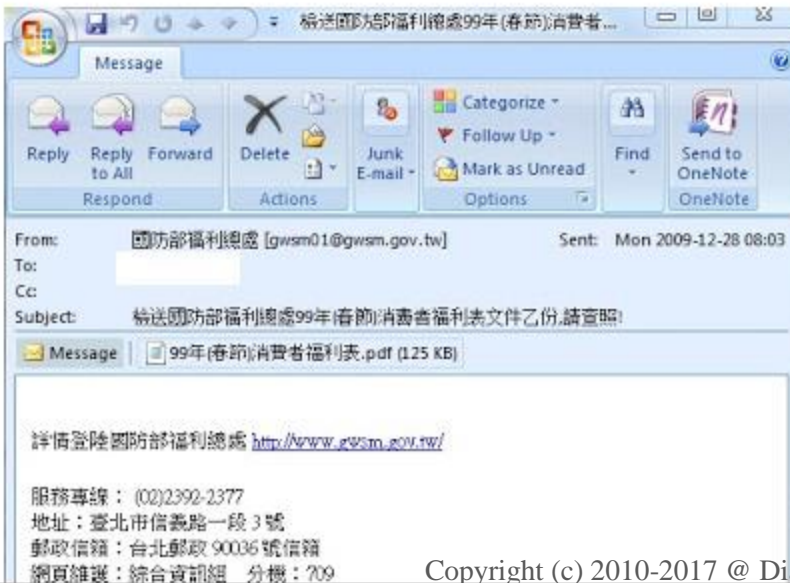
- CVE-2009-4324 Use-after-free vulnerability in the Doc.media.newPlayer method in Adobe Reader and Acrobat 8.0 through 9.2, and possibly earlier versions, allows remote attackers to execute arbitrary code using ZLib compressed streams, as exploited in the wild in December 2009.



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

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: XXXXXXXXXXXXX
 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