個案分析-

常見的手機簡訊病毒詐騙事件事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/08

I. 事件簡介

A. 近年來智慧型手機的簡訊詐騙越來越多樣化，從早期的電話通知中獎或分期轉帳詐騙，進化成智慧型手機的簡訊詐騙，駭客主要利用手機網路方式誘使用戶下載安裝惡意木馬程式，以控制裝置的權限進行財務盜竊，然大多用戶無資訊安全觀念而容易受害。

B. 目前詐騙主流多為 Android 系統的智慧型手機，因為 APP 的安裝限制較少，手機取得 Root 的方式也較為容易，第三方的 ROM 或 APP 安裝檔網路上都能輕易下載安裝，但往往成為資訊安全的漏洞。

C. 這次事件主要將常見的詐騙簡訊實地安裝測試，側錄其封包並觀察可能產生的系統網路行為。

1. 事件 A：

今年 3 月底手機收到 SMS 文字簡訊告知用戶說，「貴用戶有申請網路繳費通知，非本人操作請依照指示點擊所附連結進行取消。」連結為 http://goo.gl/UB9zBa，該號碼為中華電信的門號 0921124XXX。

左圖：事件 A

2. 事件 B：

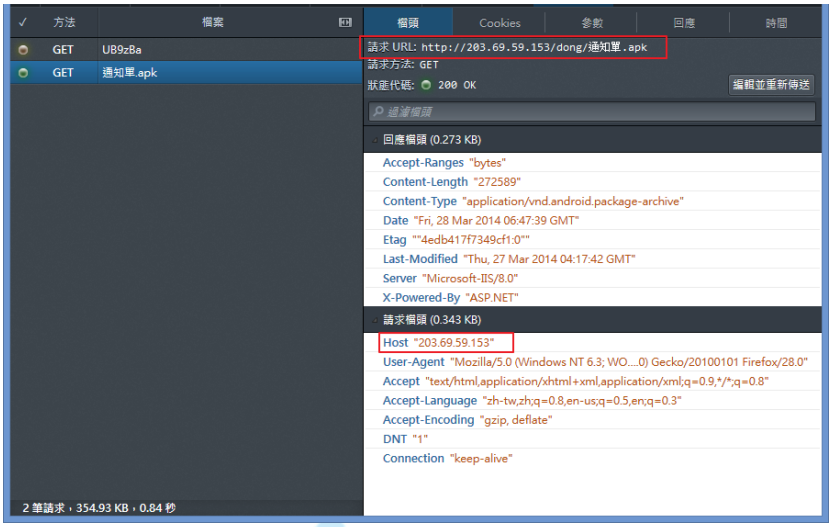
今年 4 月初手機收到 SMS 文字簡訊告知用戶說，「您的快遞通知，收件簽收憑證。」連結為 http://goo.gl/gj1LSq，該號碼為中華電信的門號 0988220XXX。

左圖：事件 B

3. 一般對於較沒網路資訊安全概念的使用者就容易依照指示開啟連結，就如同早期 ATM 取消分期轉帳的詐欺手法，利用人性對於害怕金錢損失的弱點進行攻擊。
4. 這類詐騙簡訊通常有個共同現象，就是會附帶惡意連結並要求用戶下載憑證並安裝。
5. 另外連結位址習慣使用 google 或其他的縮短址將真正網址進行遮蔽(http://goo.gl/)，讓使用者不容易察覺真正網址，還能透過 google 的縮短址管理介面得知有多少用戶點擊過，以方便駭客統計。

II. 事件 A 測試

1. 在事件 A，我們透過 Android 的模擬器 Genymotion 進行測試，使用 OS 4.3 的版本。開啟該連結後會轉到真正的網址 IP「203.69.59.153」，並下載一個名為『通知單.apk』的 Andorid APP 安裝檔。

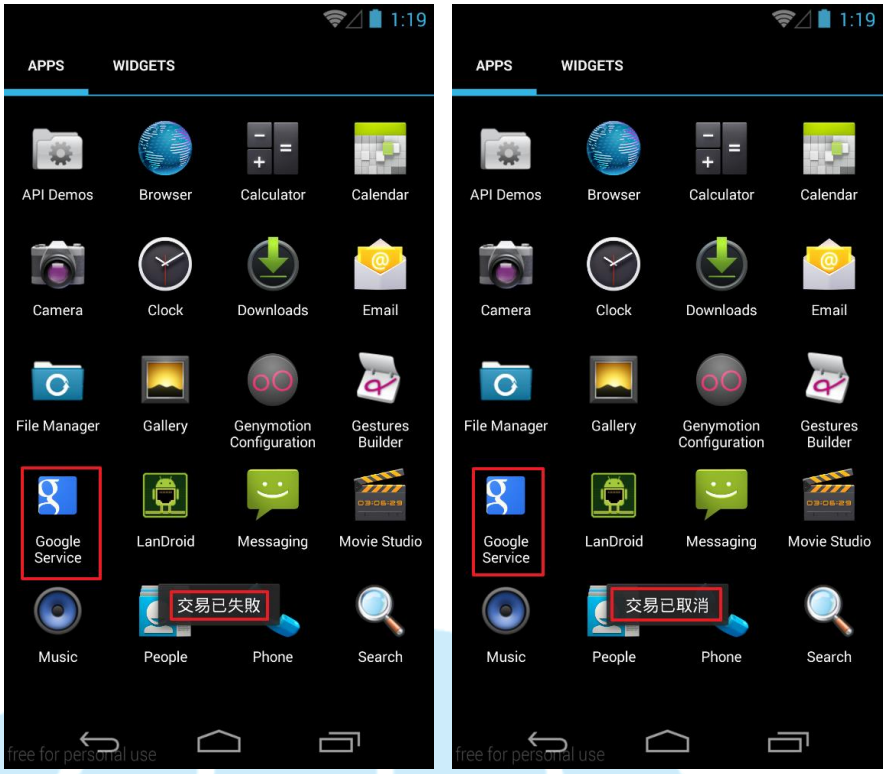


2. 對方主機 IP 位址經過調查發現是中華電信的固定制 IP，研判可能被駭客入侵植入後門程式當作跳板。

3. 實地安裝該 APK 檔之後，出現一個介面顯示是否要確認或取消此網上支付交易的選項。

4. 若選擇「確認交易」則會出現「交易已失敗」，若「取消交易」則會出現「交易已取消」的訊息。然而無論是選擇哪個項目，後門程式已成功植入系統再背景執行，顯示字串只是誤導使用者安裝認為失敗。

   a. 我們注意到該惡意程式會仿造 Google 的 LOGO，且 APP 名稱為「Google Service」，讓使用者誤以為是系統內建程式。

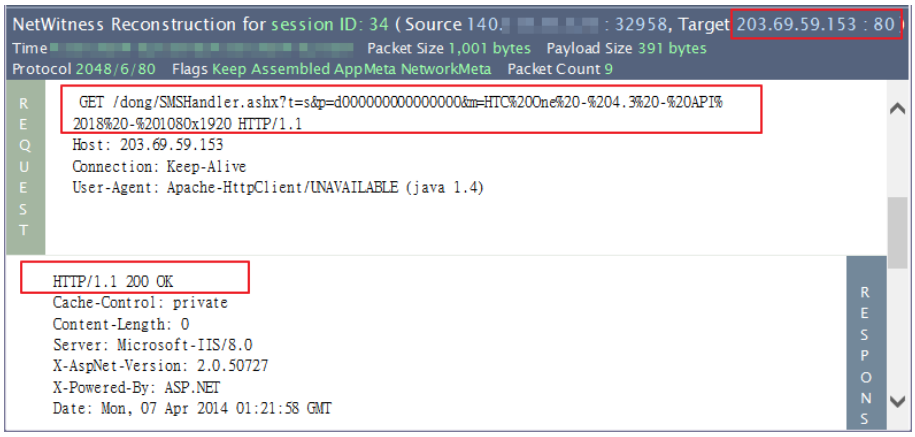


左圖：選擇確認交易　　右圖：選擇取消交易

5. 檢查側錄的封包資訊發現，該 Google Service 的 APP 會持續向 IP 203.69.59.153 進行連線，而該 IP 經由檢查發現是 HINET 的固定制 IP，而該主機有開啟遠端桌面的服務，研判是被駭客入侵當作中繼站跳板。

a. 從封包得知惡意程式主要是透過 HTTP GET 不斷向中繼站傳送感染主機資訊，主要是以「GET /dong/ SMSHandler.ashx?xxx…」將資訊以參數方式送出，從控制檔 SMSHandler.ashx 可以推斷惡意程式能夠存取簡訊的控制權限。

b. 下圖封包分析可以看出參數中帶有手機型號「HTC ONE」、OS 版本為 4.3 及解析度「1080x1920」等資訊。故手機內部的簡訊內容應該就是以此方式被駭客竊取，以控制受害人的設備。



6. 透過 APKTOOL 反組譯工具去解析「通知單.apk」後得到 AndroidManifest.xml，裡面宣告了該 APP 能夠使用的權限，其中包括了「讀取手機狀態、發送簡訊、讀取簡訊、編寫簡訊、接收簡訊、INTERNET 啟用、撥打電話、讀取聯絡人資訊以及記憶卡寫入權限」，這些權限嚴重影響使用者的個資安全，甚至會有金錢損失。

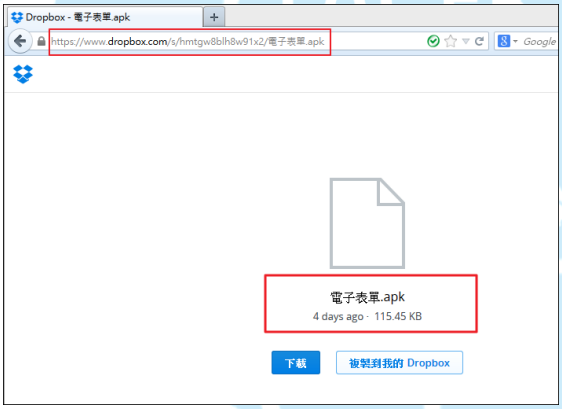
```
<?xml version="1.0" encoding="UTF-8"?>
- <manifest xmlns:android="http://schemas.android.com/apk/res/android"
  package="com.example.google.services" android:versionName="1.0"
  android:versionCode="1">
      <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
      <uses-permission android:name="android.permission.SEND_SMS"/>
      <uses-permission android:name="android.permission.READ_SMS"/>
      <uses-permission android:name="android.permission.WRITE_SMS"/>
      <uses-permission android:name="android.permission.RECEIVE_SMS"/>
      <uses-permission android:name="android.permission.INTERNET"/>
      <uses-permission android:name="android.permission.CALL_PHONE"/>
      <uses-permission android:name="android.permission.READ_CONTACTS"/>
      <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    + <application android:allowBackup="true" android:debuggable="true"
      android:icon="@drawable/ic_launcher" android:label="@string/app_name"
      android:theme="@style/AppTheme">
  </manifest>
```

7. 從 Virustotal 檢測得知病毒偵測比率為 9/51，主要的惡意行為是完全控制 SMS 簡訊功能，同樣檔案的其他別名有「oldboot.b.apk、通知單 6.apk、vti-rescan、通知單.apk、1.apk」。

防毒	結果	更新
Ad-Aware	Android.Trojan.Smssend.G	20140413
AegisLab	SmsSend	20140413
BitDefender	Android.Trojan.Smssend.G	20140413
Emsisoft	Android.Trojan.Smssend.G (B)	20140413
F-Secure	Trojan:Android/SmsSend.ET	20140413
GData	Android.Trojan.Smssend.G	20140413
Kaspersky	HEUR:Trojan-SMS.AndroidOS.Agent.je	20140413
MicroWorld-eScan	Android.Trojan.Smssend.G	20140413
Qihoo-360	Trojan.Generic	20140413

III. 事件 B 測試

1. 在事件 B 中，開啟簡訊連結 http://goo.gl/gj1LSq 後會轉址至 Dropbox 的免費空間，並出現檔案「電子表單.apk」的下載頁面，這些免費空間儼然容易成為駭客存放惡意程式的一個工具。
   a. 使用 Dropbox 的好處是容易申請，而且檔案可以直接分享連結供人下載而無須登入，就算被人檢舉關閉也能立刻重新再開立帳號，所以駭客很喜歡使用這類免費空間。

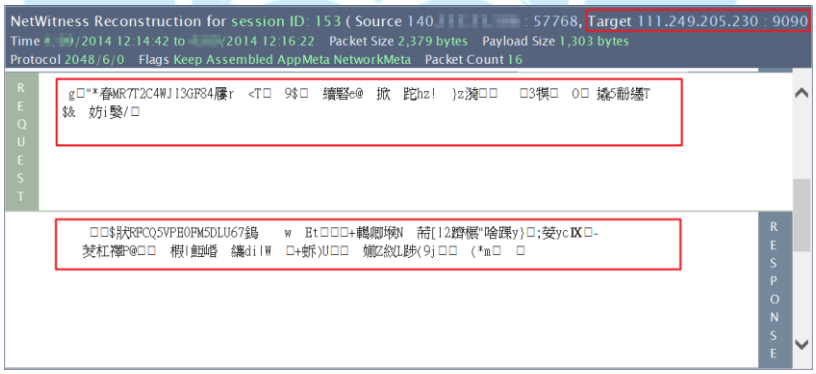


2. 實地將該 APK 檔案用 Android 模擬器安裝，發現此惡意程式會檢測所安裝的作業環境，若是模擬器的作業系統則無法正常安裝。因此我們改用實體智慧手機進行安裝測試，結果順利安裝成功，此次使用的手機型號為 Google Nexus S 的 Andorid OS 4.2 版本。安裝完後 APP 的名稱為「safeguard」且 LOGO 是 Google 內建的圖案。
3. 我們透過 apktool 的反組譯工具去解析，發現該惡意程式 APK 有做過特殊防護，故無法成功反組譯成功。但還是能從安裝過程中知道，該

APP 主要能夠存取的權限有「撥打電話、簡訊所有權、通話錄音、通話紀錄及聯絡人、記憶卡存取、網路控制權、藍芽控制及啟動執行和控制其他應用程式」，幾乎所有重要功能都能被掌控，相當危險。

4. 檢查側錄的封包資訊發現，該「safeguard」的 APP 會連到 HINET 的兩個 IP 位址，分別是「61.228.129.11」和「111.249.205.230」，經過 DNS 反解析得知為「XXX.dynamic.hinet.net」，此為 HINET 的動態位址。研判應該為被入侵的受害主機中繼站。

   a. 傳送的封包內容皆為加密過的內容，且都送至目的端的固定 Port 9090。



5. 從 Virustotal 檢測得知病毒偵測比率為 28/53，主要功能幾乎能完全存取手機狀態，同樣檔案的其他別名有「eForm.apk、file-6821568_apk、電子表單.apk、ultimate.safeguard.apk」等。

防毒	結果	更新
AVG	Android/Deng.WW	20140712
Ad-Aware	Android.Trojan.SMSSend.ND	20140712
AhnLab-V3	Android-Malicious/KorTalk	20140711
AntiVir	Android/Agent.ack.5	20140712
Avast	Android:RuSMS-AH [Trj]	20140712
Baidu-International	Trojan.AndroidOS.SMS.aTP	20140712
BitDefender	Android.Trojan.SMSSend.ND	20140712
CAT-QuickHeal	Android.Agent.GQ	20140711
Commtouch	AndroidOS/GenBl.7B4BC615!Olympus	20140712
Comodo	UnclassifiedMalware	20140712

IV. 事件 A 與 B 的比較

1. 相同點

a. 事件 A 和事件 B 都是透過手機簡訊進行的一種釣魚郵件攻擊，透過相關訊息內容去誘使使用者開啟網路連結並下載惡意程式 APK 檔並安裝。

b. 兩事件相同之處就是惡意程式 APP 傳送出去的資料都經過加密，且

APP 都能存取手機重要的權限，例如簡訊、記憶卡、聯絡人等資訊。

2. 相異點

a. 事件 A 和事件 B 最大的差異點是事件 B 的惡意程式經過改良，已經能夠偵測安裝的系統環境是否為虛擬機，一旦為虛擬機則無法安裝成功，確保能竊取真正手機的資訊。

b. 在事件 A 駭客可能透過遠端桌面入侵 HINET 的一個固定 IP 主機後，開啟 Web Server 功能提供下載木馬病毒，很容易就被舉報撤除。然而事件 B 中，駭客改用免費的網路空間存放惡意程式，相對來說比較難被撤除，也能讓惡意程式存活較久。

c. 事件 B 的 APK 檔使用防護機制因此無法直接用 apktool 進行反組譯解析，然而事件 A 的就能輕易解析。

d. 事件 B 的惡意程式多了事件 A 沒有的權限，包含「通話錄音功能、更改音效權限、控制讀取 WIFI 狀態、讀取寫入通話紀錄、藍芽控制、攔截且竄改播出的號碼、檢索正在執行的應用程式、掛卸載系統的程序、關閉背景其他程式」，全都是進階權限功能，因此相對非常危險。

3. 正常簡訊誤判為詐騙

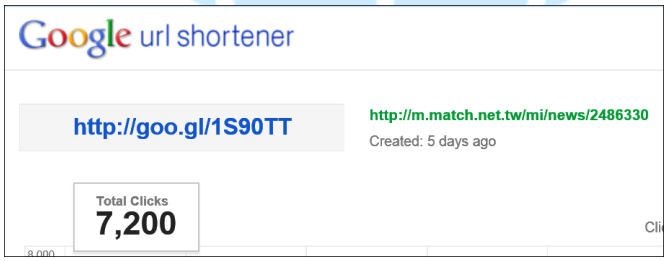
a. 由於這類型的詐騙簡訊已經非常氾濫，導致許多人看到這樣的簡訊就直接認定是詐騙，更有媒體指出凡是縮短址 http://goo.gl/ 開頭的都是惡意網址，其實這只是 Google 提供的免費縮短址服務，依據用途不同會有相異結果。

b. 這則短訊則被各大媒體直接報導為詐騙簡訊，其實為某電信業者所發送的新聞推播簡訊，其網址 http://goo.gl/1S90TT 的轉址其實為 http://m.match.net.tw/pc/news/2486330。

圖、此為翻拍網路上的截圖

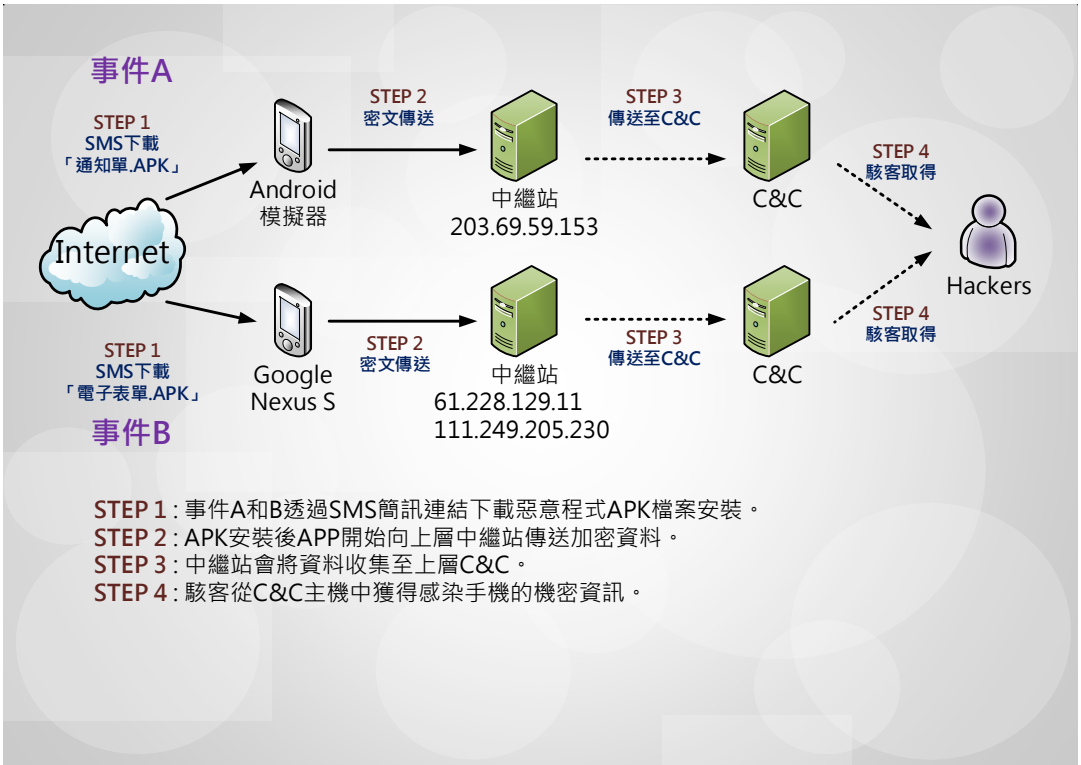
圖、縮短址對應的網站新聞

c. 其實要判斷 google 的縮短址所對應的真正位址可以在尾端加上一個「+」參數，例如“http://goo.gl/1S90TT+”，則會顯示完整位址，故真實網域“match.net.tw”為台哥大所擁有。



1. 此縮短址也能統計點擊的次數，方便網站管理。
2. 縮短址的好處是可以節省簡訊的顯示空間，以節省字數的費用，同時也常被駭客用來作為詐騙工具。

V. 網路行為架構圖



VI. 總結與建議

A. 這些事件類型都是一種透過簡訊進行釣魚詐騙的手法，且沒有特定對象，當詐騙集團或駭客掌握了大筆民眾的手機號碼後，就有可能大量發送釣魚簡訊。

B. 駭客通常會搭配時事新聞等訊息去引誘用戶點擊連結下載，此方式類似電子郵件 APT 攻擊方式，只是沒有針對特定對象。一旦安裝惡意 APK 後可能造成個資外洩及小額付款帳單暴增。

C. 惡意程式一直再改良進化，單純只用沙盒虛擬機可能也無法測試成功。

D. 駭客一旦可以竊取手機簡訊後，就能輕易進行相關消費的簡訊身分認證，或者取得其他帳號的二次驗證碼進行登入。

E. 遭受感染的手機可能也會發送惡意簡訊給自己的清單聯絡人，透過朋友的信任關係就容易上當，而成為駭客的殭屍手機或中繼站等。

F. 智慧型裝置實際上就是小型電腦，因此防毒軟體的安裝是必要的，否則遭

受感染可能會害人又害己。

G. 除了透過防毒軟體偵測移除病毒外，建議還原為出廠預設。