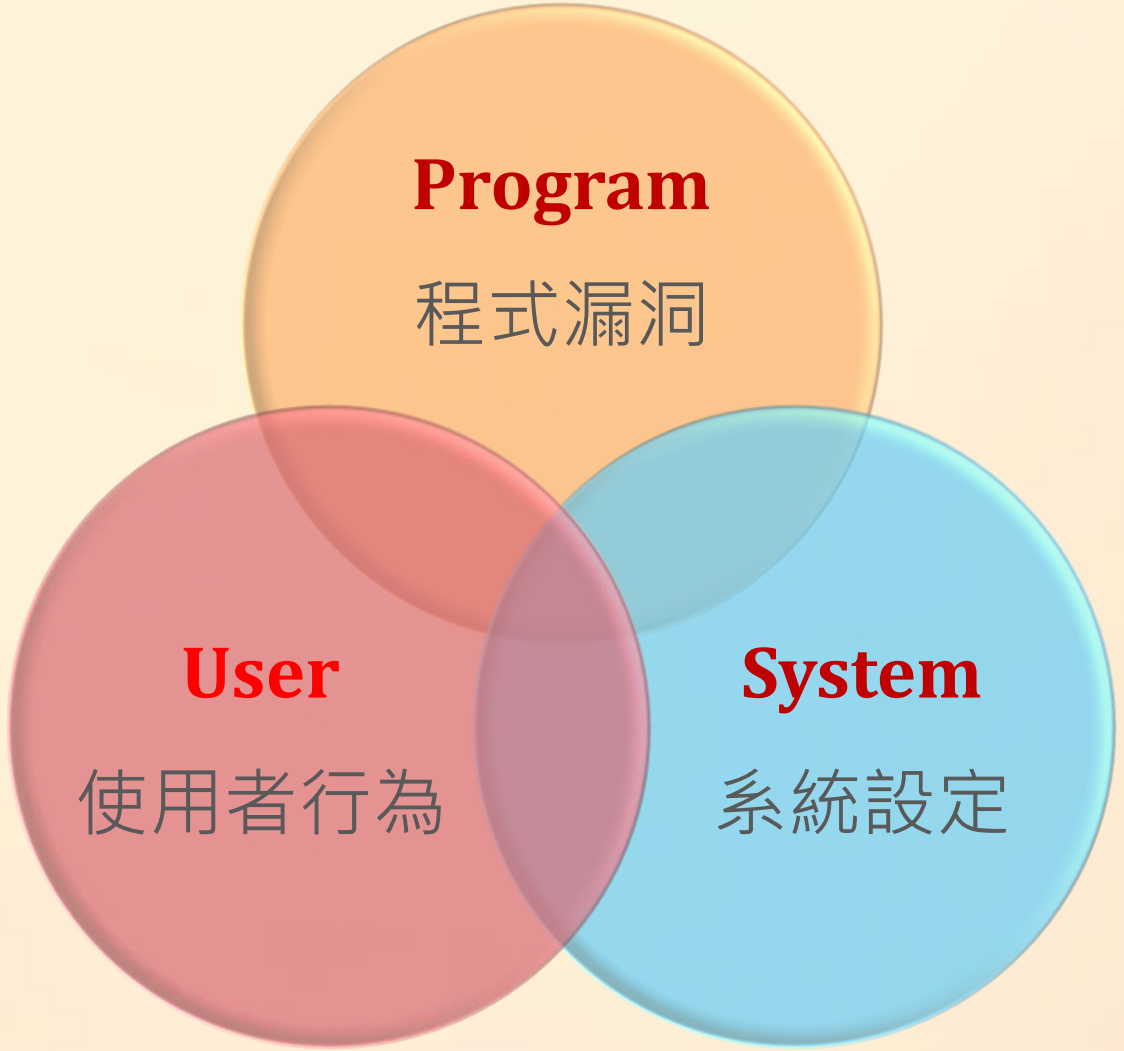
惡意程式最新動態與防治
2018 - Malware Prevention

Diamond Liu (Tei-Min Liu) 0985-604145

惡意程式最新動態與防治

- 網路安全與惡意程式的基本認識
- 網路攻擊與惡意程式的近況報告
- 勒索軟體的處理與實作
- 惡意程式 範例檔案分析實作
- Q&A

網路安全與惡意程式的基本認識



網路攻擊與惡意程式的近況報告

劉得民
Diamond Liu
dmliu99999@hotmail.com

無線網路Wifi的資安問題

資料竊取

轉送資料(竊取通訊)

(偽冒無線)

主機

機房管理員

USB竊取

iTaivvan

無線管理員

iTaiwan
(Free Wifi)

用戶端

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

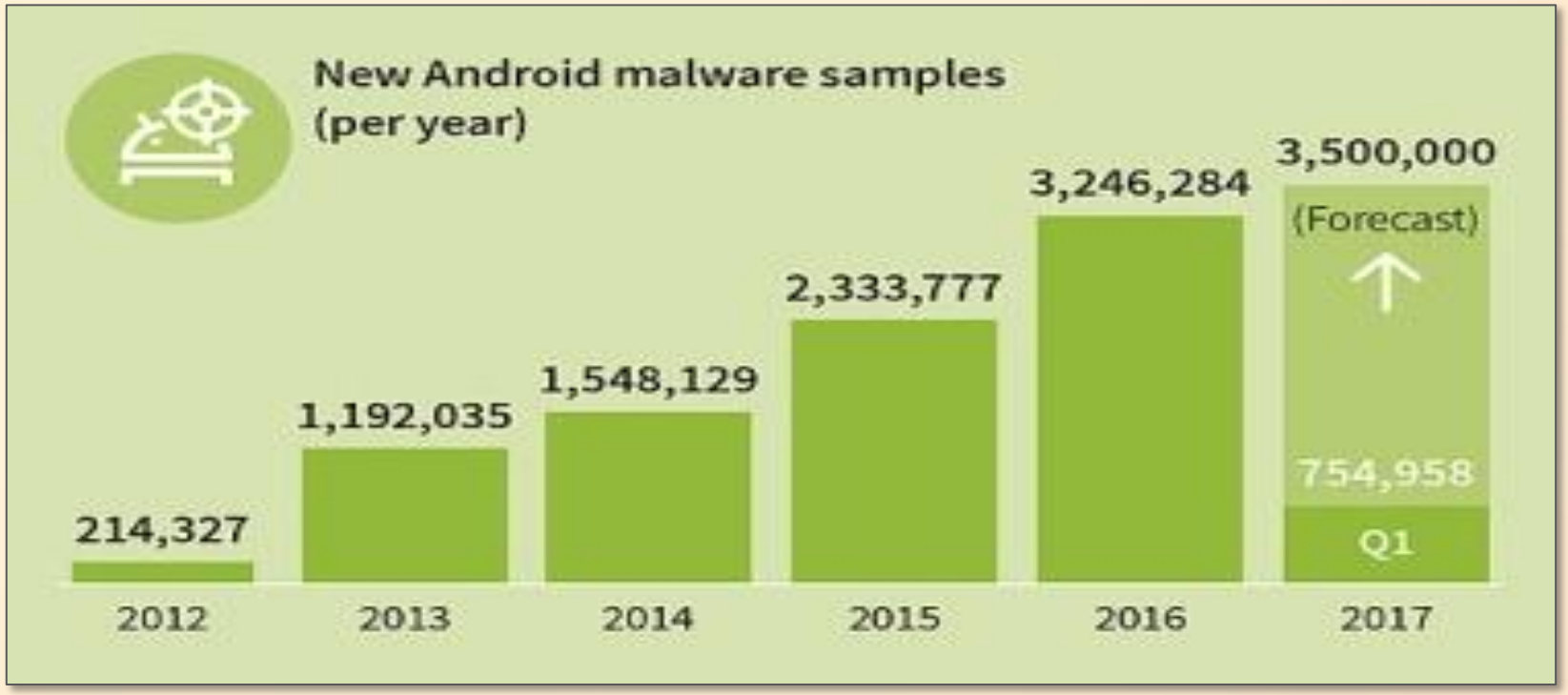
案例學習重點

- **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。
  - 手機與電腦的機敏資料，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!!
- **透過公眾無線網路，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

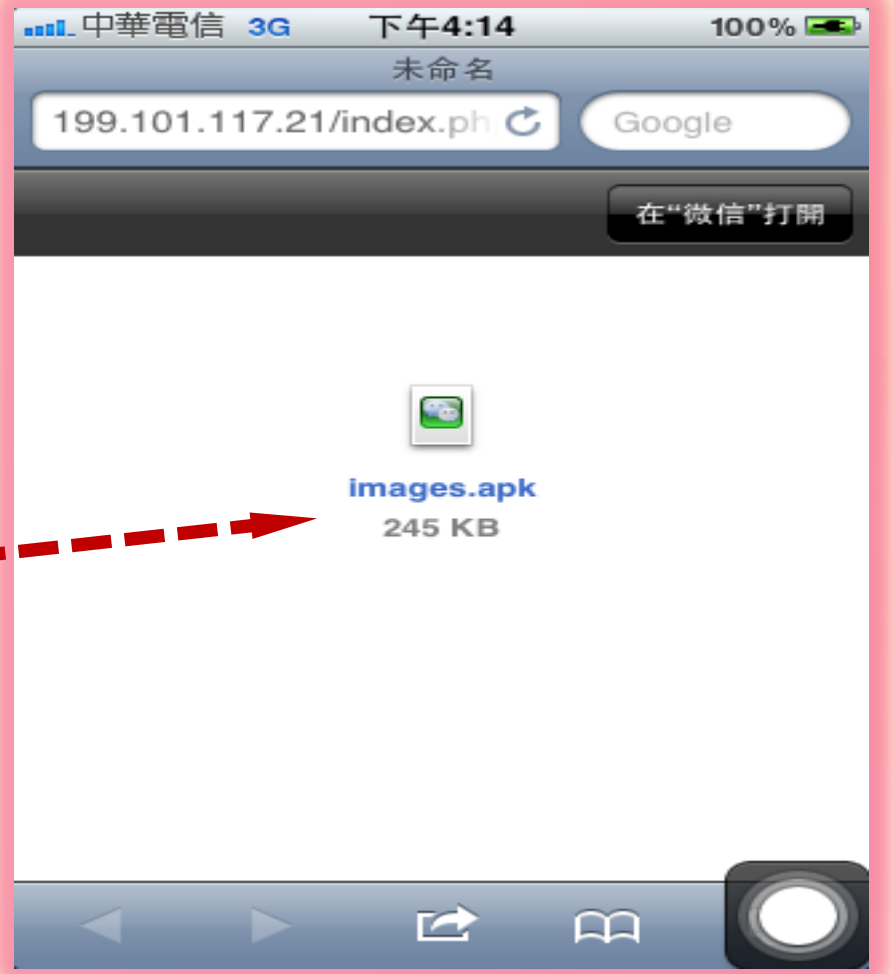
Android手機，最容易被攻擊



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...

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

Bloomberg Technology

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.

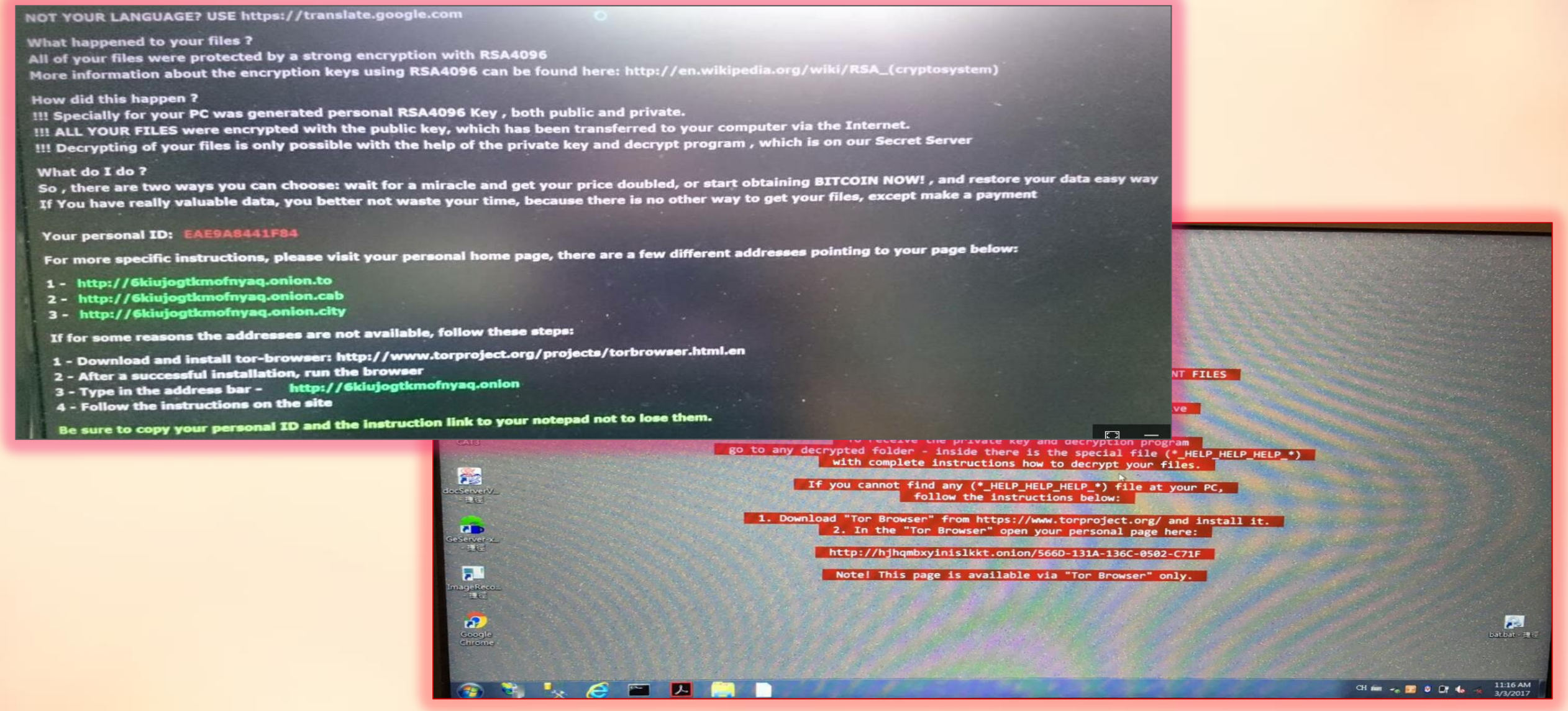
The law also requires business info and data on Chinese citizens gathered within the country to be kept on domestic servers and not be transferred abroad without permission. That last condition hampers the operations of multinationals accustomed to a global Internet computing environment.

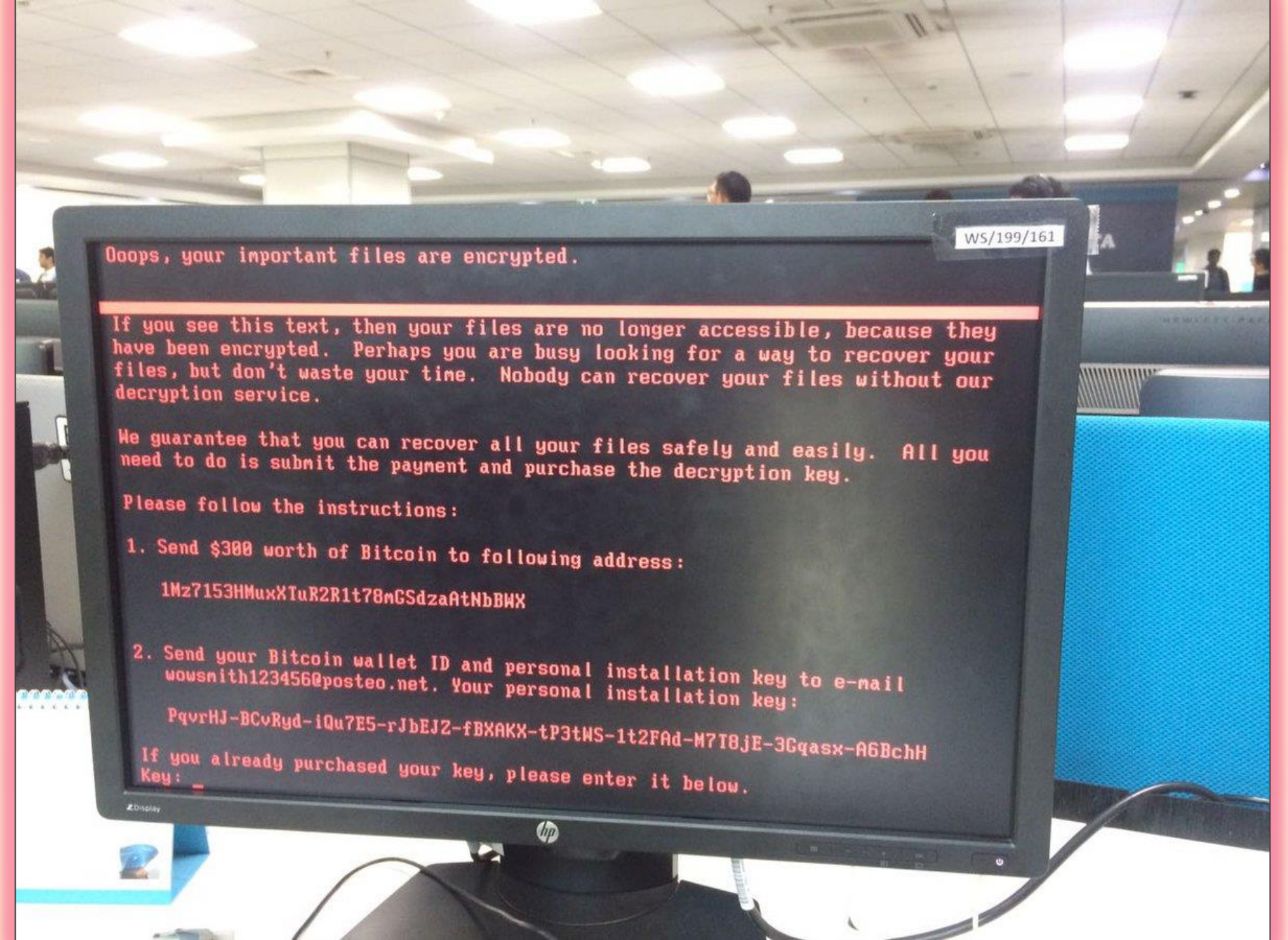
"A number of IT companies have really serious concerns. We don't want to see barriers put up," U.S. Deputy Secretary of Commerce Bruce Andrews told reporters during an October visit to Beijing. "Cross-border data flow has become increasingly important to trade and to companies in the way they operate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

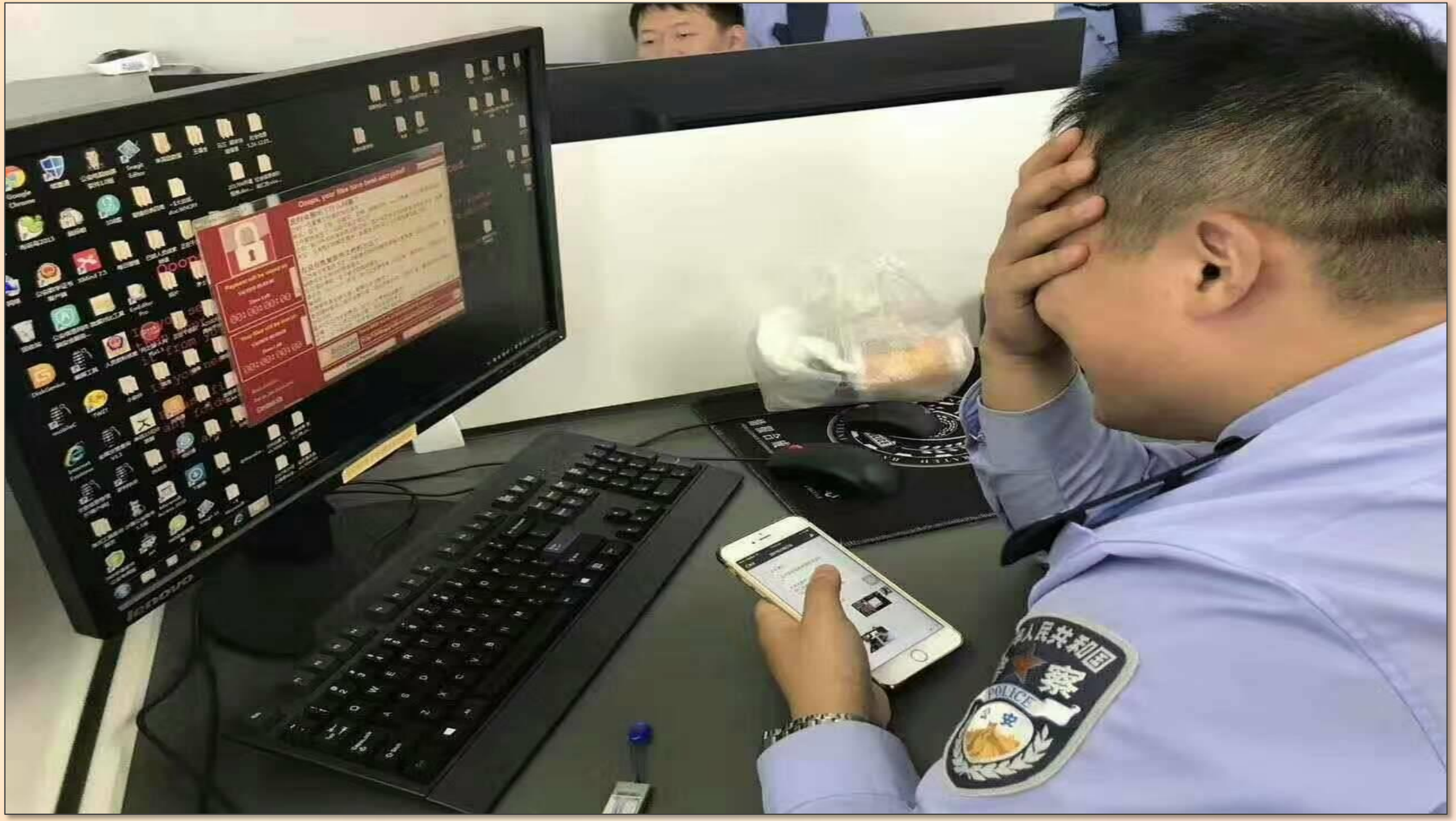
案例學習重點

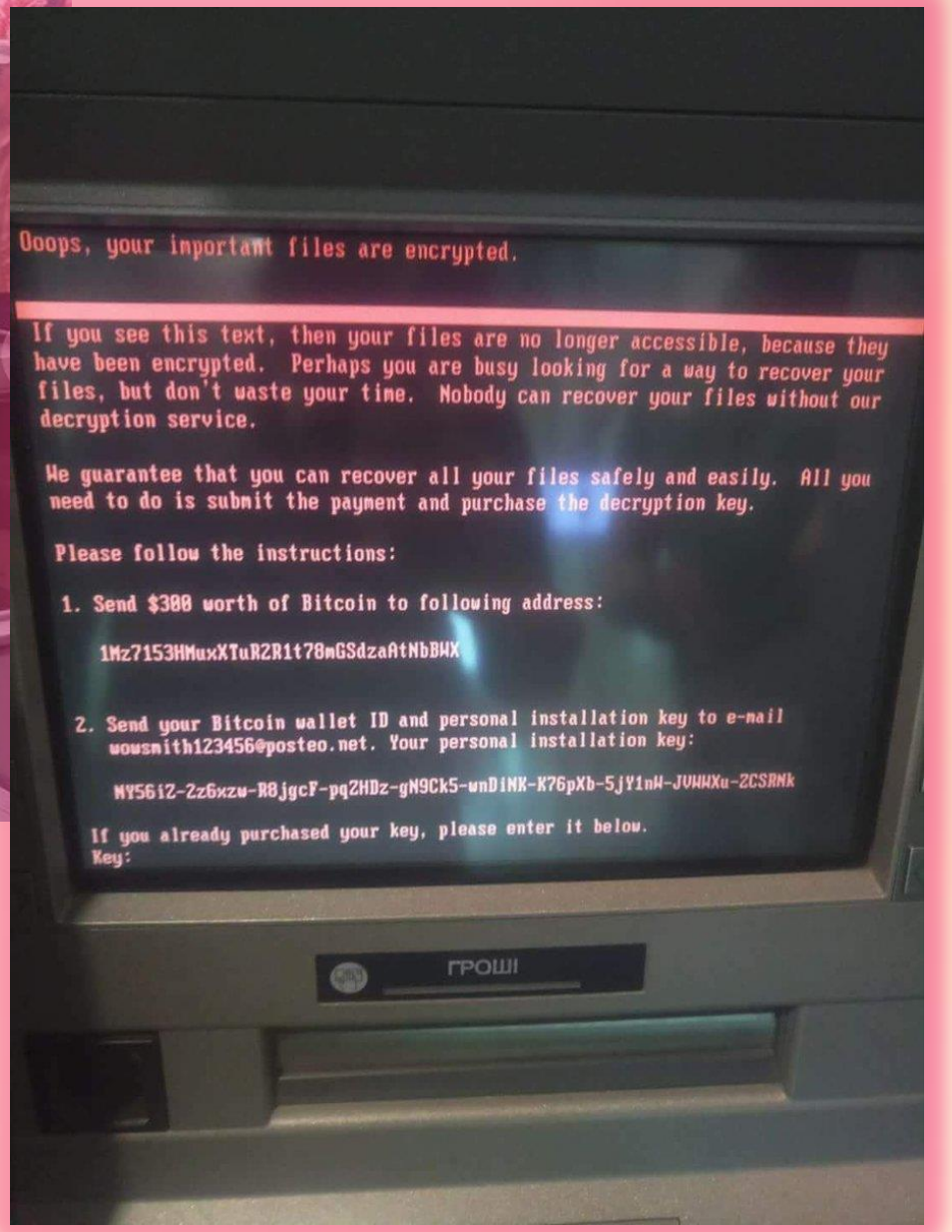
1. APK檔案，是Android的可執行檔案之一。點選 APK或apk 檔案，是危險的手機行為。
2. 不要安裝來路不明的遊戲程式，或是遊戲破解軟體。
3. 舊型Android手機(5.0以前的版本)，容易造成駭客入侵。
4. 重要資料備份，至少每2個月進行一次。
5. 某些App，疑似預藏惡意行為程式(過多的操作權限)。
6. **中國大陸政府，2017已經實施網路安全法，加強網路監控。**

惡意程式的近況報告 - 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-rJbEJZ-fBXAKX-tP3tWS-1t2FAd-M7T8jE-3Gqasx-A6BchH
If you already purchased your key, please enter it below.
Key: _

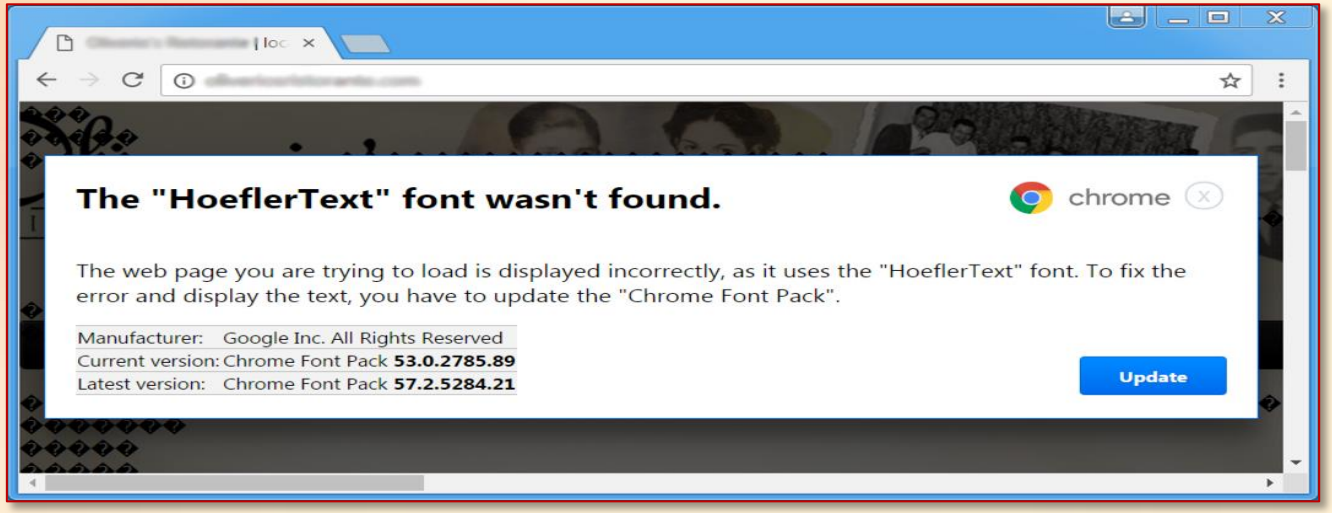


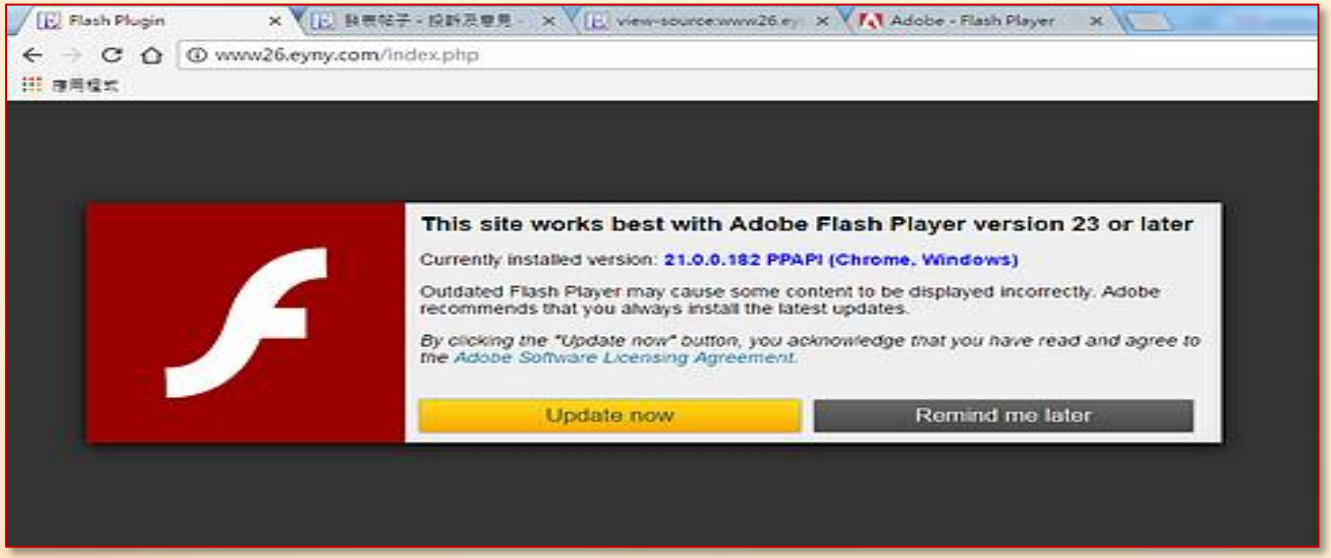


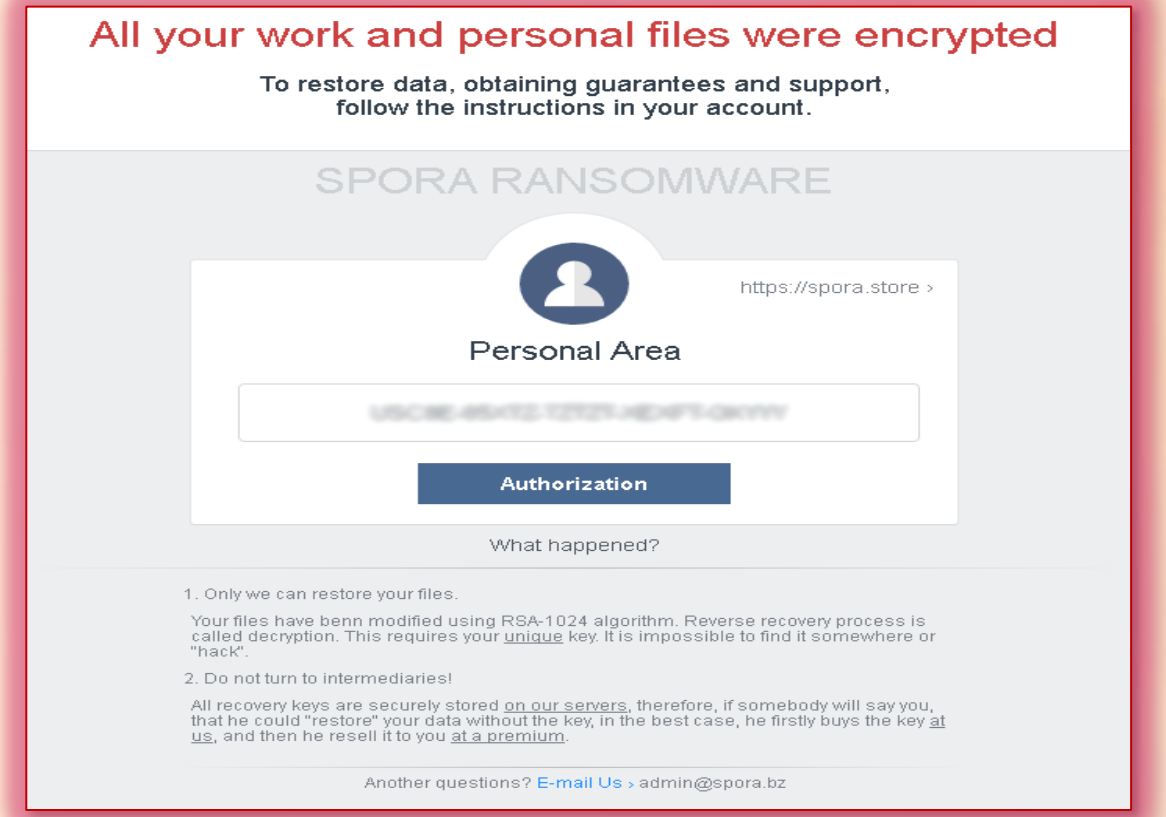
勒索病毒曾經使用的網路釣魚

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

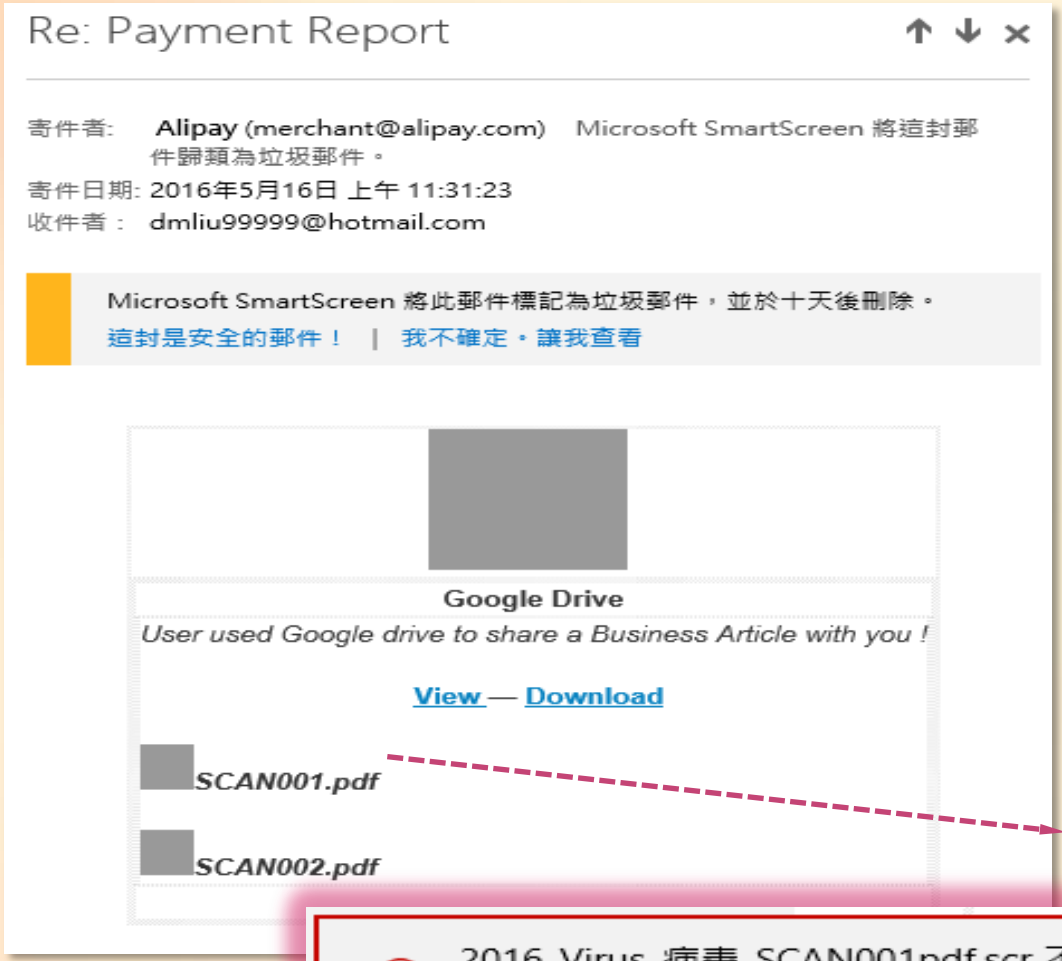
論壇網站遭入侵(網頁掛馬,假訊息)



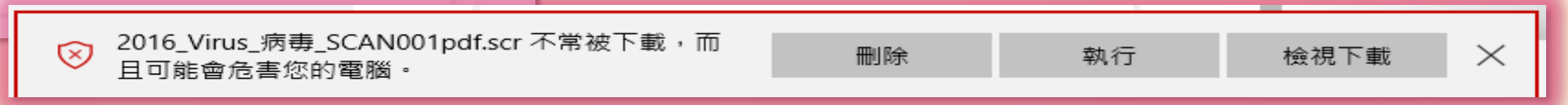




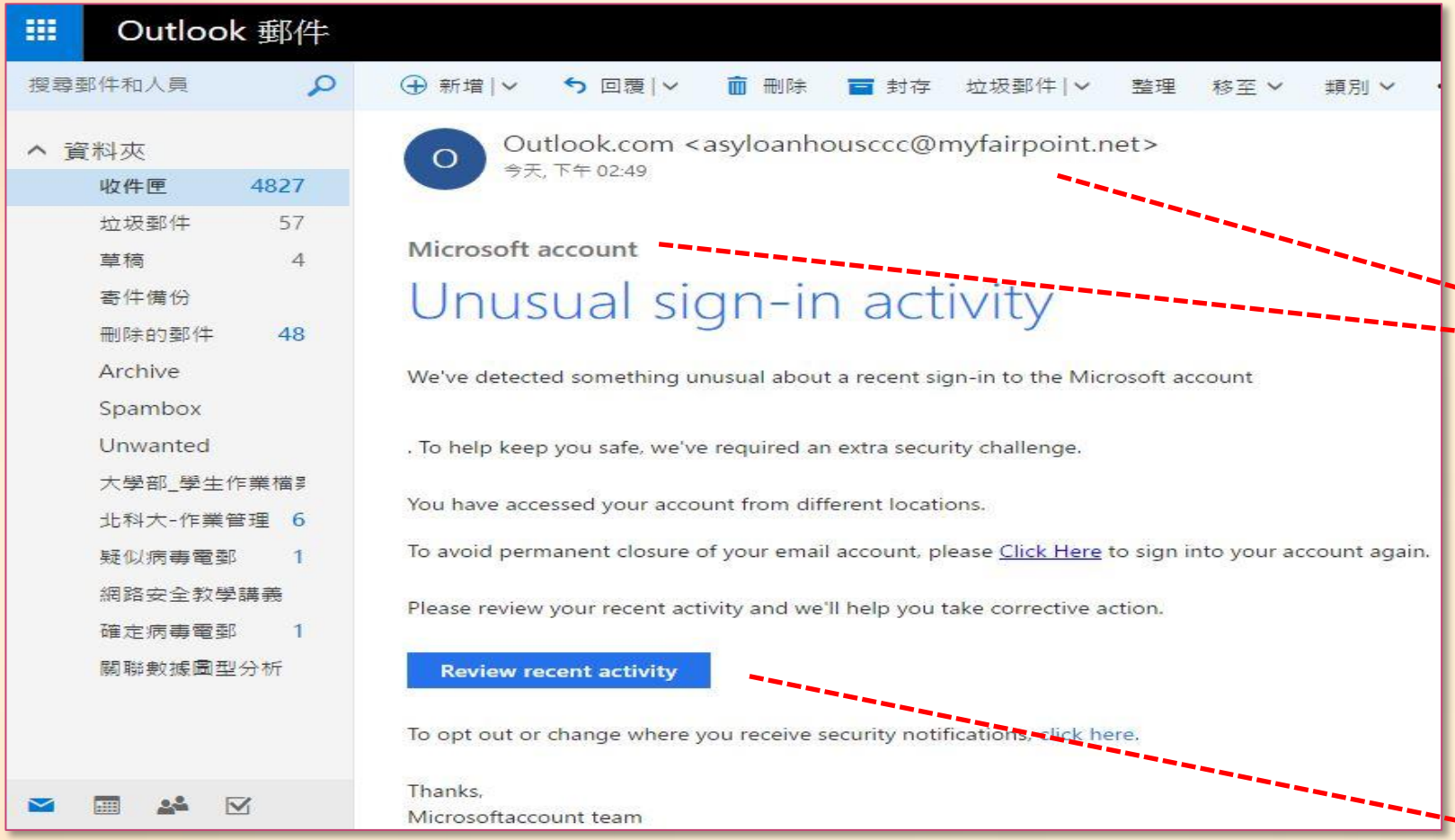
開啟電郵，電腦檔案被加密勒索



電子郵件，金融對帳單，提醒瀏覽(下載)
(這是惡意程式)



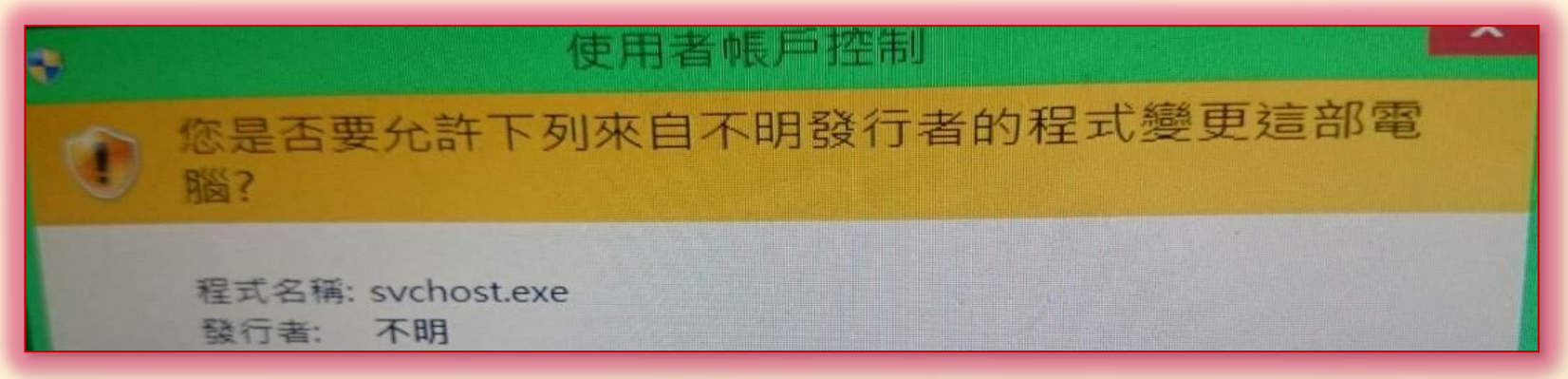
開啟電郵，電腦檔案被加密勒索

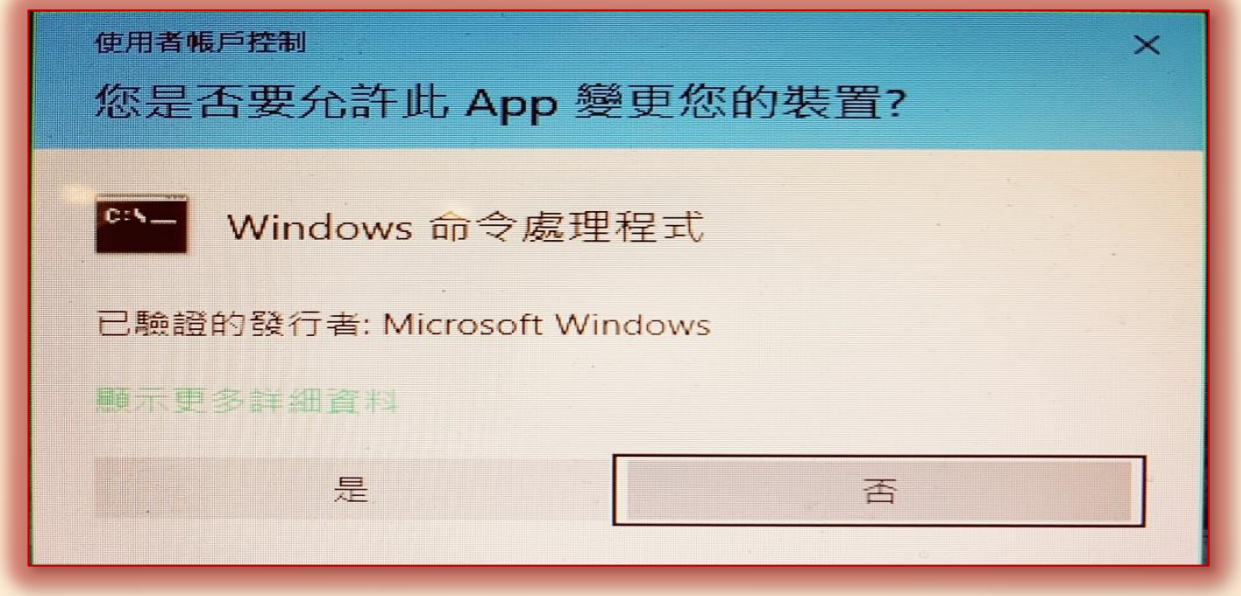


寄件人資訊，怪怪的！

駭客寄送的惡意程式

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

瞭解本機電腦的通訊現況

- netstat –an –p tcp (所有作業系統, Win, Android/Linux, Mac/iOS/Unix 均通用)
- netstat –ano –p tcp (Windows, 一般權限)
- netstat –abno –p tcp (Windows, 管理權限)

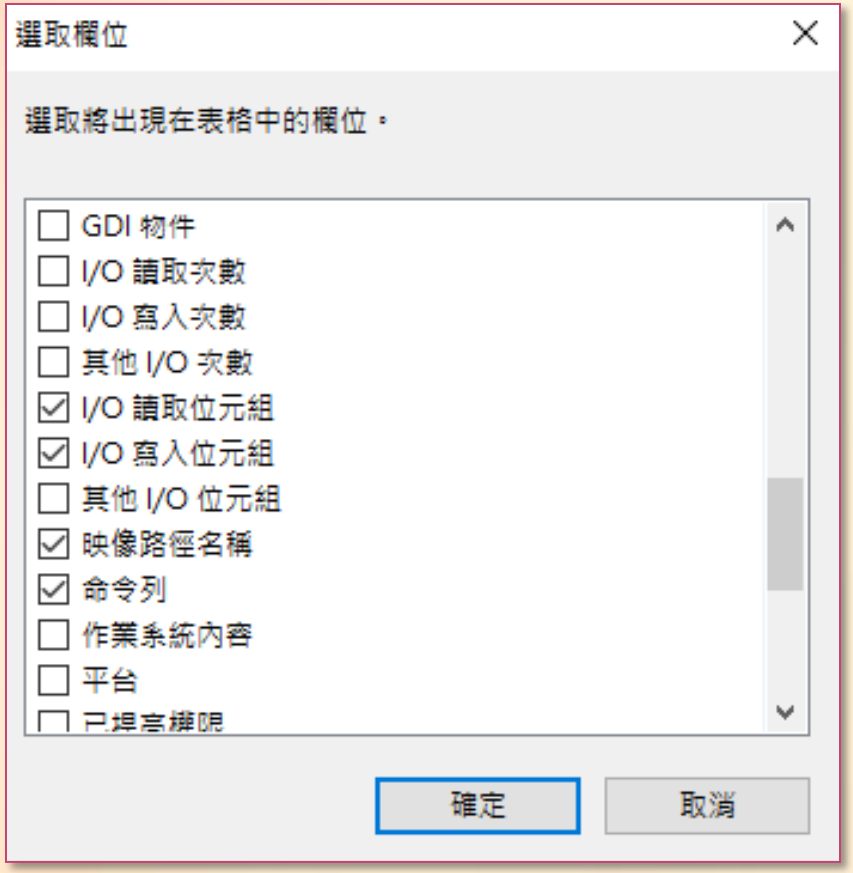
協定	本機位址	外部位址	狀態	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1132
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:902	0.0.0.0:0	LISTENING	4256
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING	4256
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING	5744
TCP	0.0.0.0:2383	0.0.0.0:0	LISTENING	5716
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	2052
TCP	0.0.0.0:27036	0.0.0.0:0	LISTENING	8928
TCP	0.0.0.0:31105	0.0.0.0:0	LISTENING	5132
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	876
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	2424
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1816
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	2960
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	96
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	4068
TCP	0.0.0.0:49675	0.0.0.0:0	LISTENING	992
TCP	10.0.200.15:139	0.0.0.0:0	LISTENING	4
TCP	10.10.1.10:139	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:1434	0.0.0.0:0	LISTENING	5744
TCP	127.0.0.1:5938	0.0.0.0:0	LISTENING	33520
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING	4304
TCP	127.0.0.1:27060	0.0.0.0:0	LISTENING	8928

TCP	10.0.200.15:139	0.0.0.0:0	LISTENING	4
TCP	10.10.1.10:139	0.0.0.0:0	LISTENING	4
TCP	127.0.0.1:1434	0.0.0.0:0	LISTENING	5744
TCP	127.0.0.1:5938	0.0.0.0:0	LISTENING	33520
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING	4304
TCP	127.0.0.1:27060	0.0.0.0:0	LISTENING	8928
TCP	192.168.0.6:51836	203.211.2.99:80	CLOSE_WAIT	16080
TCP	192.168.0.6:51837	104.18.25.243:80	CLOSE_WAIT	16080
TCP	192.168.0.6:51838	117.18.232.200:80	CLOSE_WAIT	16080
TCP	192.168.0.6:52485	203.211.2.155:80	CLOSE_WAIT	32252
TCP	192.168.0.6:52486	203.211.2.155:80	ESTABLISHED	32252
TCP	192.168.0.6:52497	203.211.2.155:80	CLOSE_WAIT	32252
TCP	192.168.0.6:52498	203.211.2.155:80	CLOSE_WAIT	32252
TCP	192.168.0.6:52499	203.211.2.155:80	CLOSE_WAIT	32252
TCP	192.168.0.6:52500	203.211.2.155:80	CLOSE_WAIT	32252
TCP	192.168.0.6:52504	203.211.2.155:80	CLOSE_WAIT	32252
TCP	192.168.0.6:52505	203.211.2.155:80	ESTABLISHED	32252
TCP	192.168.0.6:52506	203.211.2.168:80	ESTABLISHED	32252
TCP	192.168.0.6:52517	203.104.153.6:443	CLOSE_WAIT	32252
TCP	192.168.0.6:52522	203.104.142.91:443	CLOSE_WAIT	32252
TCP	192.168.72.1:139	0.0.0.0:0	LISTENING	4
TCP	192.168.75.1:139	0.0.0.0:0	LISTENING	4

Protocol	Description	Port	Note
ARP	Transfer NIC-MAC Address and IP Address on Local Area Network(LAN). Before NIC sent TCP/UDP/ICMP packet, it will send ARP Packet to ask MAC-Address.	No any Port Number	Only LAN
DNS	Transfer Host Name and IP Address on Internet. Especially, it is the pre-behavior about computer browse the Web or send/receive email.	UDP-53 Normal TCP-53 * (ISP Only)	UPD-53 often
HTTP	At first, it is used for Web page browsing. Now a day, it is used for many Internet service Interface such like Webmail, Facebook, Twitter, …	TCP-80, TCP-8080, TCP-8000, TCP-10000	Very often
HTTPS	Secure web browsing, HTTP+SSL, Web bank or email login would use this.	TCP-443 (Encryption)	Often
SMTP	Sending email. Now a day, users send email by Web-mail so that SMTP is seldom used by end users. However, mail servers still use SMTP to send email.	TCP-25 (Default, no password)	Mail Server Very often
IMAP	Receiving email. This protocol will be more popular than POP3 in cyberspace.	TCP-143 (user-ID, password)	Mail Server Very often
POP3	Receiving email. As same as SMTP, it is rare in end users because Web-mail. Mail servers still use POP3 to receive email.	TCP-110 (user-ID, password)	Mail Server Very often
FTP	Files Transfer Protocol. This protocol also would be replaced by P2P or Cloud Storage (Web, HTTP or HTTPS) but online games still use this to update Apps.	TCP-21 (TCP-20) (user-ID, password)	Online Game Very often
Telnet	It is telecomm command with plain text mode. Mostly it is used for Firewall or Wireless Access Point device by maintenance engineers.	TCP-23 (user-ID, password)	Rare (Night-Fatal)
CIFS	It is used for Network Neighborhood which provides the following purpose, (1) Login/Logout (2) Shared Resource (3) Printing Service.	TCP-139, TCP-445 UDP-135~UDP-138	Very often (WAN-Fatal)
MS-SQL	Microsoft SQL Database Server Service.	TCP-1433 UDP-1434	Rare (DBs – Often)
Remote Desktop	Windows Terminal Service. It provides remote desktop service same as Citrix RDP. Mostly it is used for Servers maintenances from WAN/LAN.	TCP-3389 (user-ID, password)	Rare (Night-Fatal)

加密勒索軟體的執行徵兆

名稱	PID	狀態	使用者名稱	工作階段	CPU	I/O 讀取位元組	I/O 寫入位元組



I/O讀取位元組, 與 I/O寫入位元組
同時會「同步增加」只有下列狀況:
(1)備份或複製檔案
(2) Libpcap 錄製封包 (Wireshark)
(3) 磁碟檔案的資料抹除
(4) 加密勒索軟體 !!!

緩衝區資料溢出攻擊的徵兆現象

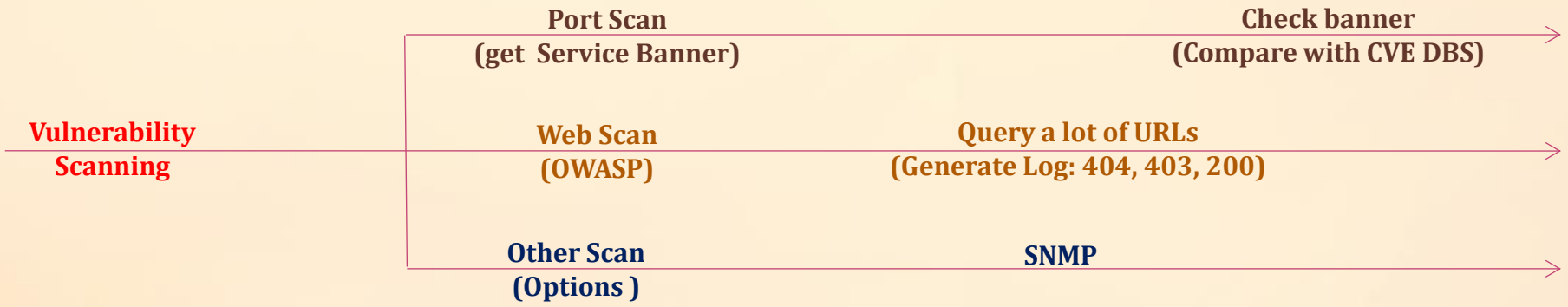
- 應用程式或網路服務的異常停止
  - 異常停止後, 出現網路服務(木馬通訊)
  - 異常停止前, 出現網路服務(後門通訊)
  - 出現未知帳號, 或是無名稱帳號(S-1-xxxx-…)
  - Unknown User-ID(UID) or Security-ID (SID)
  - 出現未知檔案或是程序(Process)

緩衝區資料溢出攻擊的紀錄分析

- 應用程式或網路服務的異常停止(EventLog)
- 網路服務紀錄分析 (netstat, Wireshark)
- 未知帳號UID或SID (net user , EventLog)
- 出現未知檔案或是程序(dir /R 或 dir /S 或 tasklist /svc)

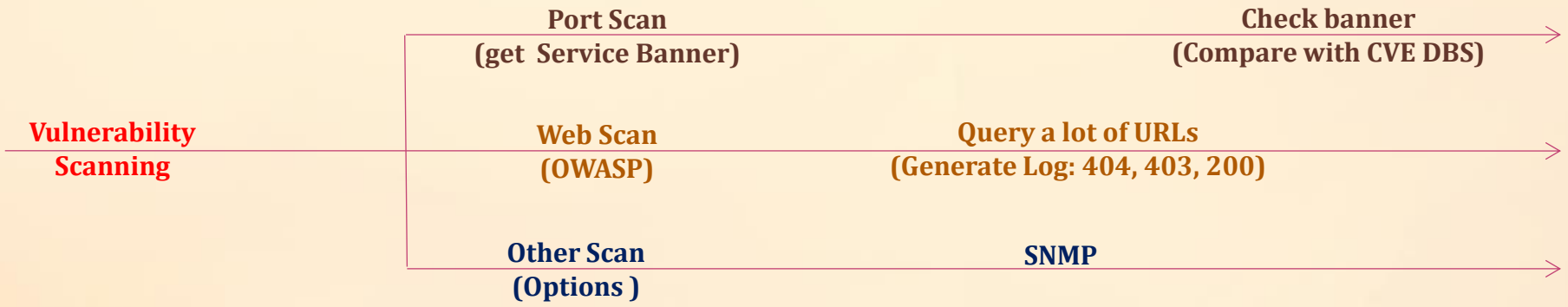
網路弱點掃描的徵兆現象

- 網路行為現象
  - Port Scan with banner
  - Web Scan for OWASP Top-10
  - Scan other Network Service



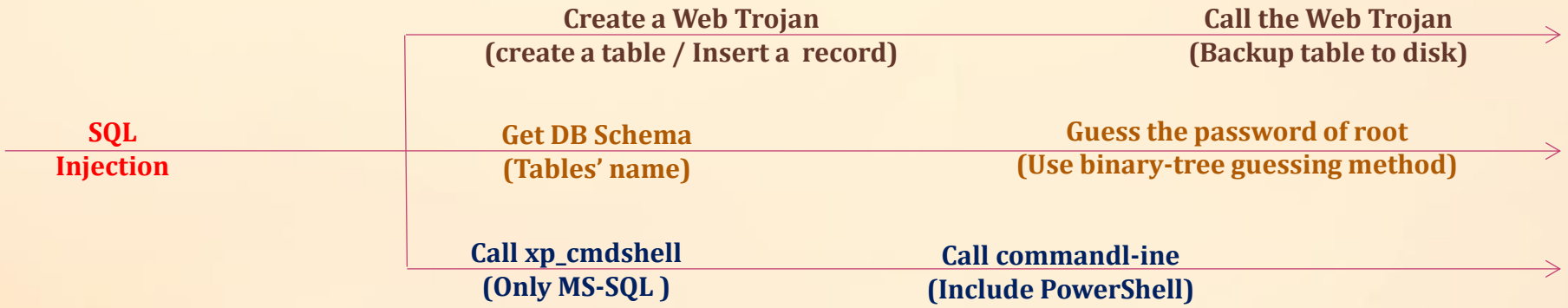
網站弱點掃描的徵兆現象

- HTTP/HTTPS 服務出現大量 404,403
- Few 200 from same Source-IP address
- No Application/Service would crash
- No account/file/process been touched



網站SQL-Injection的徵兆現象

- HTTP/HTTPS 服務出現特定IP的 500
- Few 200 from same Source-IP address
- No Application/Service would crash
- Maybe account/file/process be created



電腦的常用檢查步驟 - 1

尋找正在通訊程式 (netstat –no)

忽略本機連線

(127.0.0.1 與 本地-遠端 相同 IP 位址)

尋找異常程式的程序代碼 (Process ID, PID)

根據 PID 尋找 程式名稱 (工作管理員)

要先啟動 工作管理員 的 所有使用者的處理程序

要勾選 處理程序->檢視->選擇欄位->PID

根據程式名稱 尋找 目錄位置 (dir xxx.exe /AS /AH /S /TC)

要注意 檔案建立時間(File Create Time)

建立時間做為參考, 還要參酌其他相關資訊

尋找相同時間建立的所有檔案 (尋找 *.exe;*.com;*.dll;*.cmd;*.bat ...)

使用檔案尋找的功能, 要注意更改相關設定

再用相同檔案名稱去註冊表找相關機碼資料 (Registry)

電腦的常用檢查步驟 - 2

根據程式屬性 尋找 異常程式名稱 (dir *.exe;*.bat;*.cmd /AS /AH /S /TC)

要注意 檔案建立時間(File Create Time)

建立時間做為參考, 還要參酌其他相關資訊

根據程式名稱 尋找 PID (工作管理員)

要先啟動 工作管理員 的 所有使用者的處理程序

要勾選 處理程序->檢視->選擇欄位->PID

根據 PID 尋找 通訊埠編號 (netstat –ano)

忽略本機連線

(127.0.0.1 與 本地-遠端 相同 IP 位址)

尋找異常程式的通訊連接埠編號

尋找相同時間建立的所有檔案 (尋找 *.exe;*.com;*.dll;*.cmd;*.bat ...)

使用檔案尋找的功能, 要注意更改相關設定

再用相同檔案名稱去註冊表找相關機碼資料 (Registry)

電腦的常用檢查步驟 - 3

在USB設備，尋找 異常目錄名稱 (dir /AS /AH /TC)

要注意 檔案建立時間(File Create Time)	建立時間做為參考, 還要參酌其他相關資訊

在USB設備，尋找 異常程式名稱 (dir /TC)

要先停止 檔案總管 程序 (explorer.exe)	使用工作管理員停止，或是 taskkill 指令 來停止

比較前後兩步驟相同名稱的目錄與檔案

真正的資料目錄是隱藏目錄	**隱藏目錄 相同名稱的exe檔案 是 病毒**

先刪除 xxxxx.exe 檔案 ，再恢復 xxxxx 目錄屬性

檢查 System32 以下目錄有無 隱藏DLL檔案	要檢查 System32 下的目錄檔案隱藏情況

常用電腦設備的相關指令與工具

- 現在執行程式情況 → 工作管理員, tasklist, top
- 現在網路芳鄰連線 → net use 指令
- Windows登入帳號清單 → net user 指令
- Windows 磁碟分享現況 → net share 指令
- Windows 服務執行現況 → sc 指令
- Windows 服務啟動與終止 → net start (stop) 服務名稱
- 網路卡與網路位址現況 → ipconfig, ifconfig 指令
- 網路對外連線路徑 → tracert, traceroute 指令
- 顯示網路芳鄰資料 → nbtstat 指令
- 測試網路連接線路 → ping 指令

惡意程式 範例檔案分析實作

分析人員: Diamond Liu (Tei-Min Liu, 劉得民)
Contact : 0985-604-145, dmliu99999@hotmail.com

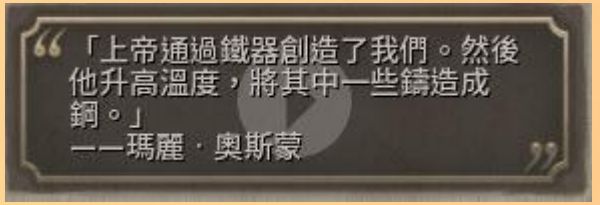
Q&A

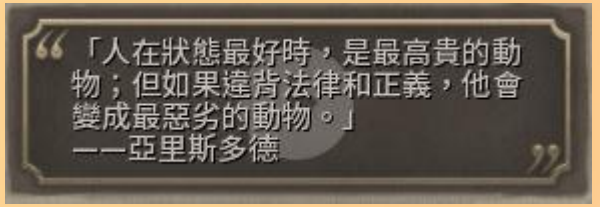
Diamond 資訊安全規則

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 (Tei-Min Liu, 劉得民) 0985-604-145
- Email : dmliu99999@hotmail.com

感謝 www.NSPACERT.org, 刑事局偵九大隊 陳詰昌, NCC 電信警察隊 莊明雄, 台北市警察局 謝其謹 協助提供資料

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