個案分析-

校園 Android 手機感染 Congur 病毒事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

106 年 11 月

I. 事件簡介

1. 隨著網路的普及與手機的使用率升高，使得手機的資安問題越來越重要，而在學術網路中，有許多學校提供學校師生無線上網的服務，因此，手機中毒之資安事件比例逐漸升高。

2. 本中心在 106 年 5 月至今，陸續開出 Andriod 系統感染 Congur 病毒的資安事件單，而從各校回覆的內容中發現，往往無法找到中毒裝置的使用者或找到該中毒裝置的惡意連線行為之來源。

教育機構資安通報平台

事件類型:入侵事件警訊

事件單編號:AISAC-12

原發布編號	ASOC-INT-201710-	原發布時間	2017-10-31
事件類型	對外攻擊	原發現時間	2017-10-31
事件主旨	通報:[大學]140. .66 Botnet: Android.Congur.Botnet,		
事件描述	ASOC發現貴單位(大學)所屬 140. .66 疑似對外進行 Botnet: Android.Congur.Botnet, 攻擊		
手法研判	貴單位疑似對外進行非法攻擊行為，Android.Congur.Botnet是一款針對Android OS的勒索木馬。此木馬透過更改小工具的PIN代碼，或者通過設置自己的PIN代碼來啟用安全功能。為此，勒索程序必須獲得管理員權限。在感染後，該木馬會會告知受害者通過QQ聯繫攻擊者以解除設備。		
建議措施	惠請貴單位： 1.確實使用Android平台提供的基本手機防護。 2.盡量避免使用Wi-Fi自動連線功能。 3.在下載來自第三方應用程式商店的APP前請審慎考慮。 4.當有程式或網頁請求授權時，請詳細閱讀其請求授權的內容。 5.安裝具有信譽且有效的智慧型手機防毒軟體。		

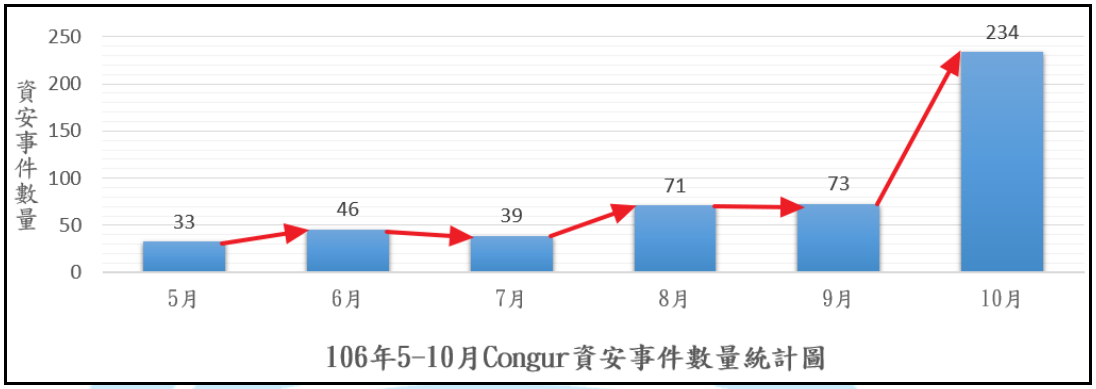
3. 從資安事件單的佐證資料顯示，該惡意行為的觸發皆會連到一個中國 IP:123.56.205.151:6280。

訊息	攻擊者連接埠	目標連接埠	目標 FQDN	目標位置	要求 URL 檔案名稱
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=14910&hash=01677651732
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=11869&hash=01677651732
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=10627&hash=01677651732
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=1183&hash=01677651732
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=966&hash=01677651732
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/clear?ts=0&ver=0&diff=0&tag=1&hash=01677651732
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=7306&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=8020&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=1528&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=367539&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=323178&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=307216&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=306252&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=222435&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=221542&hash=00652086056
Botnet: Android.Congur.Botnet	140. .66	123.56.205.151	123.56.205.151:6280	中國	/collect?ts=1459318632000&ver=38572616&diff=220580&hash=00652086056

4. 今年 6 月初在一間學校發現該資安事件單的中毒裝置使用者為一名學生，當該學生透過學校 Wifi 上網玩來自韓國的手機遊戲時會連線至中國 IP。

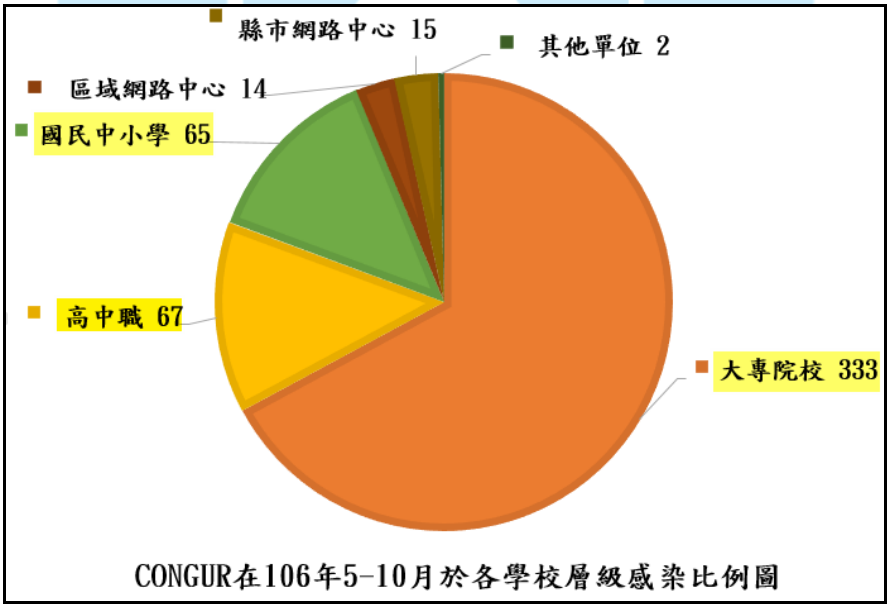
5. 今年 10 月在另一間學校發現此類型事件單之中毒裝置為桌上型電腦，該校有多名學生安裝 Android 模擬器於個人電腦並且上網玩遊戲，由此可知該類型資安事件單的中毒裝置並非只有手機，有安裝 Android 模擬器的電腦也有可能中毒。

6. 統計此類型資安事件在 106 年 5-10 月的觸發次數，發現此類資安事件共有 496 件，而且有越來越多的趨勢，需要加強防範此類事件的發生。



106年5-10月Congur資安事件數量統計圖

7. 分析此類型資安事件在 106 年 5-10 月所觸發的單位，發現大專院校佔大多數，其次是高中職與國民中小學，可能因有提供 Wifi 服務的學校以大專院校居多導致。



CONGUR在106年5-10月於各學校層級感染比例圖

8. 為了釐清是否因來自韓國的手機遊戲觸發 Congur 的資安事件單，本中心進行模擬檢測。

II. 事件檢測

1. 首先，將 IP:123.56.205.151:6280 送至 VirusTotal 檢測，發現此 IP 被防毒軟體公司檢測出為惡意的比例不高，僅 2/64，但該 IP 被 Fortinet 公司列為 Malware site。

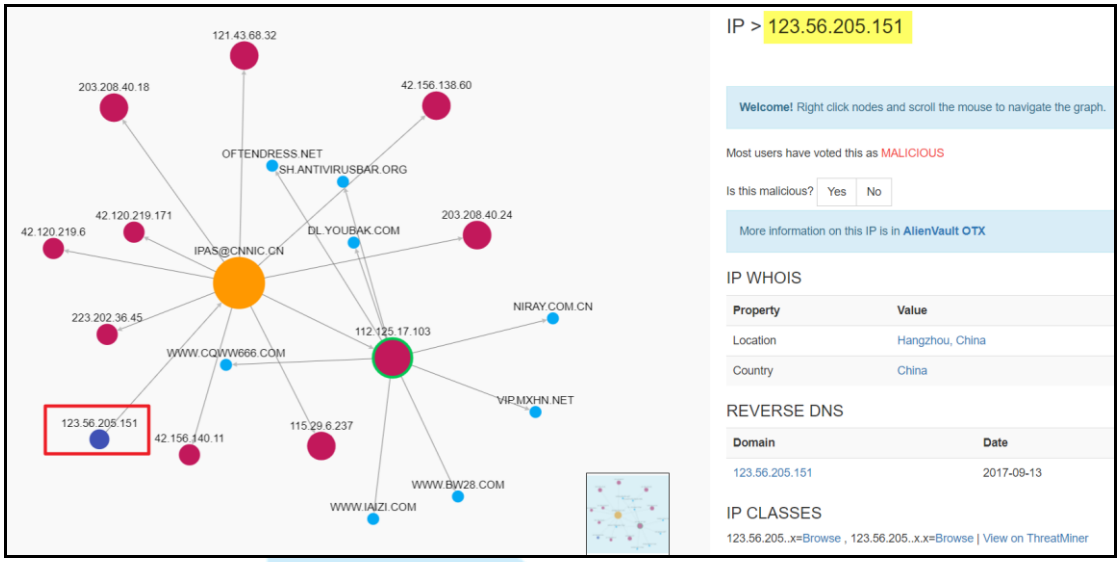
下圖的網址列表是 VirusTotal 提供與中國 IP(123.56.205.151:6280)有關係而被偵測到的惡意網址，事實上，從我們所側錄到的封包內容也可以看出該款遊戲有連到這些網址的行為。

Latest detected URLs

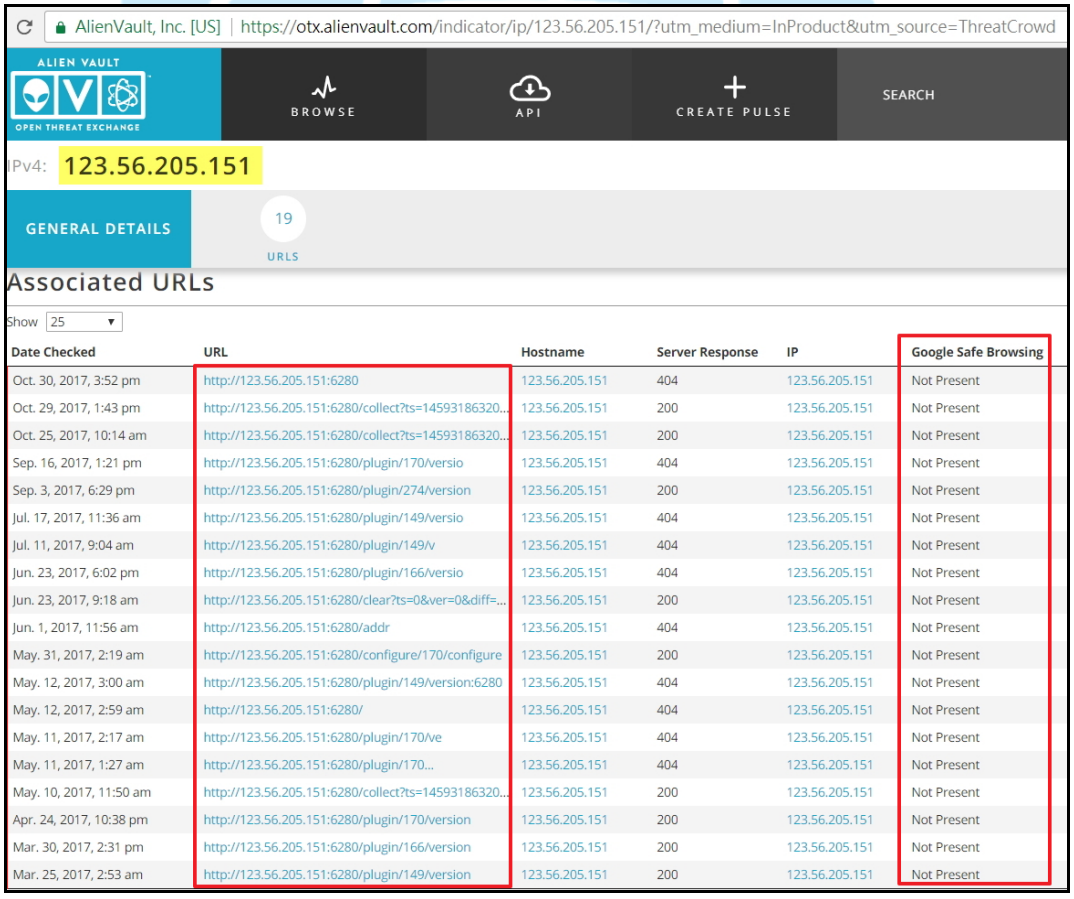
Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset**.

2/64	2017-11-01 02:43:24	http://123.56.205.151:6280/
1/63	2017-10-29 03:35:20	http://123.56.205.151:6280/collect?ts=1459318632000&ver=39735460&diff=33719&hash=01331142149
1/63	2017-10-26 22:41:40	http://123.56.205.151:6280/collect?ts=1459318632000&ver=20870318&diff=0&hash=01680255806
2/63	2017-10-26 10:18:11	http://123.56.205.151:6280/collect?ts=1459318632000&ver=35206504&diff=11960&hash=00571056307
1/63	2017-10-25 00:29:03	http://123.56.205.151:6280/clear?ts=0&ver=0&diff=0&tag=1&hash=01516585821
1/63	2017-10-25 00:04:04	http://123.56.205.151:6280/collect?ts=1459318632000&ver=40281100&diff=6684&hash=01516585821
2/63	2017-10-23 14:03:14	http://123.56.205.151:6280/collect?ts=1459318632000&ver=35908895&diff=0&hash=00498221653
1/63	2017-10-22 06:33:11	http://123.56.205.151:6280/collect?ts=1459318632000&ver=39377993&diff=1580&hash=01532297949
2/63	2017-10-19 15:37:21	http://123.56.205.151:6280/clear?ts=0\u0026ver=0\u0026diff=0\u0026tag=1\u0026hash=01367221833
3/63	2017-10-19 15:29:25	http://123.56.205.151:6280/plugin/170/version

2. 經查 IP:123.56.205.151 目前被 Fortinet 公司和 AlienVault 公司列入 IP 黑名單中，判斷可能曾經被用來作為 Android Congur Botnet C2 Server。



從下圖我們可以看出與中國 IP 有關聯的網址有哪一些，而這些網址在稍後我們所側錄到的封包內容中也有看到。另外，從下圖我們可以知道 Google 的安全瀏覽是不存在的。



3. 透過使用 Win7(x64)系統的 VM 主機進行隔離測試，並且安裝 Android 系統模擬器 BlueStacks 軟體於 VM 主機內。

4. 在 Google play 商店內搜尋韓國的手機遊戲(簡稱:遊戲 A)，發現該遊戲已有

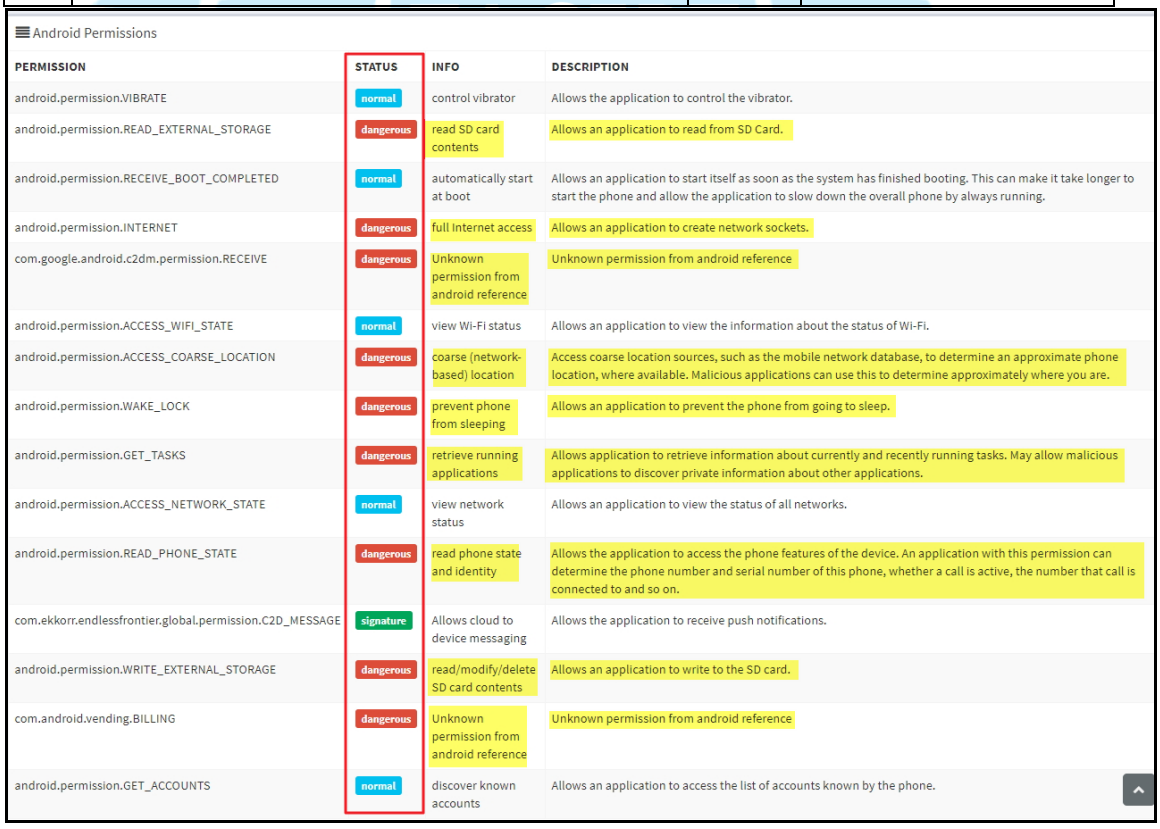
500 萬下載次數，可見此款遊戲使用者眾多。

5. 查看遊戲 A 的存取權限，發現所開啟的權限隱藏洩漏個人隱私的安全疑慮，例如:可讀取、修改或刪除 USB 儲存裝置的內容、尋找裝置上的帳戶、手機概略位置…等等。

6. 使用 MOBSF(Mobile-Security-Framework)工具檢測遊戲 A，發現在 Android 權限方面有多個權限項目存在風險，詳列如下:

NO	權限	狀態	資訊
1	android.permission.READ_EXTERNAL_STORAGE	危險	讀取 SD 卡內容
2	Android.permission.INTERNET	危險	完全存取網際網路
3	Com.google.android.c2dm.permission.RECEIVE	危險	來自 android 參考的未知權限

NO	權限	狀態	資訊
4	Android.permission.ACCESS_COARSE_LOCATION	危險	存取手機大概位置
5	Android.permission.WAKE_LOCK	危險	防止手機進入睡眠
6	Android.permission.GET_TASKS	危險	檢索執行中的應用程式來發現隱私資訊
7	Android.permission.READ_PHONE_STATE	危險	讀取手機的狀態與識別碼
8	Android.permission.WRITE_EXTERNAL_STRAGE	危險	讀取/修改/刪除 SD 卡內容
9	Com.android.vending.BILLING	危險	來自 android 參考的未知權限



Android Permissions

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
com.google.android.c2dm.permission.RECEIVE	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
com.ekkorr.endlessfrontier.global.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
com.android.vending.BILLING	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.GET_ACCOUNTS	normal	discover known accounts	Allows an application to access the list of accounts known by the phone.

7. 使用 MOBSF 工具檢測遊戲 A，發現在惡意程度分析方面存在四個問題，分別敘述如下:

NO	問題	嚴重性	說明
1	應用程式資料可以備份，Flag 遺失	中	該 Flag 應該設置為 false。 默認情況下，它被設置為 true，並允許任何人通過 adb 備份您的應用程式資料。它允許使用 USB 偵錯來複製應用程式資料的使用者關閉裝置。
2	內容提供者不受保護	高	發現內容提供者被設備上的其他應用程式共享，因此設備上的任何其他應用程式都可以存取內容提供者。
3	廣播接收器不受保護	高	發現廣播接收器被設備上的其他應用程式共享，因此設備上的任何其他應用程式都可以存取廣播接收器。
4	廣播接收器不受保護。存在一個有意圖的過濾器。	高	發現廣播接收器被設備上的其他應用程式共享，因此設備上的任何其他應用程式都可以存取它。有意圖過濾器的存在表明廣播接收器被明確地導出。

Manifest Analysis

ISSUE	SEVERITY	DESCRIPTION
Application Data can be Backed up [android:allowBackup] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) is not Protected. [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
Broadcast Receiver (com.ekkorr.endlessfrontier.global.LocalNotificationReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

8. 使用 MOBSF(Mobile-Security-Framework)工具檢測遊戲 A，在 Android Library Binary 分析方面，發現 elf 建立沒有堆疊保護，會大大增加利用堆疊緩衝區溢出的難度，因為它迫使攻擊者通過一些非傳統手段（例如破壞堆疊上的其他重要變數）來獲得對指令指針的控制，屬於高嚴重等級。

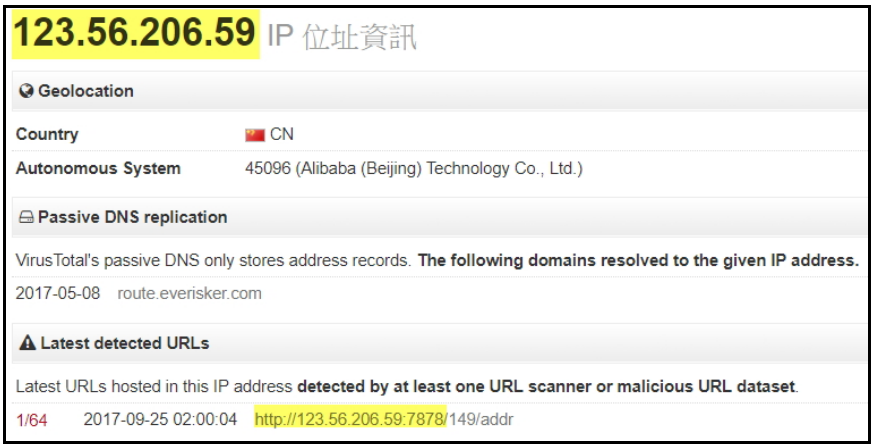
Android Library Binary Analysis

ISSUE	SEVERITY	DESCRIPTION
Found elf built without Stack Protection	high	Stack canaries can greatly increase the difficulty of exploiting a stack buffer overflow because it forces the attacker to gain control of the instruction pointer by some non-traditional means such as corrupting other important variables on the stack. Built with option **-fstack-protector**.

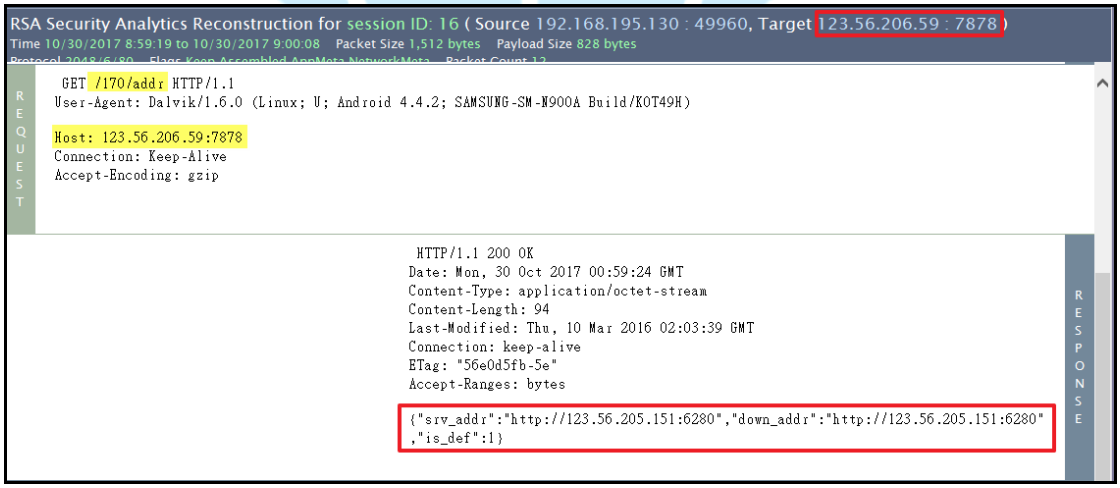
9. 在 Android 系統模擬器 BlueStacks 內安裝遊戲 A，發現當開啟遊戲 A 時，會有連線中國 IP:123.56.205.151:6280 的連線行為產生，而且當此遊戲 A 執行期間其連線次數頻繁，當遊戲 A 被關閉後，則會每隔一段時間連線至中國 IP，此連線行為如同執行一個後門程式來定期連至某一個 IP。另外，也發現在遊戲 A 開始執行時，會有短暫一、兩次連至中國 IP:123.56.206.59:7878 之連線行為。

Proto...	Local Address	Remote Address	State
TCP	127.0.0.1:53076	127.0.0.1:2871	ESTABLISHED
TCP	127.0.0.1:53520	127.0.0.1:2861	ESTABLISHED
TCP	127.0.0.1:53552	127.0.0.1:2871	ESTABLISHED
TCP	127.0.0.1:53563	127.0.0.1:2872	ESTABLISHED
TCP	192.168.195.130:53402	172.217.24.14:443	ESTABLISHED
TCP	192.168.195.130:53403	64.233.189.188:5228	ESTABLISHED
TCP	192.168.195.130:53436	172.217.24.14:443	ESTABLISHED
TCP	192.168.195.130:53459	172.217.24.14:443	ESTABLISHED
TCP	192.168.195.130:53464	172.217.27.147:443	ESTABLISHED
TCP	192.168.195.130:53465	172.217.24.14:443	ESTABLISHED
TCP	192.168.195.130:53469	216.58.200.42:443	ESTABLISHED
TCP	192.168.195.130:53499	216.58.200.42:443	ESTABLISHED
TCP	192.168.195.130:53504	216.58.200.42:443	ESTABLISHED
TCP	192.168.195.130:53519	216.58.200.234:443	ESTABLISHED
TCP	192.168.195.130:53521	216.58.200.234:443	ESTABLISHED
TCP	192.168.195.130:53543	172.217.24.14:443	ESTABLISHED
TCP	192.168.195.130:53544	172.217.24.14:443	ESTABLISHED
TCP	192.168.195.130:53590	172.217.27.147:80	ESTABLISHED
TCP	192.168.195.130:53591	123.56.206.59:7878	ESTABLISHED
TCP	192.168.195.130:53593	13.57.68.223:80	ESTABLISHED
TCP	192.168.195.130:53594	123.56.205.151:6280	ESTABLISHED
TCP	0.0.0.0:5555	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7777	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9999	0.0.0.0:0	LISTENING
UDP	0.0.0.0:12000	*:*	
UDP	0.0.0.0:54479	*:*	
UDP	127.0.0.1:2866	*:*	

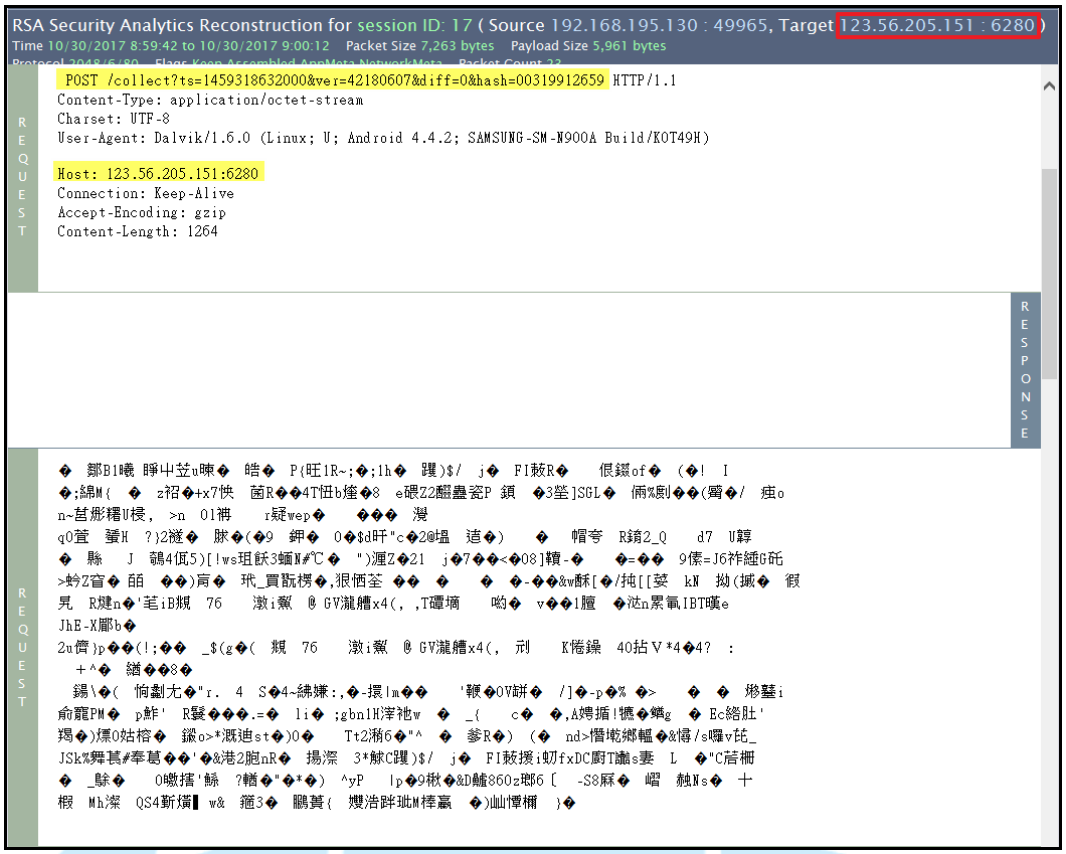
10. 透過 VirusTotal 網站檢測 IP:123.56.206.59，發現該 IP 被 Fortinet 公司視為 Malware site。



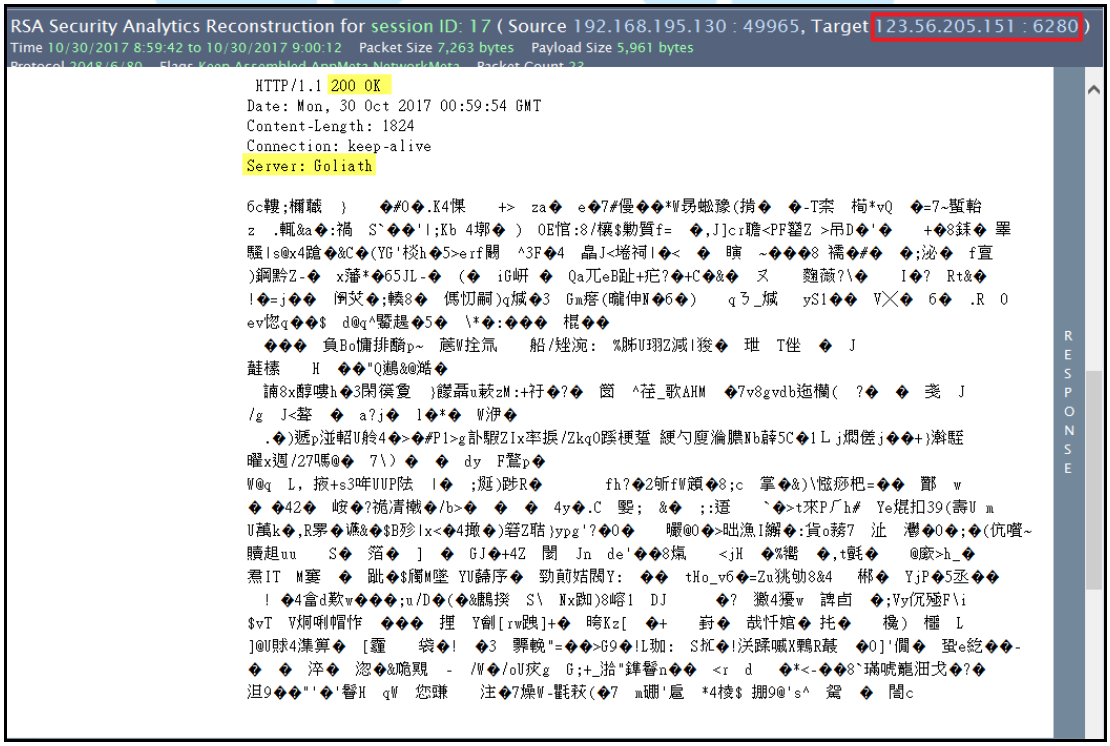
11. 檢視側錄的封包內容，發現 Android 系統模擬器會連到中國 IP:123.56.206.59:7878 去取得資料，所取得資料內容為伺服器位置:http://123.56.205.151:6280 與下載位置:http://123.56.205.151:6280。



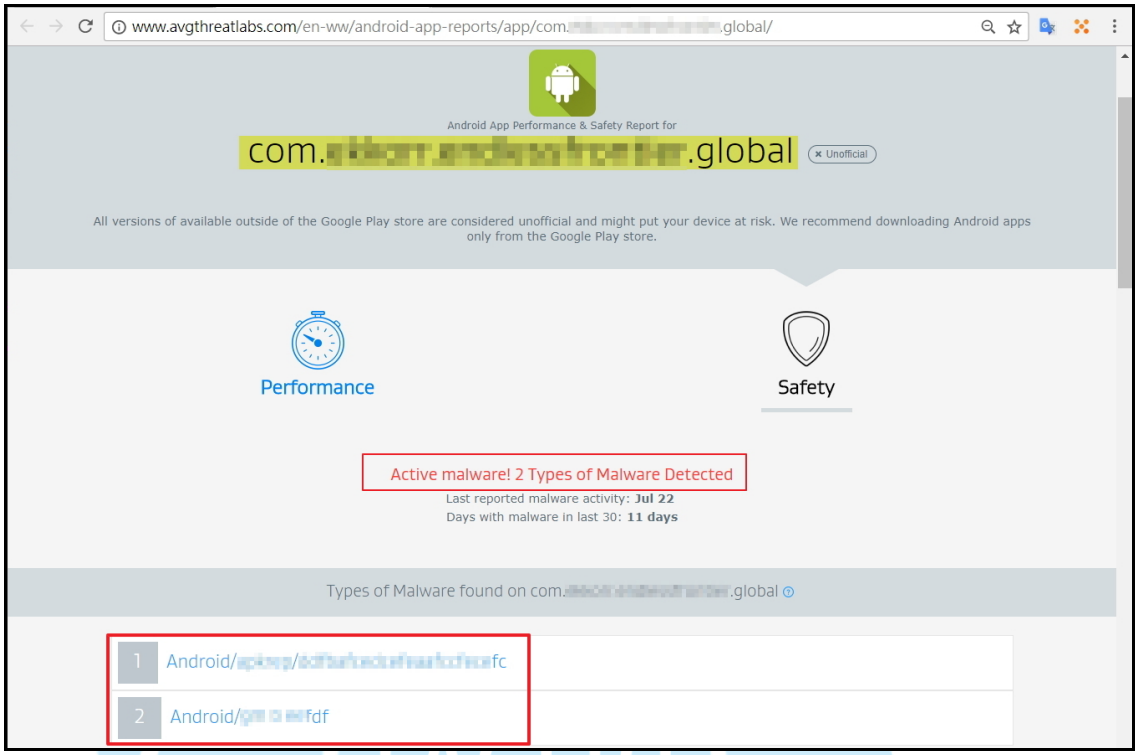
接著它便會連線到 IP:123.56.205.151:6280 去上傳資料，



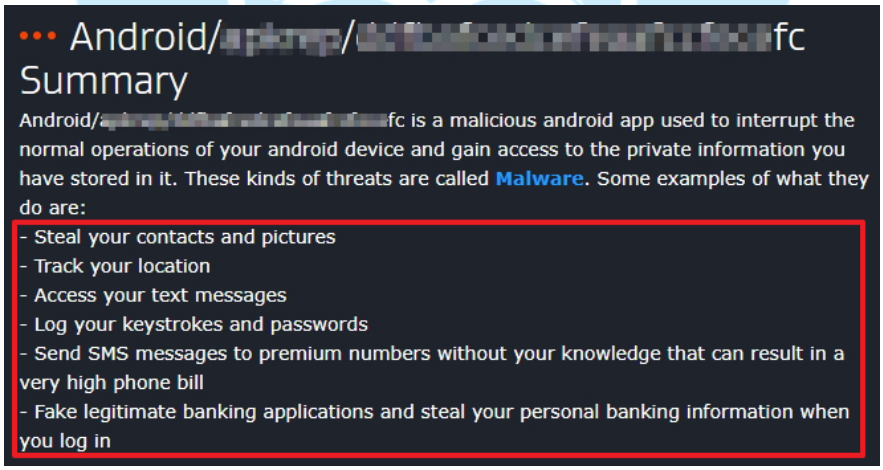
IP:123.56.205.151:6280 (Server: Goliath)會回應請求成功，並且傳送資料給 Android 系統模擬器。之後，Android 系統模擬器會陸陸續續每隔一段時間連到 IP:123.56.205.151:6280 去上傳資料。

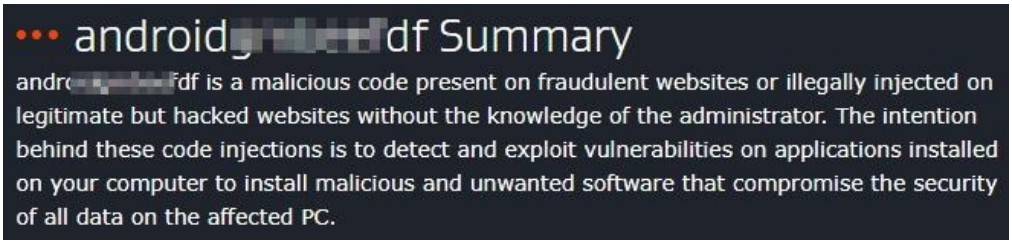


12. 從 Avgthreat Lab 所出的 Android App 報告內容，得知遊戲 A 為活動中的惡意程式，而且被偵測到內含兩個惡意子程式。

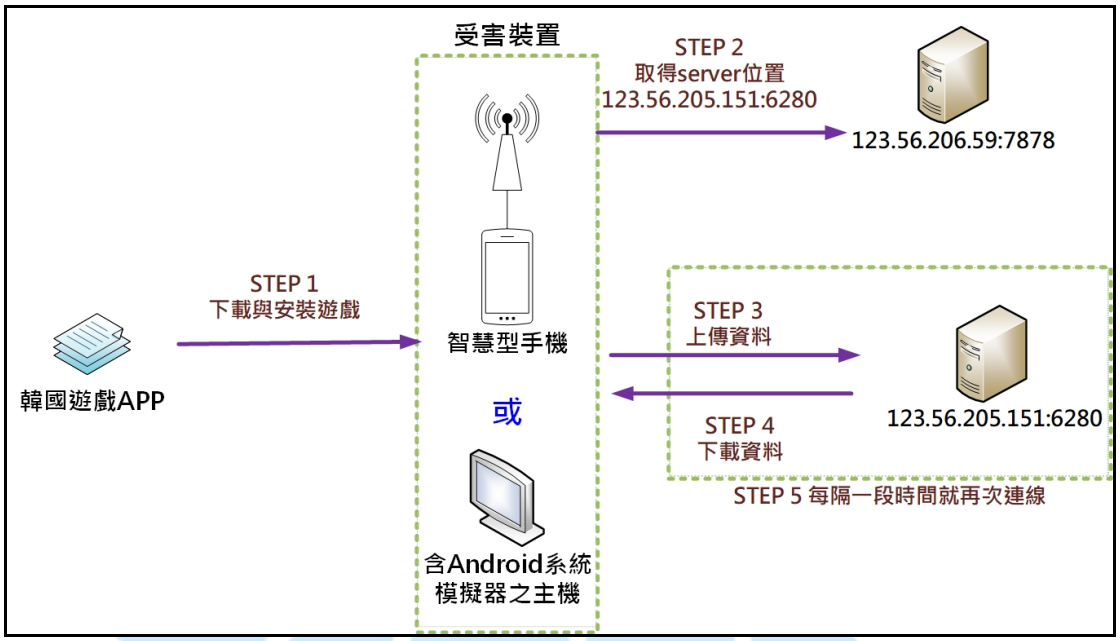


這些惡意子程式會中斷手機的運作與竊取使用者的個人資訊，也會注入代碼來檢測與利用使用者手機上安裝的應用程式漏洞，以安裝惡意與不需要的軟體，危及受影響手機上所有資料的安全性，可見該遊戲 A 存在惡意行為。





III.網路架構圖



1. 使用者下載與安裝韓國遊戲 APP。
2. 連至一個中國 IP:123.56.206.59:7878 取得 Server 位置:123.56.205.151:6280 的資訊。
3. 上傳資料給 IP:123.56.205.151:6280 的伺服器。
4. 從 IP:123.56.205.151:6280 的伺服器下載資料。
5. 每隔一段時間再次連線 IP:123.56.205.151:6280。

IV.建議與總結

因在學術網路中陸續發生許多 Android. Congur 資安事件（偵測規則：Android.Congur.Botnet 或 MALWARE-CNC Andr.Trojan.Congur variant outbound connection detected），經本中心檢測觸發原因來自一款韓國的手機遊戲，當使用者於 Android 系統玩此遊戲時，會出現連至中國 IP:123.56.205.151:6280 之連線行為，此 IP 目前被 Fortinet 公司和 AlienVault 公司視為惡意 IP，並列入黑名單，建議各學校遇到此類資安事件時，優先封鎖此惡意 IP，封鎖該 IP 不影響該遊戲之使用。