2017-網路資訊安全

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

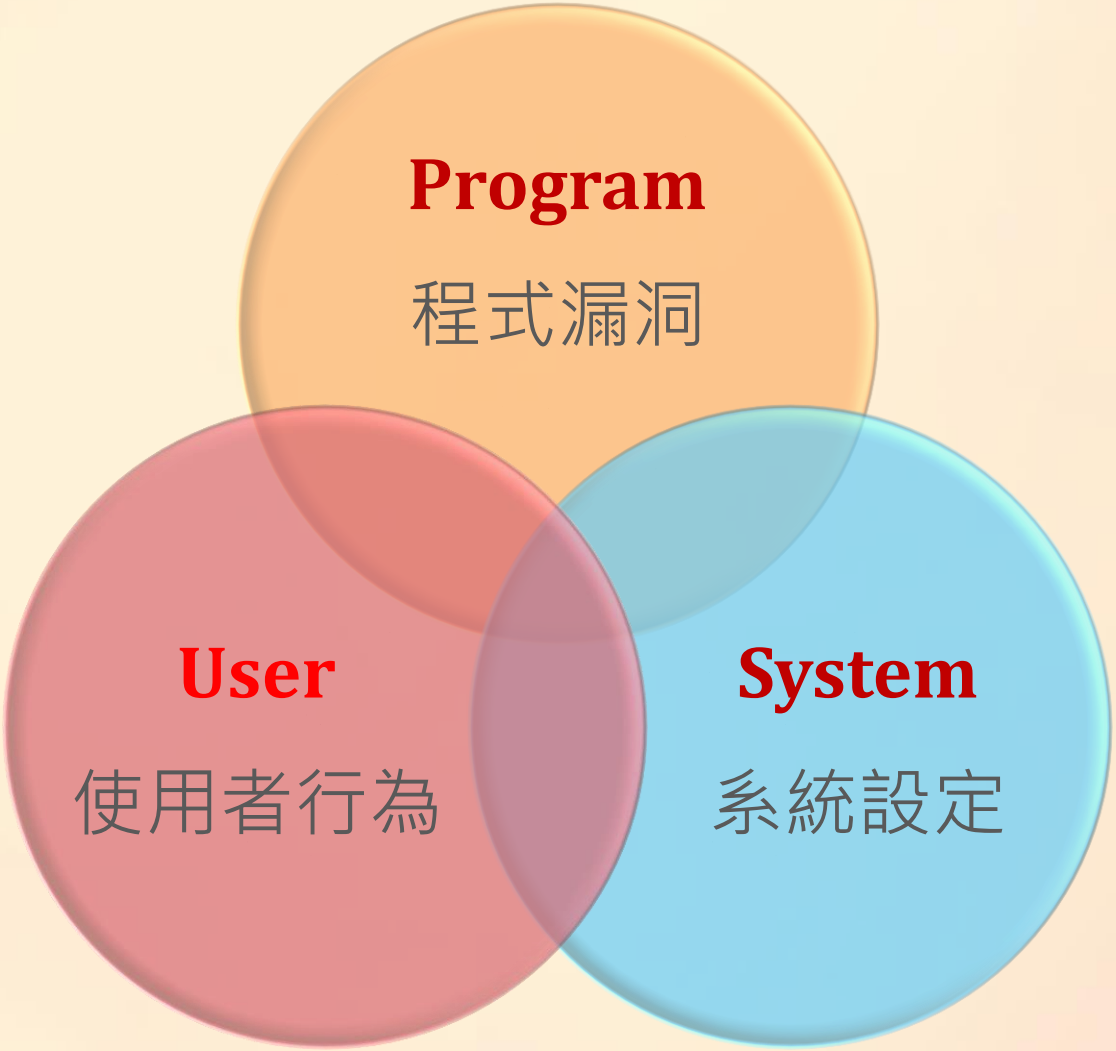
2017-網路資訊安全

- 資訊安全之基本說明
- 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

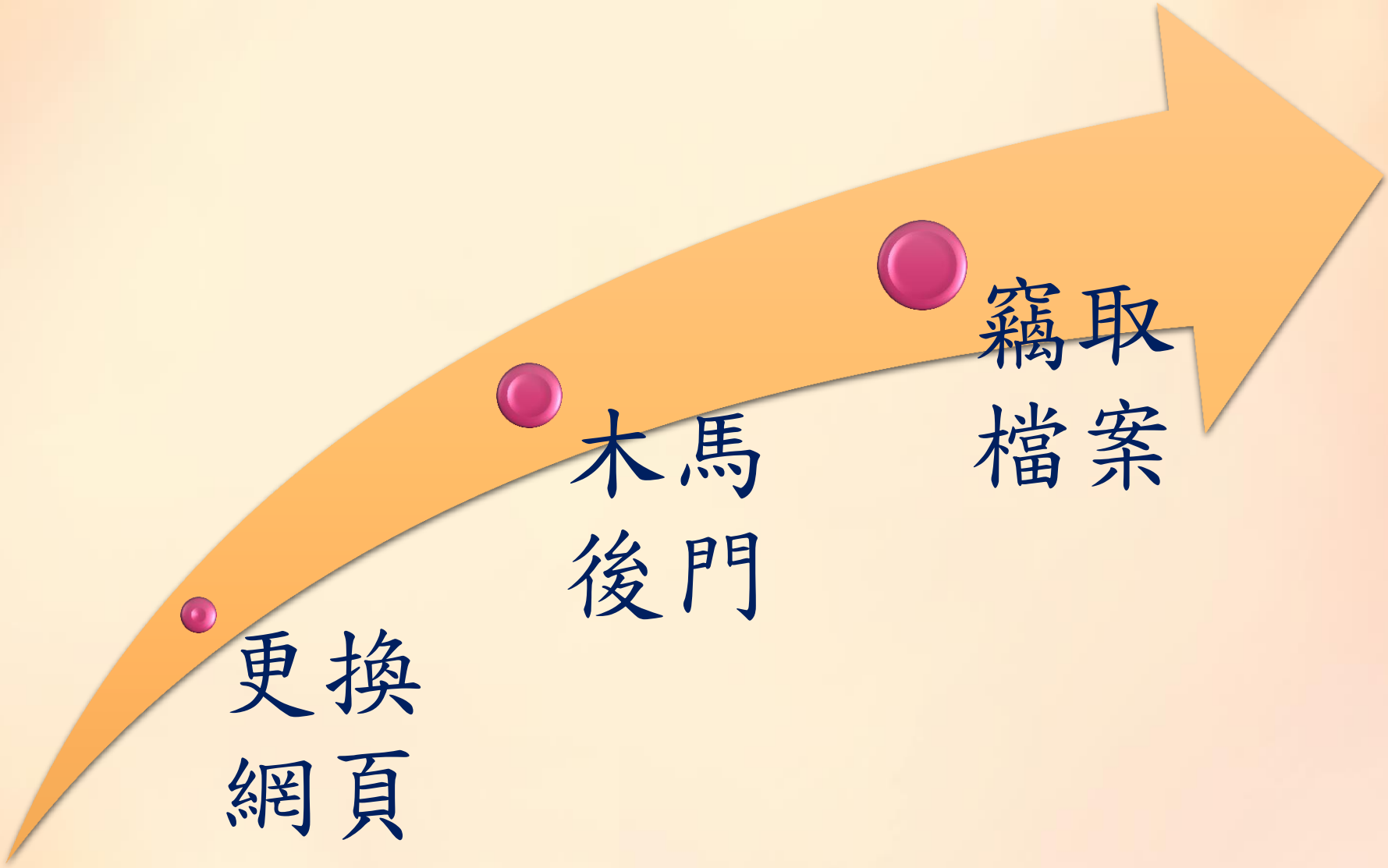
資訊安全之基本說明

劉得民
Diamond Liu
dmliu99999@hotmail.com

網路駭客攻擊的主要途徑

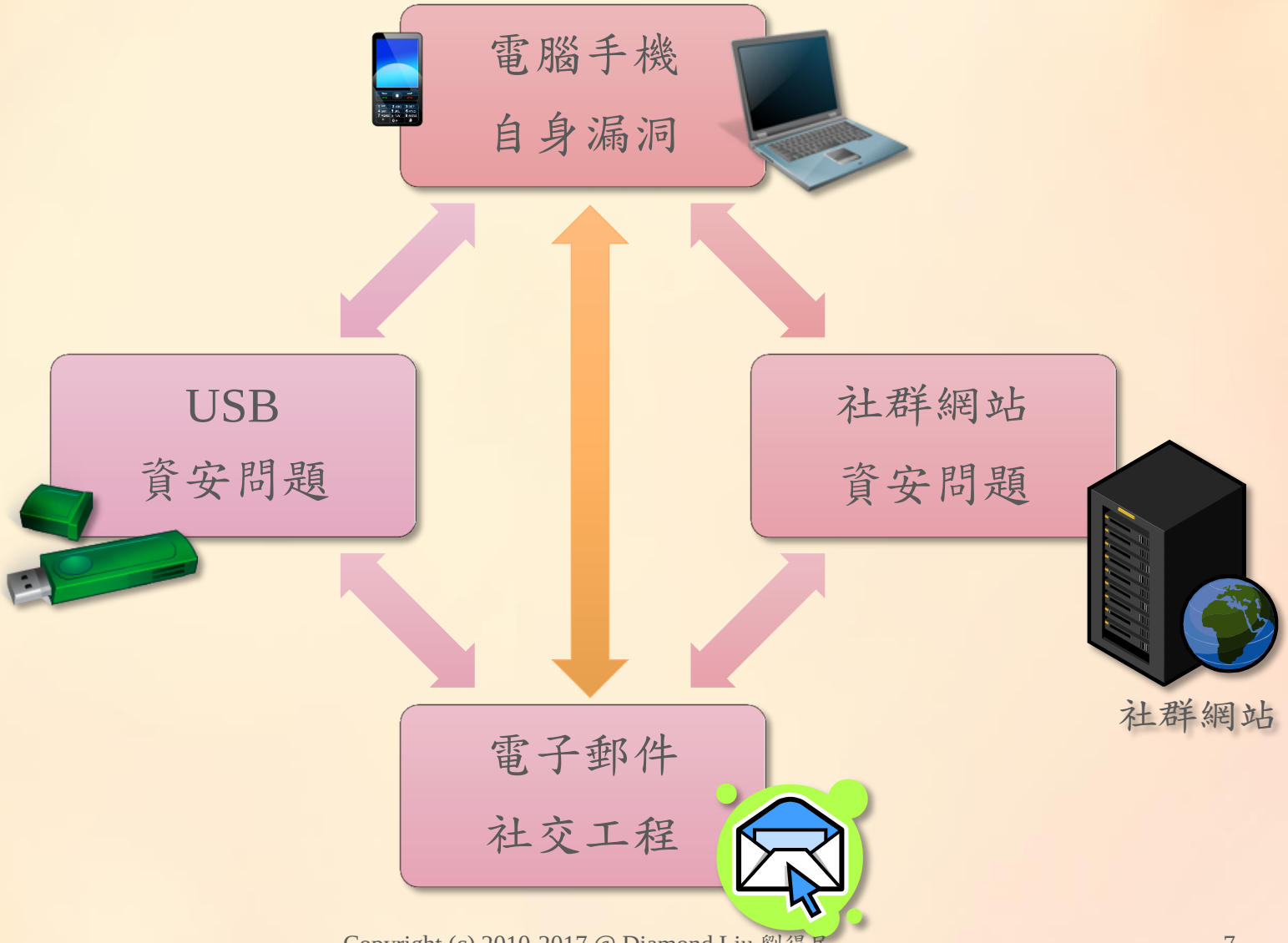


主機端 犯罪模式發展



用戶端 犯罪模式發展

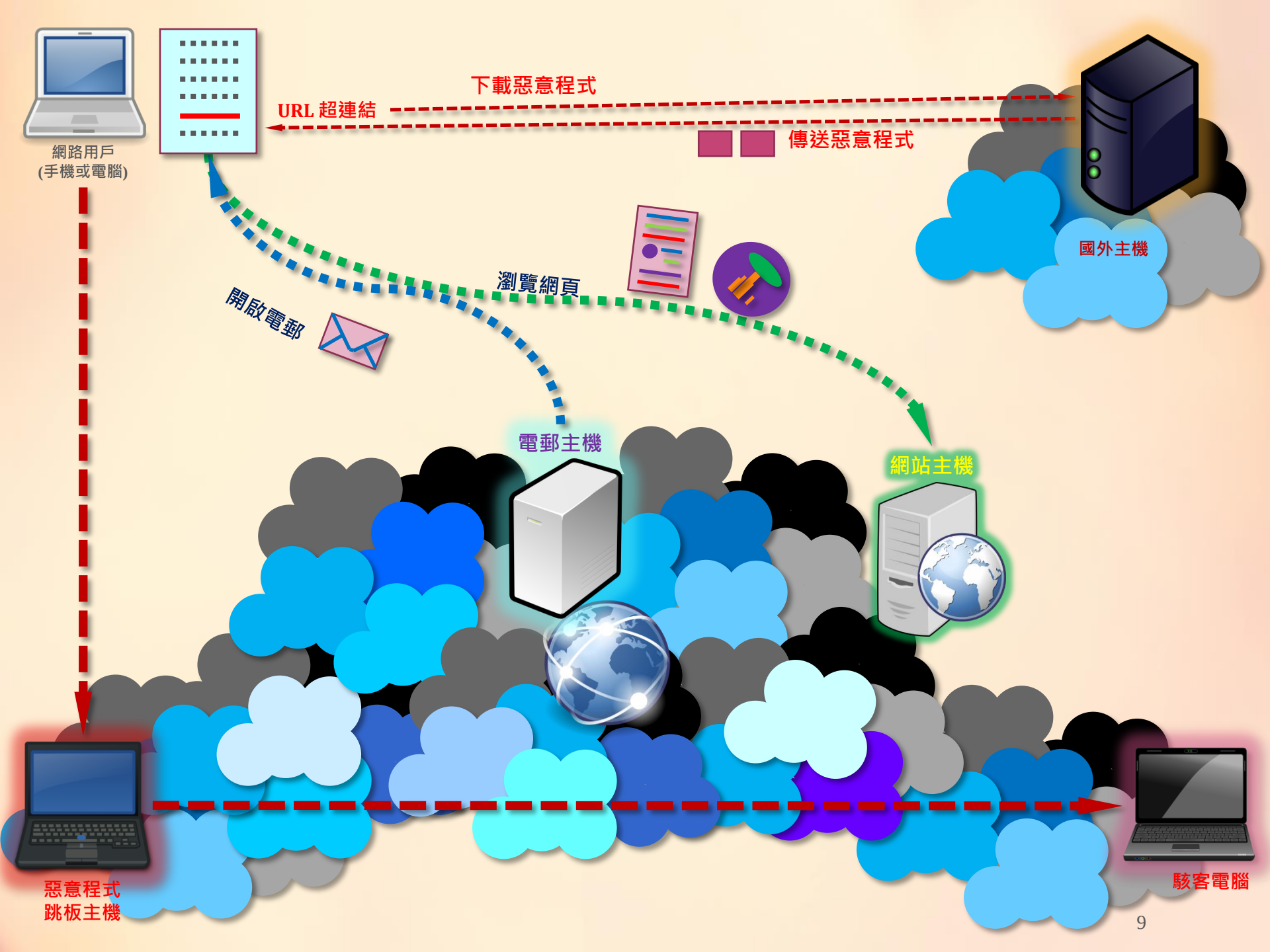
常見資安防範基本知識



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」

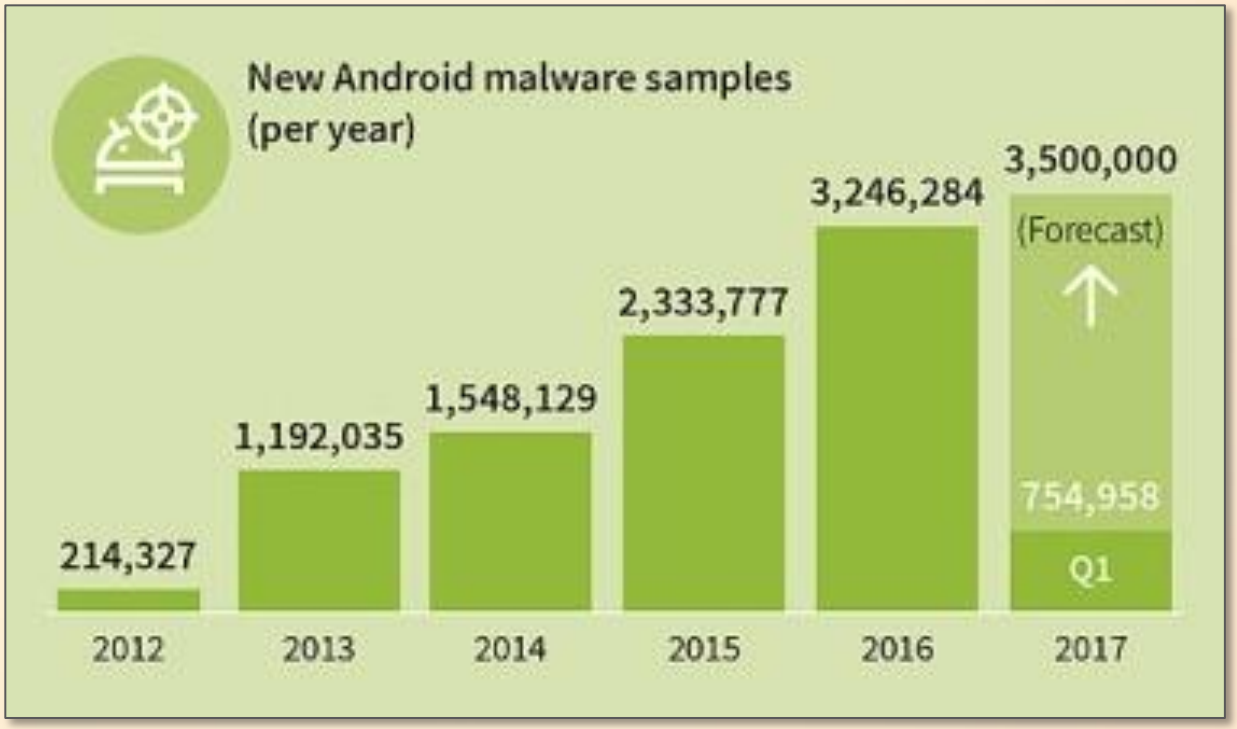
- 網路社交工程，可能的攻擊方式
  - 電子郵件夾帶附件檔案(開啟附件)
  - **郵件內容要求點選URL超連接網址(下載檔案)**
  - 郵件隱含可執行程式碼(JavScript)
  - **瀏覽影片網站或是手機瀏覽影片圖片**
  - **從非官方網站下載檔案(偽裝真網站)**


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

手機安全與個資防護

劉得民
Diamond Liu
dmliu99999@hotmail.com

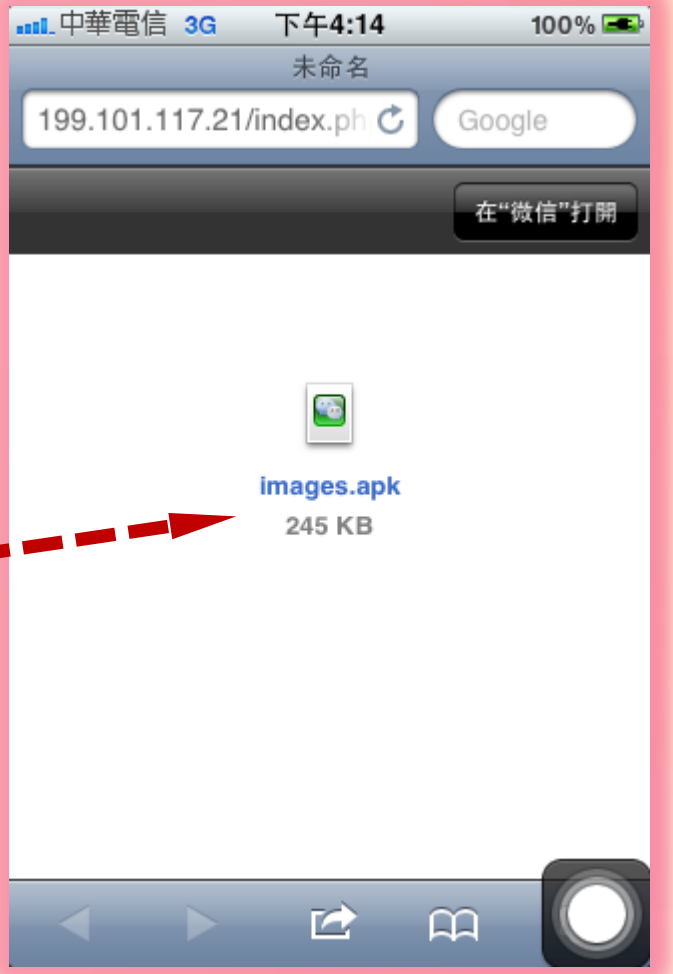
Android手機，最容易被攻擊



舊型Android系統，容易被駭

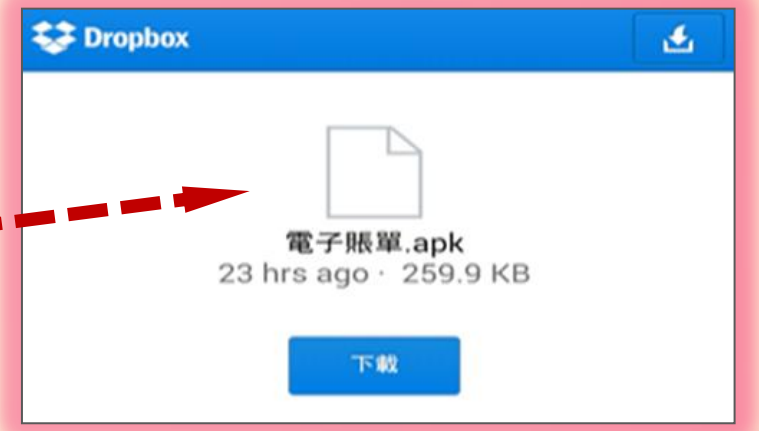
- 每 10 秒鐘就會發現一款新的 Android 惡意應用程式。
- 2017年5月的統計資料
  - 全球只有4.9%的Android裝置升級Android 7.0，而該系統已經發佈了8個多月。
  - 升級到Android 6.0的手機，31.2%。
  - 將近32%的手機使用Android 5.0 (漏洞很多)。
  - 20%執行Android 4.4以下的版本 (容易感染病毒)。
- 沒有更新到最新的Android版本，主要因素
  - **手機製造 OEM 廠商不提供舊裝置的Android系統更新。**
- 大部分手機惡意應用程式，主要出現在非Google官方的第三方應用商店。

Android手機 的 可執行檔案 APK



手機 各種詐騙方式

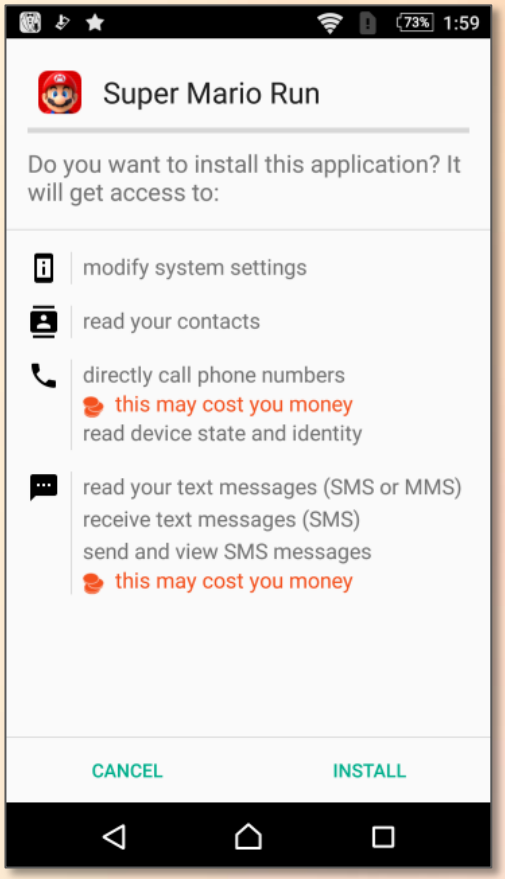
- 手機接獲訊息（內含網址URL連結）
  - 費用帳單、快遞資訊、好友訊息 …
  - 「上次聚餐照片，你不在好可惜！」 、 「被偷拍的是你嗎？」、「取消網路支付電費」、「快遞簽收單」…



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

Bloomberg Technology | 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."

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

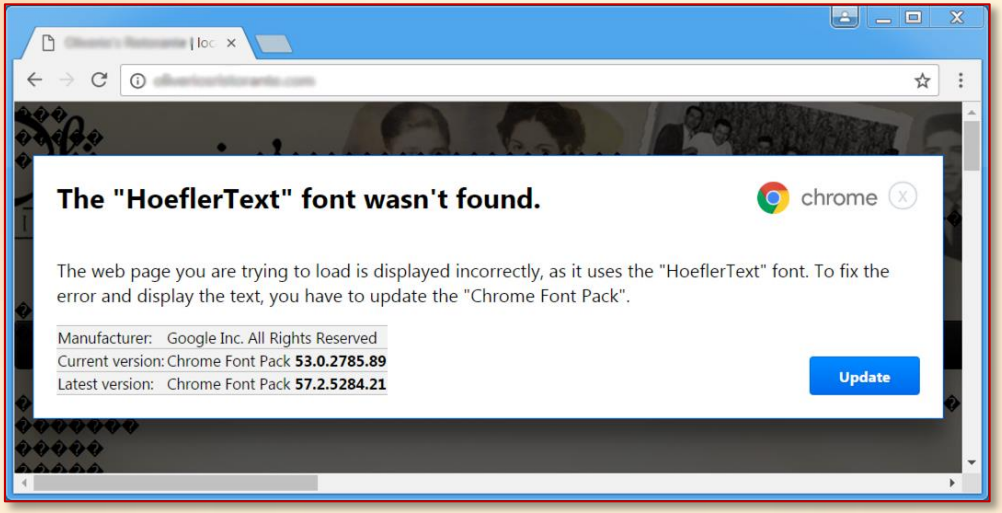
案例學習重點

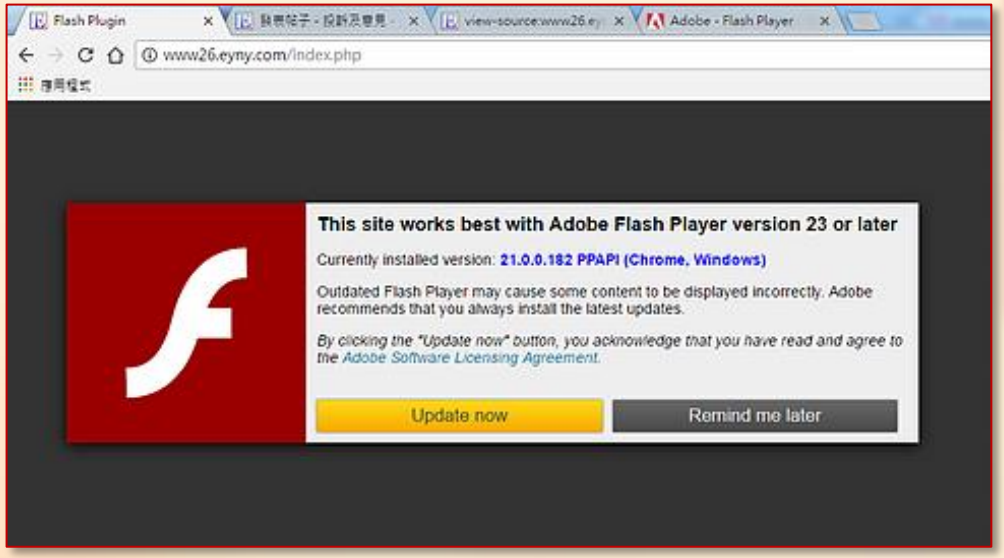
1. APK檔案，是Android的可執行檔案之一。點選 APK或apk檔案，是危險的手機行為。
2. 不要安裝來路不明的遊戲程式，或是遊戲破解軟體。
3. 舊型Android手機(5.0以前的版本)，容易造成駭客入侵。
4. 重要資料備份，至少每2個月進行一次。
5. 某些App，疑似預藏惡意行為程式(過多的操作權限)。
6. **中國大陸政府，2016已經通過網路安全法，加強網路監控。**

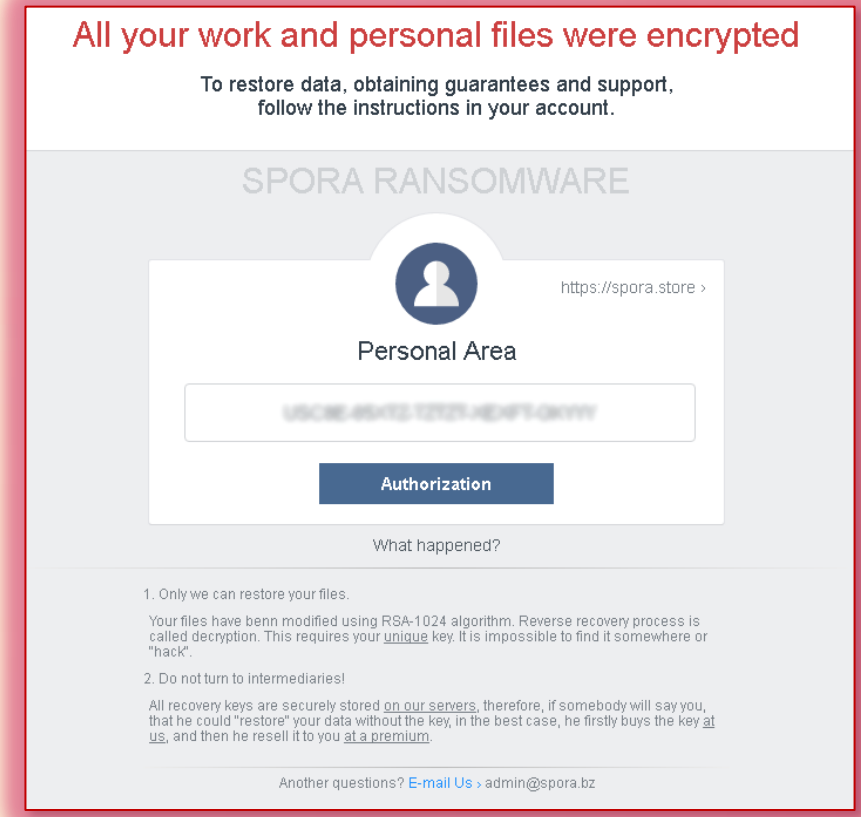
檔案加密勒索與防範

劉得民
Diamond Liu
dmliu99999@hotmail.com

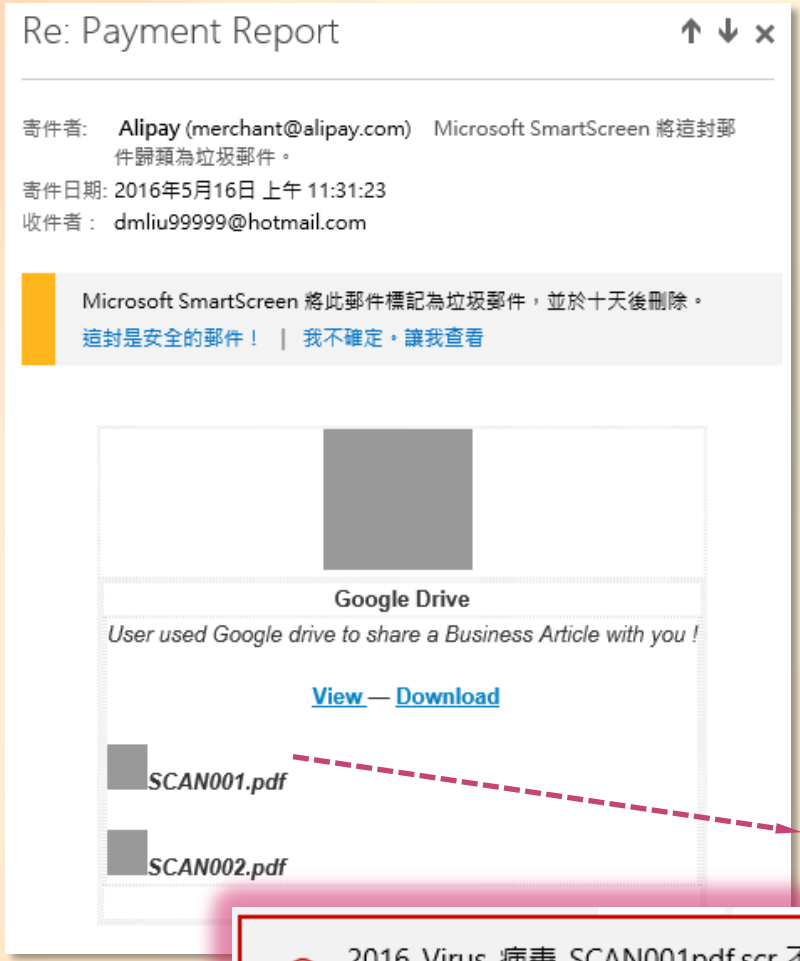
論壇網站遭入侵(網頁掛馬,假訊息)



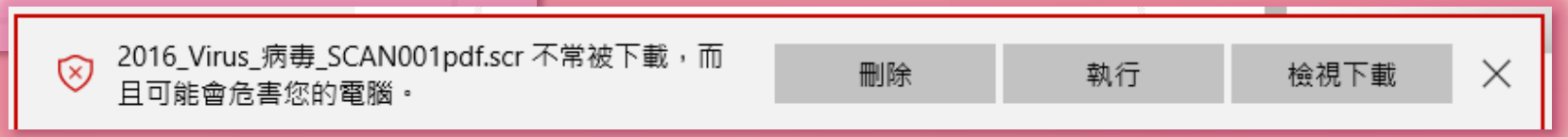




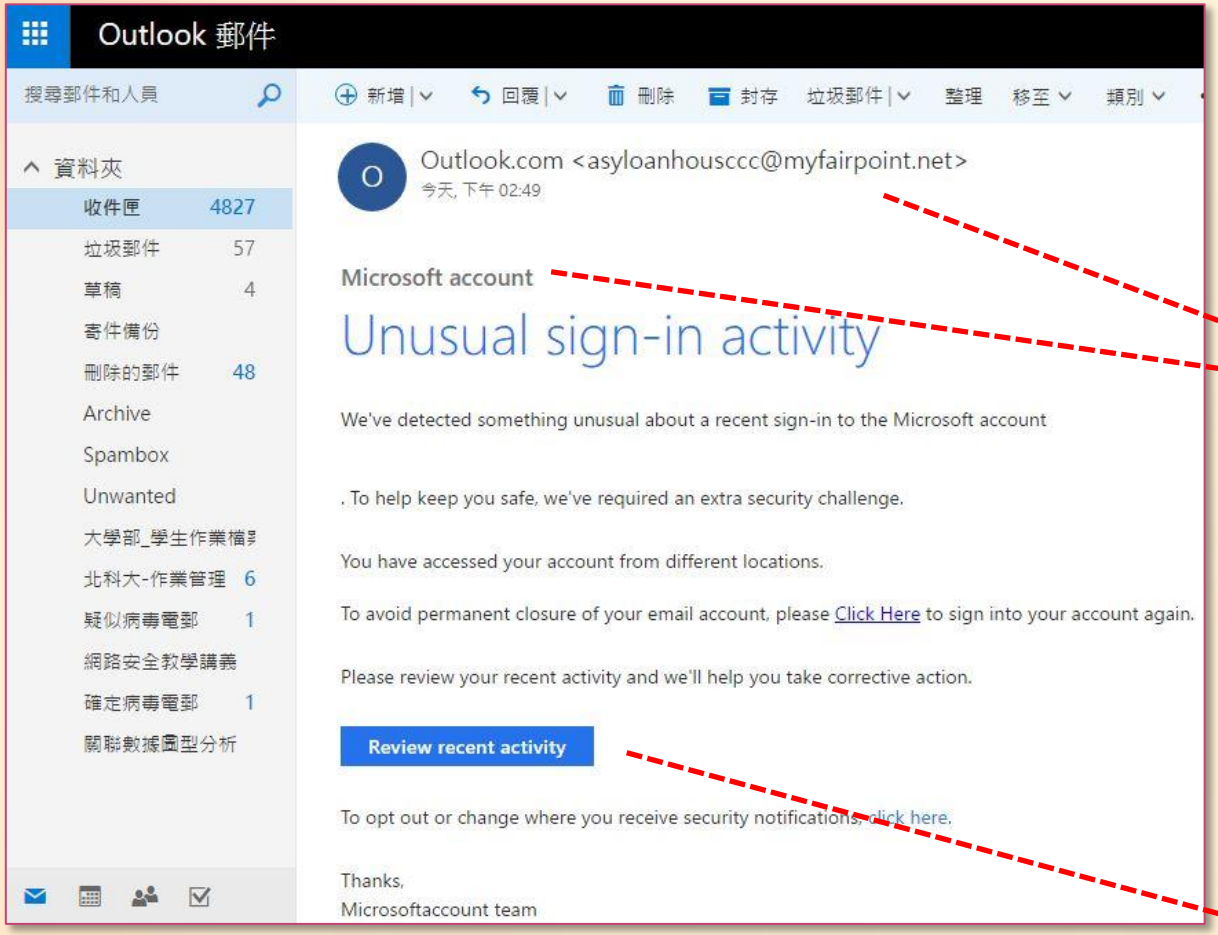
開啟電郵，電腦檔案被加密勒索



電子郵件，金融對帳單，提醒瀏覽(下載)
(這是惡意程式)



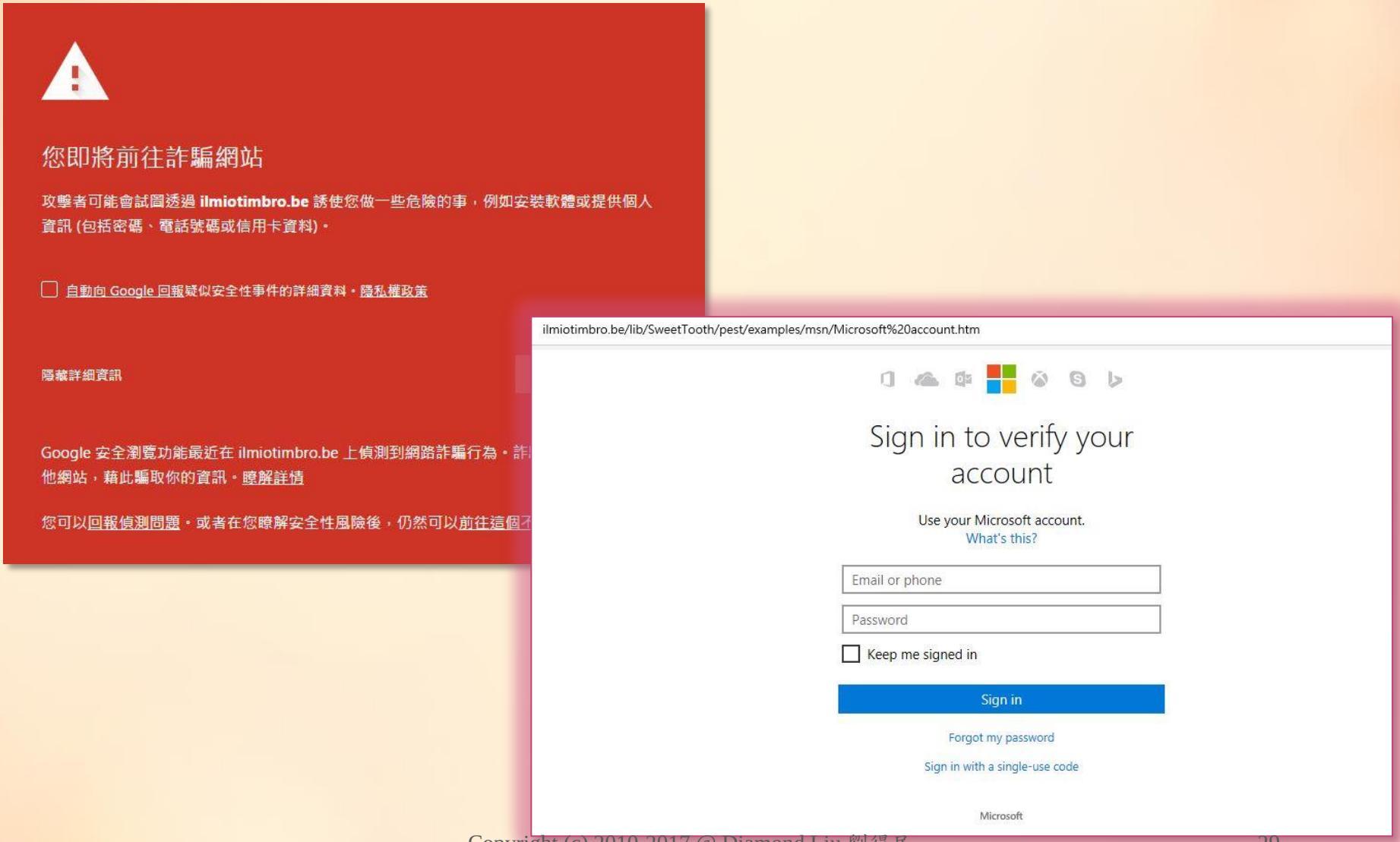
開啟電郵，電腦檔案被加密勒索



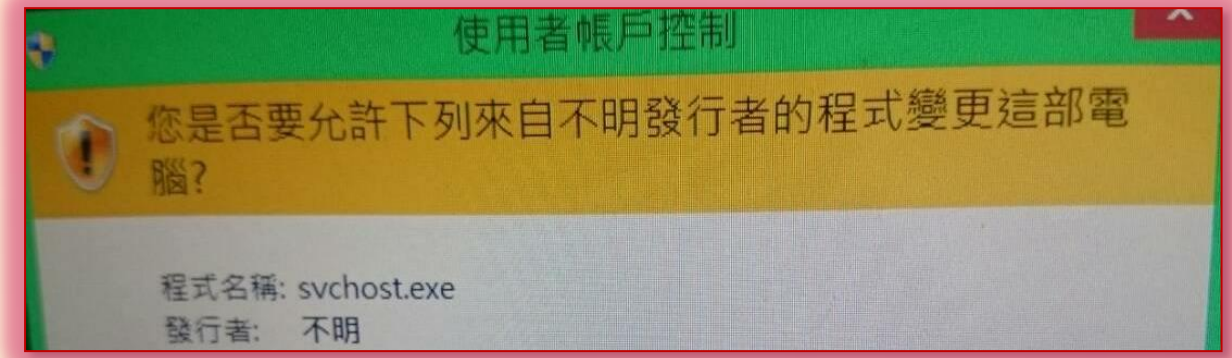
寄件人資訊，怪怪的！

駭客寄送的惡意程式

開啟電郵，電腦檔案被加密勒索

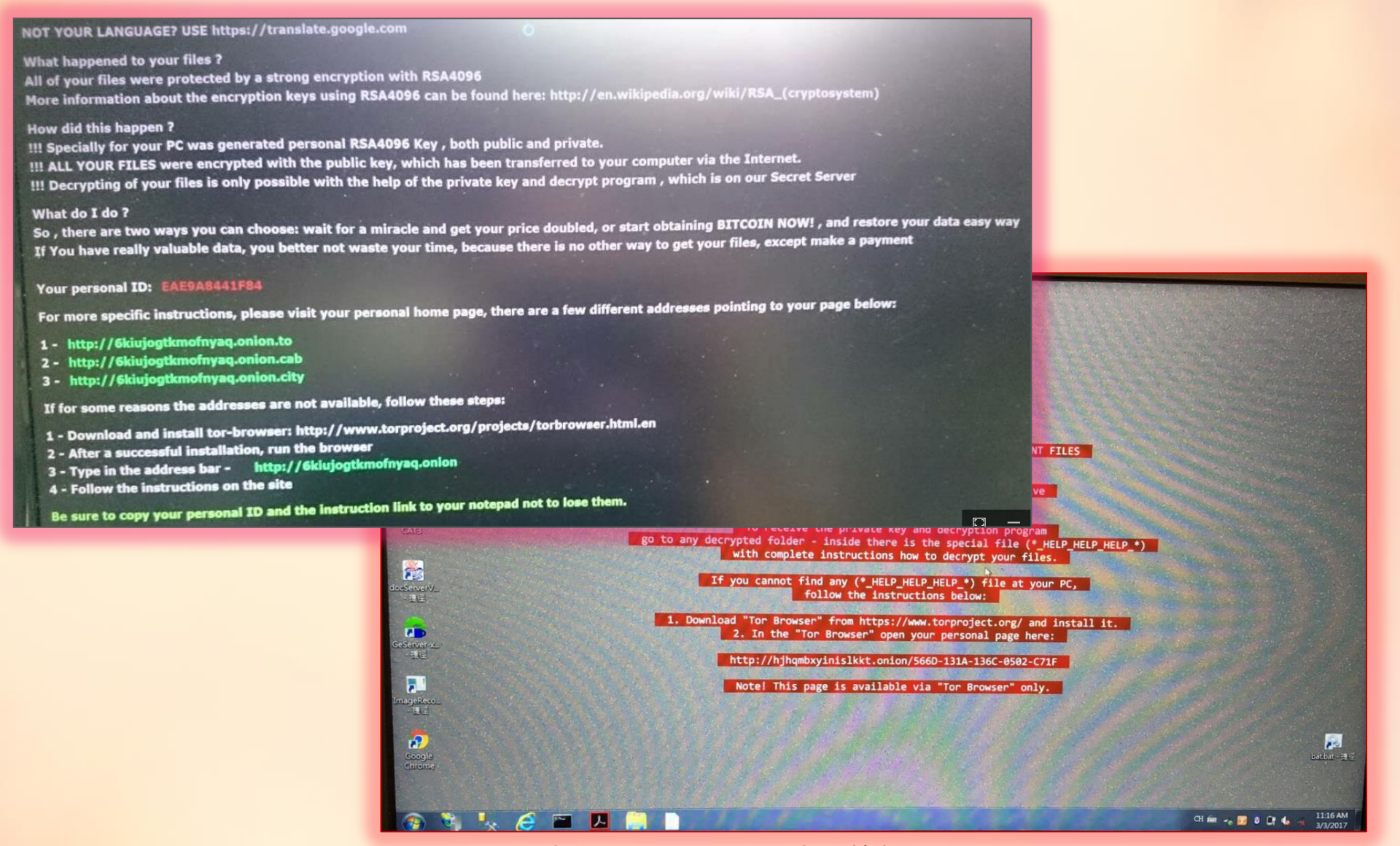


瀏覽網頁，需要特殊權限?



小心!! 這是駭客放置的加密勒索病毒

瀏覽網頁，電腦檔案被加密勒索



撕票型加密勒索病毒案例

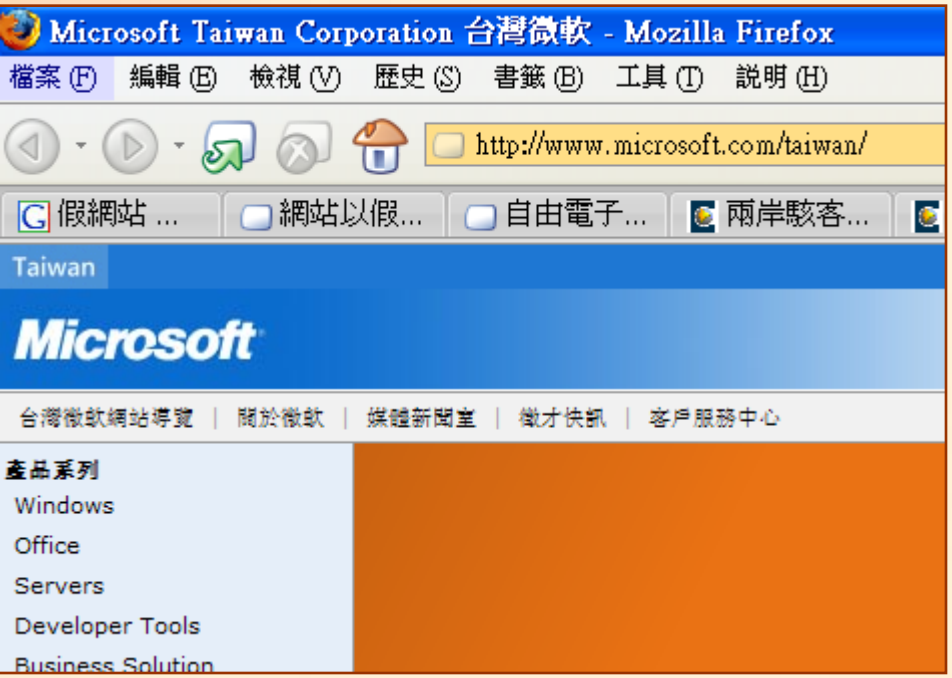
- 此病毒會在螢幕上顯示一個 10 分鐘的倒數計時器，每次 10 分鐘一到，就會刪除受害者一個被加密的檔案。
- 此病毒是經由惡意網站感染，或是由其他惡意程式植入系統當中，受害者可選擇英文或法文介面。
  - 首先，勒索病毒會將自己複製一份到系統上，然後在系統登錄當中增加一筆設定讓系統在重新開機時自動執行該病毒並觸發加密程序。
  - 被加密的檔案名稱末端會多了「.lelele」副檔名。
  - 除此之外，French Locker 還會查看系統上是否有下列執行程序 (Processhacker、Taskmgr、Wireshark、Chrome、Firefox、Skype)正在執行…。

撕票型加密勒索病毒案例

假Google資料，感染勒索病毒

- 稱為「Mole」(鼴鼠) 的 CryptoMix 勒索病毒，它會利用 Google Doc 連結來感染受害電腦 ，台灣目前也傳出受駭案例。
- 此勒索病毒是經由垃圾郵件散布，案例是假冒美國郵局的名義，內含網址連結(假 Microsoft Office 入口網站)，該網站會指示使用者，點選某個按鈕來下載所需的外掛元件(字型檔案或是Adobe/Java更新檔案)。
- 它會下載勒索病毒檔案到電腦系統，其真正連結是個 Google Docs 網址，該網址每個樣本都不同。每當駭客上傳一個新的樣本時，就會產生一個對應的新網址。

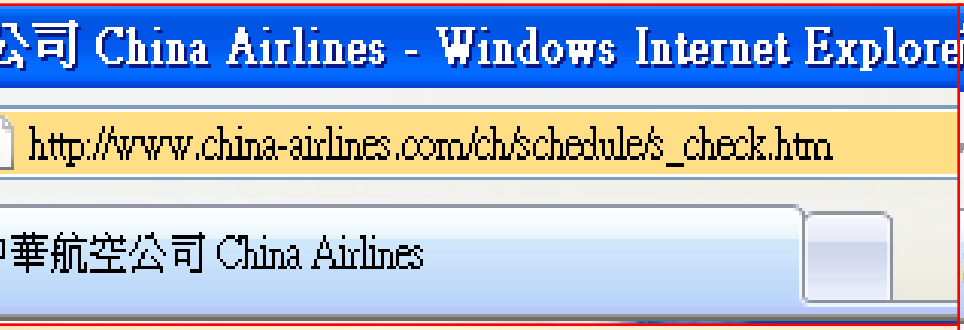
在2秒鐘內，能發現2者差異嗎?



http://www.microsoft.com

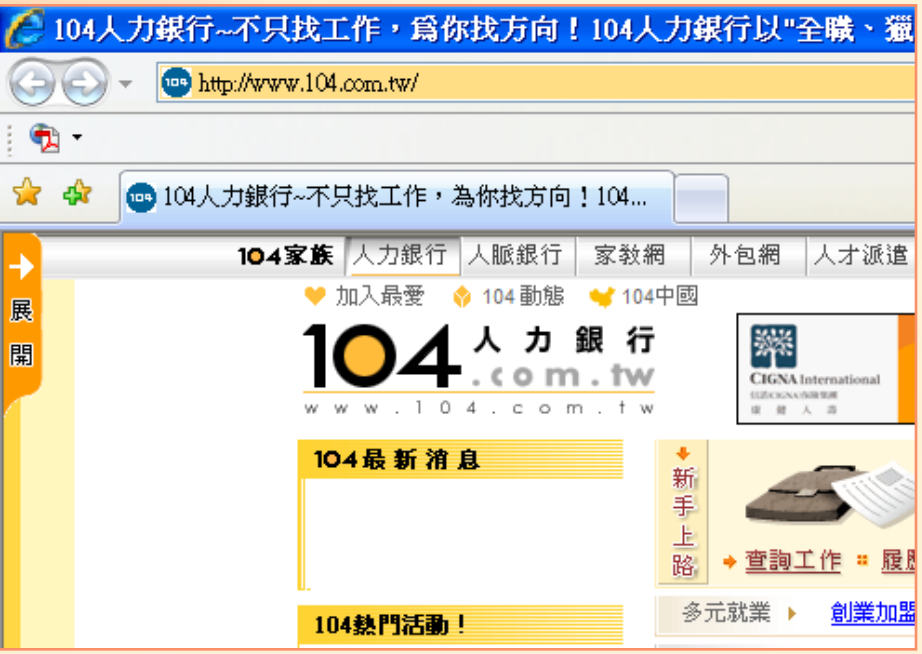
http://www.rnicrosoft.com

在2秒鐘內，能發現2者差異嗎?



在2秒鐘內，能發現2者差異嗎?

能分辯真假網站嗎?



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

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,...)

其他駭客攻擊之案例討論

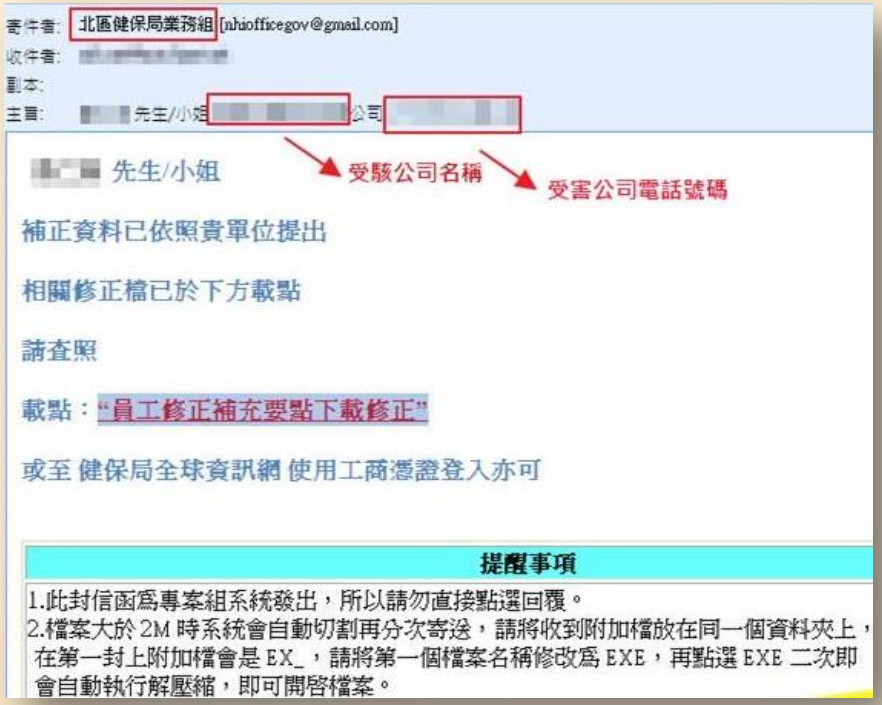
劉得民
Diamond Liu
dmliu99999@hotmail.com

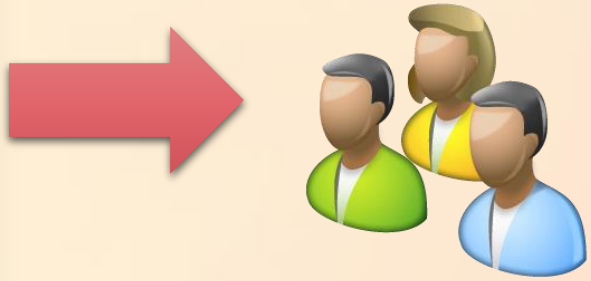
偽冒健保局寄發惡意電子郵件

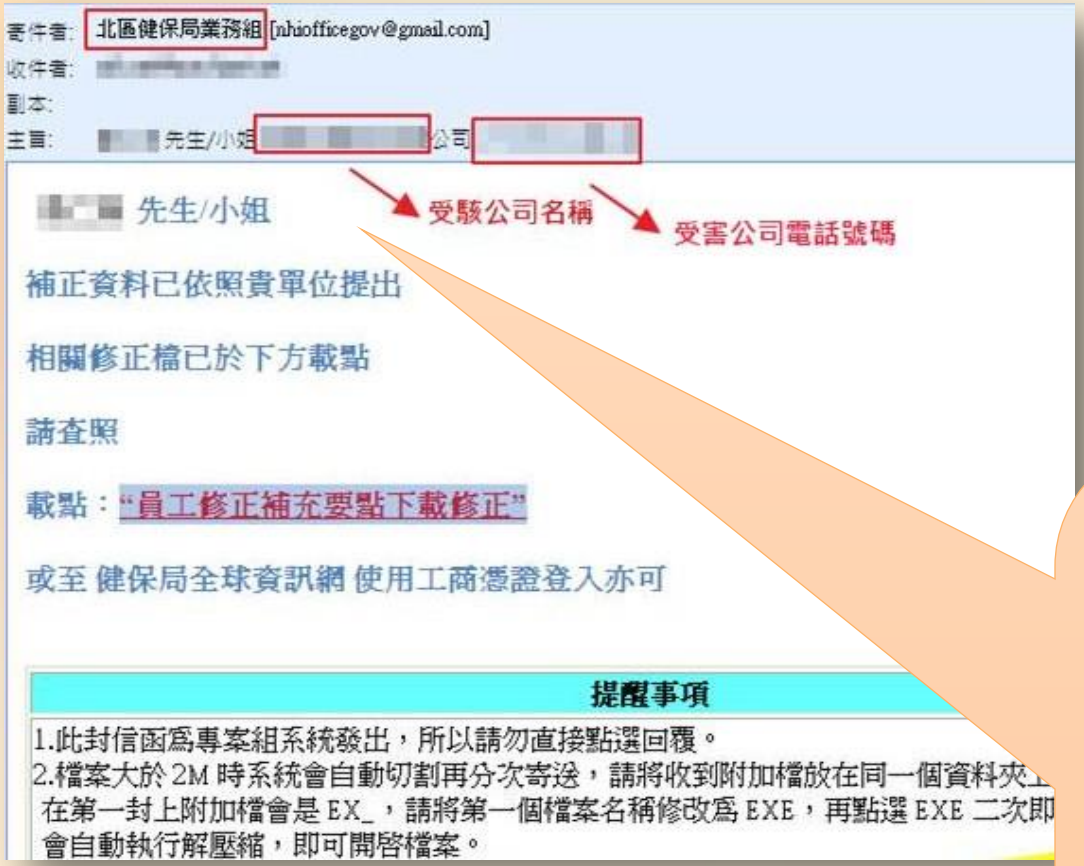
(一)時間：102年4月。

(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。

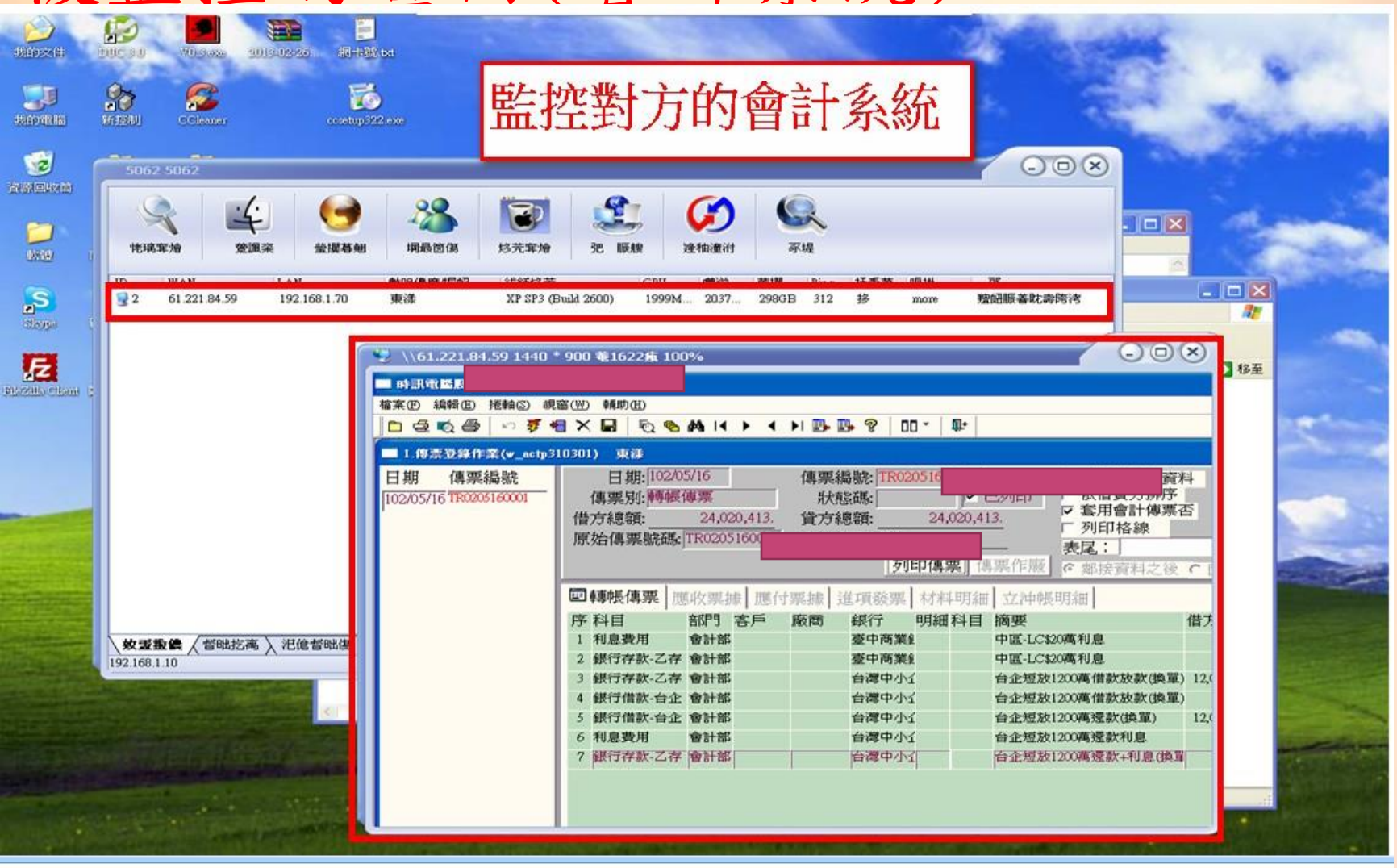






嫌犯被逮捕後表示當初從網路上搜尋取得或他人指定之中小企業公司會計部門或負責人寄送含惡意程式之電子郵件，由於電子郵件主動出現對方姓名，多半不疑有他點選惡意程式並注入後門程式成功!

被監控的畫面(會計系統)



44

2010-02-22 _diguapinggao@gmail.com_Taiwan 2010_Taiwan 2010.doc
2010-02-23 _tony_tseng@gmail.com_回覆 RE 學長好!!_照片(加密).bmp.rar
2010-03-06 _press02@mofa.gov.tw__ATT64535.pdf
2010-03-08 _titx@oa.tku.edu.tw_敬邀參加兩岸關系研討會__.pdf
2010-03-10 _plwang@gmail.com_FW 請收悉_[].pdf
2010-03-17 _chchang@gmail.com_選舉情勢分析_2010.pdf
2010-03-23 _yukochung@gmail.com_FW 快樂的五個簡單規則_ATT59244.ppt
2010-03-24 _h670928@ndu.edu.tw_2010第十八屆國防管理學術暨實務研討會_ATT43728.pdf
2010-03-25 _fovery.wait@kimo.com_Fw 瑪雅成人論壇最新網址--防遮置版，附件為最近一星期合集，_ATT3790...
2010-03-25 _jesseandy2@gmail.com_conference memo_conference memo.PDF
2010-03-25 _xiaobo.chen781@kimo.com_老兄：具體策劃方案已擬好，詳見附件，請您指教修正_ATT70176.pdf
2010-03-31 _beneco.taipei@webmail.gov.tw_每日網情彙編990331_-99031.doc
2010-03-31 _beneco.taipei@webmail.gov.tw_每日網情彙編990331_-990331.ppt
2010-04-03 _edward46@mail.moe.gov.tw_敬邀參加「淡江戰略學派之建構與當代戰略趨勢研討會」_990508_.pdf
2010-04-03 _yk397@yahoo.com.tw_小S老工夜店親近搜辣妹(副圖)壓縮密碼668_ATT93841.rar
2010-04-06 _jchiang@webmail.gov.tw_小組會議報告990406_0406.rar
2010-04-12 _msshen@gmail.com_明室稿件_ATT22152.pdf
2010-04-15 _chuc.ling@yahoo.com_Fw 歐巴馬政府與美中台關係徵稿公告_ATT95097.pdf
2010-04-18 _bank.csc@inibr.chinatrust.com.tw_中國信託提醒通知函_ATT13624.pdf
2010-04-25 _shunwengw@npf.org.tw_企劃書--蔡老師70華誕學術研討會_-.pdf
2010-04-26 _liwunc@yahoo.com_丁樹範老師文章_MCSS().pdf
2010-04-26 _RSISPublications@NTU.EDU.SG_South China Sea Emerging China -Taiwan Cooperation by Li ...
2010-04-26 _RSISPublications@NTU.EDU.SG_South China Sea Emerging China -Taiwan Cooperation by Li ...

2010-05-01 _pishin@ey.gov.tw_請問馬總統博士陛下_ATT16747.pdf
2010-05-03 _zhonggonv@nccu.edu.tw_2010 年中共年報_2010 .doc
2010-05-03 _zhonggonv@nccu.edu.tw_2010 年中共年報_2010 .pdf
2010-05-06 _jjsung@ntu.edu.tw_蔡政文教授七十華誕系列活動簡報_ATT59802.pdf
2010-05-07 _lsf@gate.sinica.edu.tw_201004_遠見民調中心_台灣民眾政黨傾向追蹤分析_GVSRC_PID_201004_C....
2010-05-10 _0922750173@mail.ahccddi.org.tw_99下半年國防工業評鑑日期表_ATT39755.xls
2010-05-11 _taup@seed.net.tw_轉發訊息：5_16(日)早十點～新臺灣國策智庫研討會-恐懼的總和：馬政府執政兩...
2010-05-11 _taup@seed.net.tw_轉發訊息：5_16(日)早十點～新臺灣國策智庫研討會-恐懼的總和：馬政府執政兩...
2010-05-13 _taup@msa.hinet.net_FW 三軍總醫院健康檢查中心提供健康食譜.xls_ATT42396.xls
2010-05-14 _wod1129@yahoo.com.tw_十個方法全面“搞定”花心男！_!.rar
2010-05-17 _wod1129@yahoo.com.tw_蠢感都米了,悲劇啊.... _..... .rar
2010-06-08 _jirj@nccu.edu.tw_天安艦後的朝鮮半島新局勢_ATT77316.pdf
2010-07-11 _chengkunm@gsn.gov.tw_美國聯邦調查局公佈中國收買間諜的活動監控錄影_ATT44082.pdf
2010-07-11 _jirj@nccu.edu.tw_雙週報 1579期_ATT50892.pdf
2010-07-12 _ljwi@nsb.gov.tw_美俄“間諜門”_ATT54496.pdf
2010-07-12 _sefo197@gmail.com_海基會「交流」雜誌112期_ATT73820.pdf
2010-07-18 _lennkuo@mail.gio.gov.tw_由兩岸的「經濟合作架構協議」解析自由貿易的精髓_--.pdf
2010-07-19 _renshianw@mac.gov.tw_ECFA文本的特色與意含_ECFA.pdf
2010-07-21 _kozhokin@riss.ru_o covmes ucheniiakh SHA i yuzhnoi korei_o covmes ucheniiakh SHA i yuzhnoi ...
2010-07-25 _kellcy316@yahoo.com_8月份財政預算_8.xls
2010-07-26 _mishus@gsn.gov.tw_電腦科技對空軍航電系統之衝擊_ATT21407.pdf
2010-07-27 _henry_0823@yahoo.com.tw_99年度國防淨評估論壇_99(0727).pdf
2010-07-28 _anwsJI@ms1.anws.gov.tw_特蒐臺北人氣美食TOP5_TOP5.pdf

2011-07-20 _titx@www2.tku.edu.tw_Fw 南海問題-兩岸軍事互信之契機龔陸生_-.pdf
2011-07-24 _shtin99.john@msa.hinet.net_FW 高鐵安全注意事項_ATT10433.doc
2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜，請 查照。_2 .doc
2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜，請 查照。_4 .doc
2011-07-26 _titx@www2.tku.edu.tw_轉寄：函知100學年度第1學期選課相關事宜，請 查照。_ATT13628.doc
2011-07-27 _chao.wei@msa.hinet.net_溫州動車脫軌事故安全啓示_ATT43518.rar
2011-07-31 _honto.denki@msa.hinet.net_FW early headlines_headlines.doc
2011-08-01 _mikina89@ndu.edu.tw_請及時將附件的資料補齊_ATT81208.doc
2011-08-02 _engkong.kh@msa.hinet.net_台灣基督長老教會2011年行事曆_2011().xls
2011-08-04 _ebill@ebsmtp01.TaiwanMobile.com_台灣大哥大100年07月份電子帳單寄送函_10007-982458470...
2011-08-04 _justin.fanny@msa.hinet.net_非凡美食大探索_861-7145.xls
2011-08-04 _viki.info@yahoo.com.tw_「二０一一年臺北國際航太暨國防工業展」_2011--TAIPEI.doc
2011-08-08 _jojobox@ms21.hinet.net_爸爸節快樂!_ATT50833.rar
2011-08-24 _thougntsl68@gmail.co_國防部整合評估室誠摯邀請各位貴賓出席8_29歡迎酒會及8_31晚宴_ATT109...
2011-08-26 _hsatan7788@yahoo.com.tw_台灣安保協會「亞太區域安全與台海和平」國際研討會邀 請 函_20110...
2011-08-26 _hsatan7788@yahoo.com.tw_台灣安保協會「亞太區域安全與台海和平」國際研討會邀 請 函_20110...
2011-08-28 _sating.cheng@msa.hinet.net_「九二共識」究竟怎麼看_ATT44112.doc
2011-08-29 _jazn2085@email.cib.gov.tw_少年仔火氣指數診斷新招_0901.pdf
2011-08-29 _ynlin@oop.gov.tw_附件_ATT59379.doc
2011-08-30 _chang.james@msa.hinet.net_阿常致馬總統的一封信_ATT76862.pdf
2011-08-30 _Guang.yn@msa.hinet.net_誤植愛滋器官：一之為甚，豈可再乎？_ATT97724.doc
2011-08-30 _szuyingh@dpp.org.tw_說帖from思．穎．_ATT89844.pdf
2011-08-31 _claire.andre@msa.hinet.net_男性更年期症狀的飲食療法_ATT25574.doc

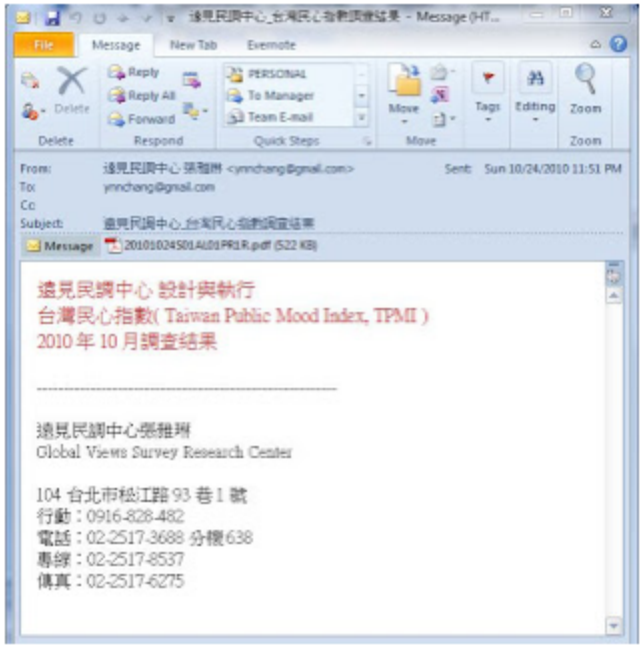
http://contagiodump.blogspot.tw/search?updated-min=2010-01-01T00:00:00-05:00&updated-max=2011-01-01 contagio

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)



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

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. 電腦被植入木馬程式後，可以竊取重要機敏檔案，進行各種詐騙行為。
4. 養成良好習慣，要檢查電子郵件的真實寄送帳號(而非自稱的帳號)。

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) 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