個案分析-

Android 智慧型裝置的 APP 惡意程式事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/7

I. 事件簡介

1. 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。
2. 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。
3. 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。
4. 檢測方式透過 Android 模擬器及實體手機進行測試。

II. 事件檢測

1. 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。
2. 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。

3. 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。
    1. 主要有能夠「讀取手機狀態、簡訊 SMS 所有功能、GPS 定位、聯絡人

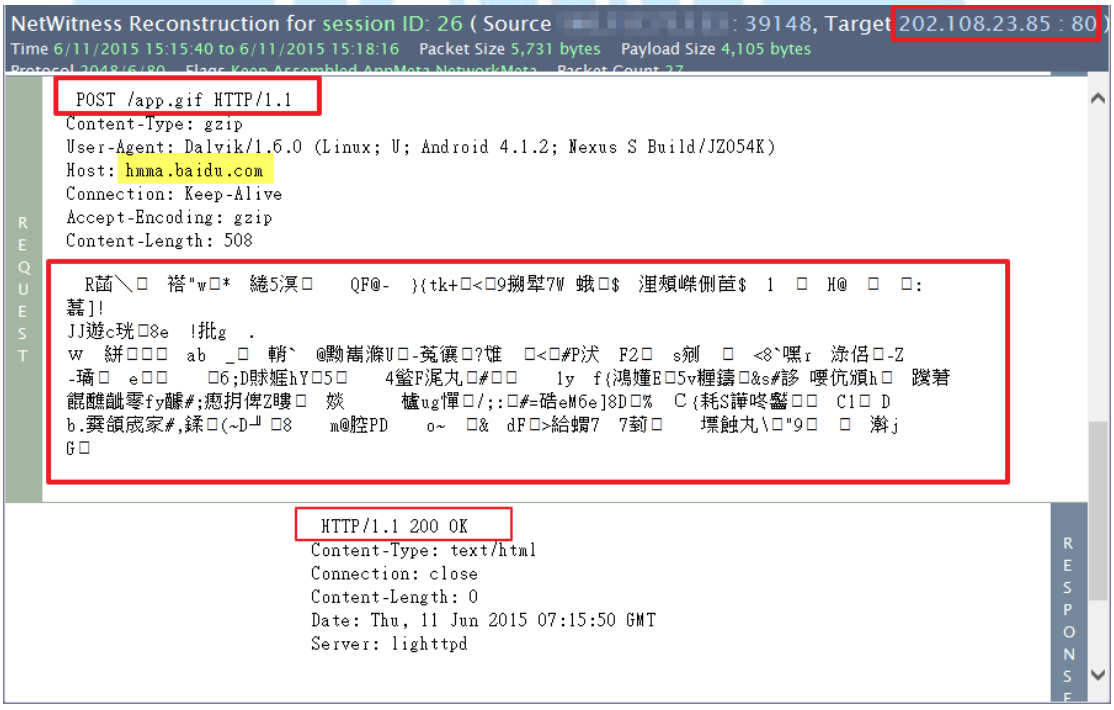
通話紀錄、SD 卡內容、網路狀態及啟動執行等。」

4. 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。

5. 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。
6. 然而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。
7. 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。

8. 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 。



9. 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。

10. 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。

11. 透過 SSH 連入手機，並且輸入 netstat 指令觀察可疑的 port，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
```

12. 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。

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

13. 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其他人受害，不可不防。

Interesting calls

Calls APIs that provide access to information about the telephony services on the device. Applications can use such methods to determine telephony services and states, as well as to access some types of subscriber information.

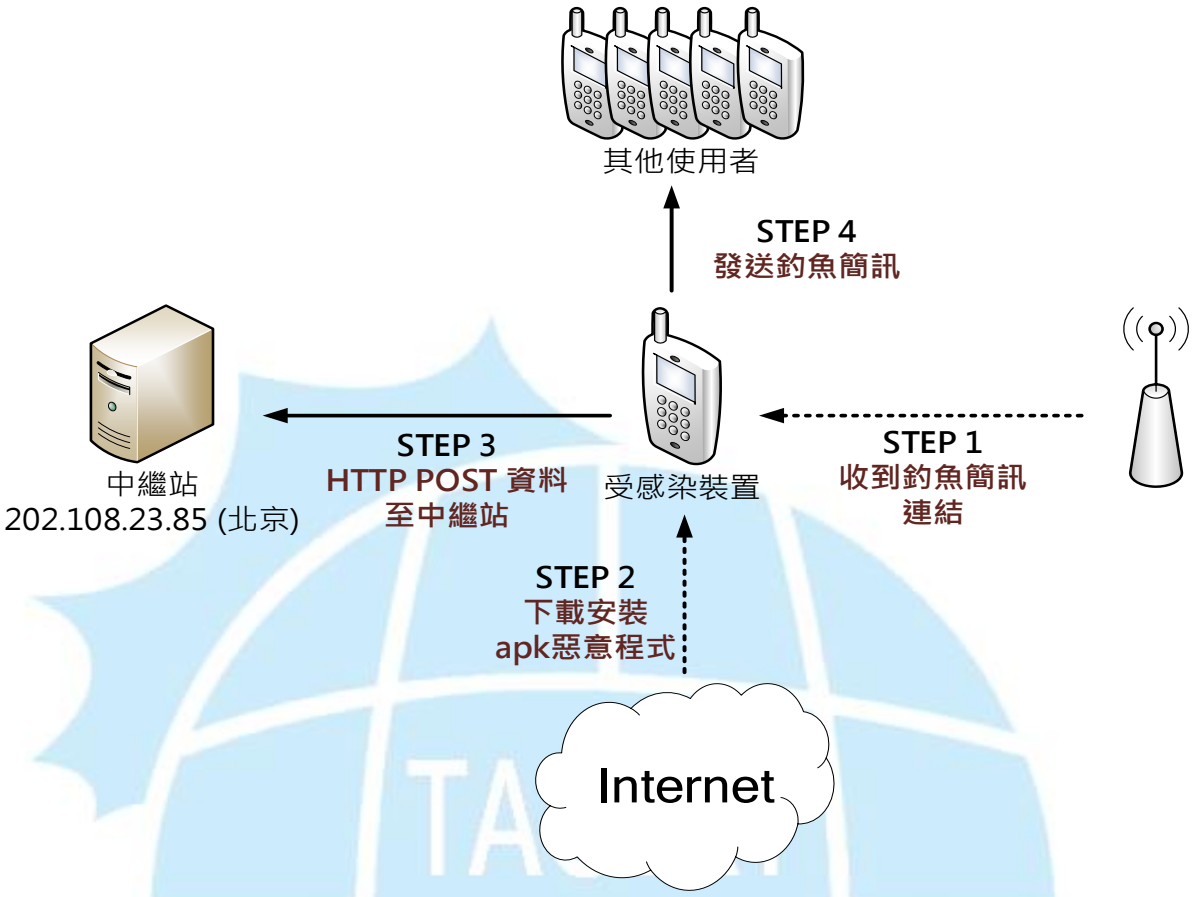
Calls APIs that manage SMS operations such as sending data, text, and pdu SMS messages.

14. 惡意程式能夠存取的權限如下，幾乎掌控所有權限。

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*)

III. 網路架構圖



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。

IV. 建議與總結

1. 此事件的惡意程式通常透過手機簡訊方式感染
2. 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。
3. 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。
4. 使用者開啟安裝的 APP 後無法正常操作該軟體「PhoneContent」。

5. 感染裝置可能會向通訊錄聯絡人發送釣魚簡訊。
6. 此時就算將 APP 移除，但手機的個資已經被回傳竊取。
7. 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。
8. 建議安裝手機用的防毒軟體，大多病毒都能被偵測阻擋。
9. 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。