Android 惡意程式收集、分析與評估

許珈榮 林盈達 蔡濠全 李佳穎
國立交通大學資訊工程系
Email:crazygod.cs01g@nctu.edu.tw; ydlin@cs.nctu.edu.tw;
haochuan@nbl.org.tw; cylee@url.com.tw
September 28, 2012

摘要

Android 程式最早時期只有出現在官方市場，而這時期的惡意程式(Malware) 數量較少。現在，非官方市場的出現，造成惡意程式數量增加。因此，即時收集新型惡意程式，以便讓防毒軟體做最有效率的病毒資料庫更新是必須的。此實驗透過分析非官方網頁的 HTML 碼，取得 APK 下載網址進行下載，並上傳至 virustotal 做第一層的掃描，統計結果並分析惡意程式的行為及種類。另外，將可能感染惡意程式的 APK 檔案安裝至模擬器進行第二層掃描，統計結果並算出手機防毒軟體的準確率。此實驗也評定非官方網站的更新頻率，透過兩個時間點 7/7 和 8/18 做收集，而收集到的檔案數目分別為 5730 個與 6998 個，利用檔名比較方法得更新數量，並計算出更新頻率。由實驗結果得知，目前非官方的感染比例為 187/1745(11%)而官方的感染比例為 2/92(2%)，而惡意程式種類個數，Trojan 有 12 種，Adware 有 8 種，backdoor 有 2 種，另有 7 種無歸類。惡意程式的行為分布上以 adware 佔了 49%，Trojan 與 backdoor 分別為 24%與 26%。防毒軟體準確率而言，以 Aegislab Antivirus 較能偵測惡意程式。另外，針對 http://android.d.cn/game/做收集成效分析，42 天即可收集到 2588 個新的 APK 檔案。

關鍵字：Android、惡意程式、APK 檔、APK 檔案收集

一、Android 作業系統簡介和 APK 檔案結構

Android 作業系統

Android 為一種建構在 Linux 上的作業系統，主要設計於手持式的設備上。Google 為了能讓 Android 在移動設備上有良好的執行，對 Linux 核心進行的修改及擴充[1][2]。另外，Dalvik 為 Google 在 Android 系統上所提供的 Java Bytecode 虛擬器[3]，所有的應用程式皆須透過 Dalvik 編譯成為一個 APK 檔案結構來存取系統。Android 系統利用 permission mode 去管理使用者的操作，所有的操作都需有特定的權限，比方說利用 wifi 方式取得所在位置，就需要 Android. Permission. ACCESS_COARSE_ LOCATION 這個權限[4]。惡意程式

即是透過某些方法取得所要執行惡意行為所需的權限，以便執行惡意行為。

Application package file

由於惡意程式為 repackaged APK 檔案，因此我們要先對 APK 檔案有初步的認識。表 1 為 APK 檔案架構圖，當建立一個 Android 專案時，專案會建立 2 個資料夾分別為 META-INF 與 Res[5]，前者包含 mainfest.mf、Cert.rsa、Cert.sf 檔案，後者則是存放像圖片等的 resource。同時，還會創建幾個檔案記錄訊息，Resource.arsc 記錄 resource 的位址，AndroidManifest.xml 則是記錄 Android 專案名稱、版本、與權限，classes.dex 則是 Java 程式經過編譯後產生的檔案。而 repackaged APK file 通常會修改 Manifest.xml 裡面的權限，而造成程式執行時，有更高的權限去執行惡意行為。

表 1: APK 檔案架構

APK 檔案架構		說明
META-INF (Directory)	Manifest.mf	Manifest file
	Cert.rsa	Application certification
	Cert.sf	List of resources/SHA-1
Res (Directory)		Resource used by APK(png/xml)
Resources.arsc		List of resource locations
AndroidManifest.xml		Android binary containing name, version, permissions
Classes.dex		Compiled source code

二、 惡意程式行為種類

根據惡意程式的行為模式，大致可以分為 Trojan(對使用者的資料，做惡意的行為)、Rootkit(權限的更動)、Spyware(監聽使用者隱私)、Adware(對使用者散播無意義廣告)、PuA(對使用者的手機資源惡意使用)、Backdoor(利用程式中的後門，在使用者執行程式時竊取資料)。而常見的惡意程式種類如同表 2 所列舉。

表 2-惡意程式行為及種類

	Trojan	Rootkit	Spyware	Adware	PuA	Backdoor
Geinimi	✓					
PJApps	✓		✓			
ADRD	✓					
DroidDream	✓	✓				
droidKungFu						✓
SMS.FakeInst	✓					

GGTracker	✓					
J.SMSHider	✓					
DroidDreamLight						✓
BgServ	✓					
RogueSPPush	✓					
NickySpy			✓			
Toolbar.MywebSearch					✓	
Ropin				✓		

三、PC 與 Android 惡意程式之比較

行為、傳播、偵測方式

Android 與 PC 的惡意程式在行為上非常的類似，差別在於 PC 架構上比較複雜，因此，行為上相對於 Android 會比較多樣。以 PC 而言，有用戶端行為與網路端行為，前者以資料檔案破壞、佔用大量系統資源等，後者以網路擁塞為主，而 Android 行為上以資料的破壞、隱私竊取等。傳播方式，由於 PC 與 Android 架構上的差異，導致傳播上會有不同的類型，以 PC 而言，通常會透過超連結、電子郵件的附件、p2p 軟體等進行傳播，而 Android 傳播則是以 APK 檔案為主。偵測方式，隨著防毒軟體不同而有不同的設計，以 PC 而言，是以 behavior -based 與 signature-based 偵測，而 Android 以 signature-based 為主。

表 3–PC 與 Android 行為/傳播/偵測方式比較

	PC	Android
行為	➢ 用戶端行為 資料檔案破壞、隱私竊取、系統執行程序錯亂、佔用大量的電腦資源 ➢ 網路端行為 網路擁塞	資料破壞、隱私竊取、金融商業行為
傳播	超連結、電子郵件附件、P2P 軟體、USB/磁片/光碟	APK 檔案
偵測方式	Behavior-based detection & Signature-based detection	Signature-based detection

收集方式

探討收集方式之前，要先了解 PC 與 Android 的架構及執行程式的差別，由於 Android 為 linux-based 的作業系統，其中 linux 與 Unix 相類似，皆以

核心為基礎，並完善的保護多程序的操作系統，安全考量較為嚴謹，因此，Android 惡意程式都需經過解壓縮、執行、才可進行感染。PC 上程式的執行需經過作業系統排程，作業系統負責 cpu 的分配，cpu 執行程式，因此，PC 惡意程式常透過各樣的手段進行感染，安全性上漏洞也較多。目的而言，PC 主要以竊取隱私、破壞資料等，而 Android 為手持裝置的作業系統，主要以電力的消耗，資料的破壞，隱私的竊取為主，透過架構及目的的比較，接著便探討收集方式的不同，PC 而言，以超連結，email 等途徑進行收集，而 Android 僅以 APK 檔案為主要收集方法如表 4。

表 4-PC 與 Android 的收集方式比較

	PC	Android
嚴謹性	差	佳
目的	竊取個人隱私、破壞程式、資料檔案	竊取隱私，取得權限、賺取廣告費、流量費損失、耗電
收集方式	URLs 、Emails、Skype、P2P 軟體	APK 檔案

四、PC 與 10 家手機防毒軟體之比較及手機防毒軟體功能性評比

PC 與 10 家手機防毒軟體之比較

PC 與手機防毒軟體皆提供非常類似的功能，表 5 主要針對檔案掃描/SD 卡掃描、web 下載掃描、雲端掃描、sandbox、即時監控、黑名單設定、敏感檔案鎖定、遠端資料刪除、尋找遺失設備等功能做比較，而 PC 防毒軟體與 Android 防毒軟體僅差別在於雲端的掃描、Sandbox、和即時監控的有無。

表 5-PC 與手機防毒軟體之比較

Function	PC Antivirus	Android Antivirus
檔案掃描/SD 卡掃描	Yes	8/10
Web 下載檔案掃描	Yes	3/10
雲端掃描	Yes	1/10
Sandbox	Yes	0/10
即時監控	Yes	0/10
黑名單設定	Yes	3/10
敏感檔案鎖定	Yes	2/10
遠端資料刪除/手機鎖定	Yes	5/10
尋找遺失設備	Yes	5/10

（註:8/10 表示 10 家防毒軟體中有 8 家防毒軟體有此功能）

手機防毒軟體功能性評比

表 6 為針對 10 家防毒軟體進行四個功能(SD card scan、Web scan、Auto-scan、Signature Auto-update)的比較，基本的 SD card 掃描大部分的防毒軟體皆有提供，比較結果以 Webroot 提供的功能最為完善

表 6-手機防毒功能性評比

Android Antivirus	SD Card Scan	Web Scan	Auto-Scan	Sig Auto-update
NetQin Mobile Antivirus	✓	✓		
Trend Micro Mobile Security	✓			
McAfee Mobile Security	✓			
Doctor Web Anti-virus Light	✓	✓		
AVG Anti-Virus Free for Android				
Lookout Mobile Security			✓	
Webroot Mobile Security Basic	✓	✓	✓	✓
HAURI ViRobot Mobile	✓			
360 Mobile Safe	✓			
AegisLab AntiVirus Free	✓			✓

五、 實驗流程與收集方法

實驗流程

先透過第一層掃描，利用 virustotal 將大量的 APK 檔案進行過濾，先判定可能為惡意程式的檔案，再透過第二層掃描，安裝至手機用防毒軟體偵測，並針對統計的結果進行分析。

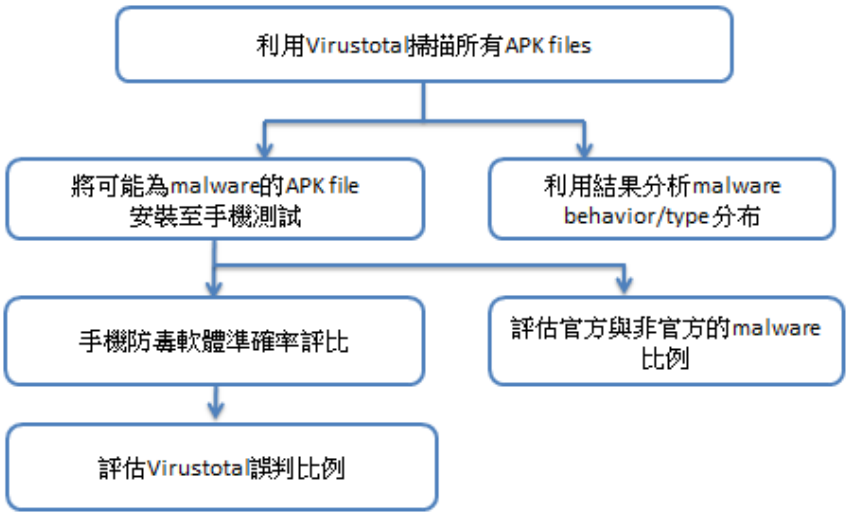

圖 1-實驗流程

收集方法

利用分析 HTML 碼的方法，其中可以搭配 jericho.jar 的使用[6]，即可擷取下載 APK 檔案的網址，再利用 wget 下載檔案。或直接利用 wget 方法[7] (ex:wget -r -nd -P D:\inde_study\ http://www.jimi168.com/)，並搭配參數的使用，即可直接進行下載，但此方法的缺點是，若參數沒設好的話，可能會將整個網路的東西都抓下來，比較危險。

六、 實驗結果

非官方網站的分析結果

透過圖 2 及表 7 可知，大部分的檔案是未受感染的，小部分為 virustotal 中有防毒軟體認為是惡意程式，接著會再針對這些惡意程式做行為與種類的分析。此三個非官方網站其感染率分別為 11%、14%與 5%，使用者在非官方的網站下載 Android 程式會有相當部分比例是會下載到含有惡意程式的檔案。

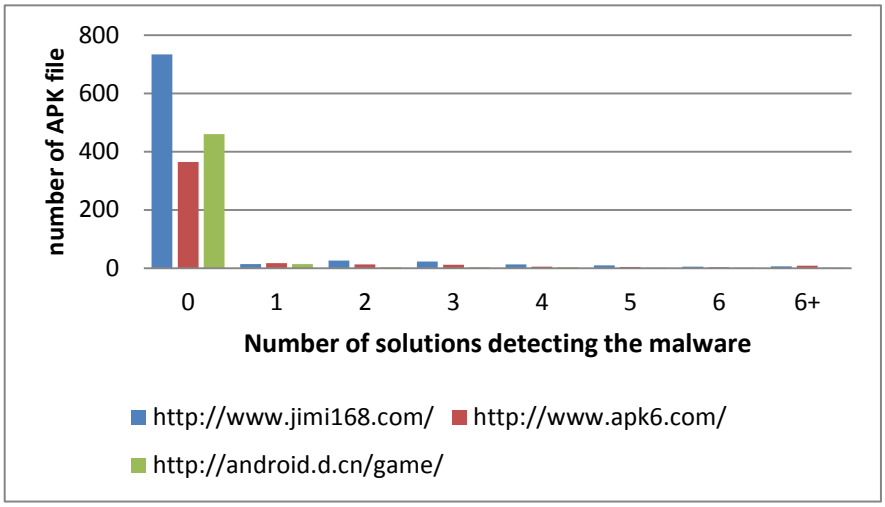

圖 2-非官方網站分析結果

表 7-非官方網站感染比例

非官方網站	感染比例
http://www.jimi168.com/	11%
http://www.apk6.com/	14%
http://www.android.d.cn/game/	5%

Collected 惡意程式行為/種類分布

a. 行為分布

惡意程式行為分布上，以 Adware 佔了大多數(49%)，也就是使用者在使用程式的過程中，常會有莫名的廣告干擾，而 Trojan 與 Backdoor 則暫居其後(24%與 26%)，兩者皆會在不受使用者的注意下破壞使用者的資料並執行

惡意的行為。

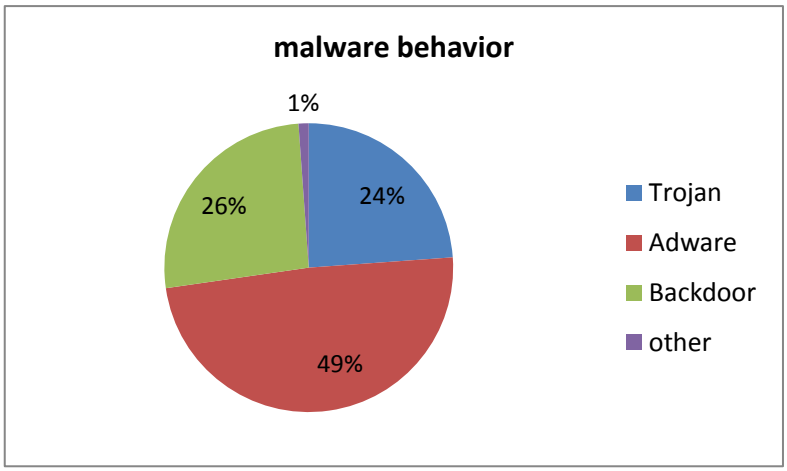

圖 3-行為分布

b. 種類分布

表 8 為目前收集到的惡意程式種類，Trojan 有 12 種，Adware 有 8 種，backdoor 有 2 種，另有 7 種無歸類，種類上相當多樣，以此種趨勢，將來惡意程式種類會增加非常快速。

表 8-已收集的惡意程式種類分布

惡意程式行為	惡意程式種類
Trojan	Moghava、TROJ_GEN.F47V0719、Hispo、Lootor、GinMaster、Win32.Trojan、Plangton、GingerMaster、TROJGappusin
Adware	Ropin、AirPush、Startapp、Leadbolt、Izp、Leadbolt、Gappusin、AdsWo
Backdoor	Hack.Exploit.Win32.CVE-2008-0015.a、KungFu
other	NewyearL、SmsSend、Counterclank、AGENTABLK、Ropin、Wapsx

官方與非官方的感染比例

表 9 說明了不管是官方還是非官方，皆會有惡意程式隱藏在程式內，差別在於比例的多寡，即使官方網站在將 Android 程式上架時都會利用 Bouncer 安全機制掃描，但仍會有漏網之魚，但出現的機率並不會太大，而非官方網站相較於官方網站感染率則是大上許多。

表 9-官方與非官方感染比例

	感染比例
官方(GooglePlay)	2/92 (2%)

非官方	187/1745 (11%)

手機防毒準確率評比

圖 4 可知各家防毒軟體對於惡意程式所擷取的特徵碼判別嚴謹度不同，而造成偵測數量上的差別。從實驗結果來看，Aegislab 有較完善的病毒特徵碼辨別，而 netqin 對於病毒特徵碼判斷上較為不足。

表 10 說明 Virustotal 上的防毒軟體之惡意程式特徵碼未必為最新版，因此會對判斷惡意程式的結果產生誤判/漏判。相較之下，在模擬器上所安裝的皆為最新版，在相比較後，得 virustotal 的誤判/漏判率，以 Dr.web 與 McAfee 兩家防毒軟體對 virustotal 做誤判/漏判率的評估，其值分別為 1/35(2%)與 3/35(8%)。

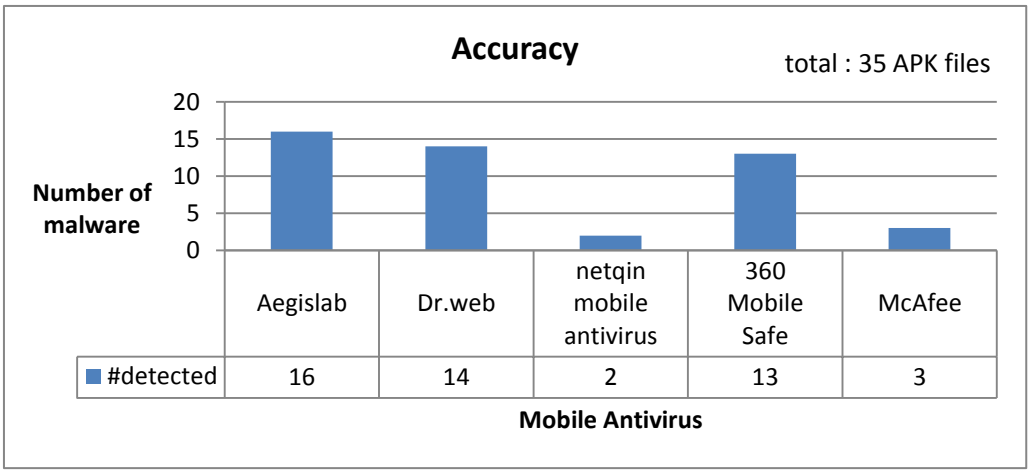

圖 4-準確率

表 10-Virustotal 失誤率

	Aegislab	Dr.web	netqin	360 mobile Safe	McAfee
Emulator	16	14	2	13	3
Virustotal	-	15	-	-	0
Error rate	N/A	2%	N/A	N/A	8%

（註：『-』代表 virustotal 上無此防毒軟體）

APK 檔案收集成效與分析結果

收集成效

要探討收集的成效，我們要先知道一個網站的更新的頻率，透過這個訊息，我們可以選擇更新頻率較高的網站作為收集 APK 檔案的良好供應商。

由表 11 可知，7/7 與 8/18 分別收集到 5730 個與 6998 個 APK 檔案。42 天可以收集到 2588 個新的 APK 檔案，可透過此方法，針對幾個網站做收集成效的比較，更新頻率較高的網站有利於新型惡意程式的收集。

表 11-7/7 與 8/18 收集檔案個數

Date	Number of APK file
7/7	5730 個
8/18	6998 個

Virustotal 分析結果

圖 5 為新收集到的 APK 檔案分析結果。經過分析之後，新收集到的 APK 檔案偵測到的感染率為 9%，比例上算蠻高的，因此可以從此網站下手，持續收集不同的惡意程式，利於防毒軟體更新。

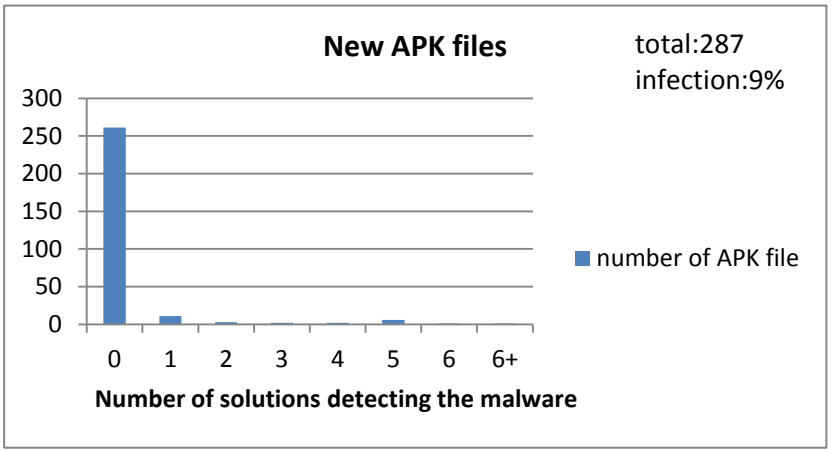

圖 5-New APK file 分析結果

七、 結論

由以上圖表，我們歸納出幾個結論：

1. 目前非官方的感染比例約為 187/1745(11%)而官方的感染比例為 2/92(2%)，官方與非官方皆有相當大的比例會感染惡意程式，因此，在下載 Android 應用程式時應格外的小心。
2. 由於目前收集到的惡意程式種類非常的多樣，且現在網站的更新頻率都非常高，根據這樣的趨勢，將來必定會產生更多種類的惡意程式，防毒軟體特徵碼的判定上會更加的困難，無法辨別的情形也會增加，盡可能的少碰來路不明的軟體才是因應之道。
3. 以惡意程式行為分布而言，大部分是以廣告的干擾為主，其次為惡意行為像資料的破壞、個人資料的洩漏等。

八、 參考文獻

[1] 楊豐盛著，陳佳新譯;「Android 技術內幕:探索 Android 核心原理與系統開發」;碁峰資訊, 2011。

[2] Wiki android operation system, http://en.wikipedia.org/wiki/Android_(operating_system)

[3] Android 筆記–Dalvik 的漫談, http://loda.hala01.com/2011/03/android%E7%AD%86%E8%A8%98-dalvik%E7%9A%84%E6%BC%AB%E8%AB%87-2/

[4] Android 權限大全, http://www.eoeandroid.com/blog-548102-1685.html

[5] 吳亞峰，蘇亞光編著；「深入淺出 Android 遊戲程式開發範例大全」;博碩文化, 2011。

[6] Jericho HTML Parser, http://jericho.htmlparser.net/docs/index.html

[7] wget 指令及參數, http://itgroup.blueshop.com.tw/pendm/blog?n=convew&i=9401

[8] 資安論壇, http://forum.icst.org.tw/phpbb/viewforum.php?f=8

[9] 義集思(AegisLab)安全研究部落格, http://blog.aegislab.com/index.php?blogId=2

[10] APK downloader-download APK files from android Market to PC, http://codekiem.com/2012/02/24/apk-downloader/

[11] Chien-Hung Chen, " Identifying Malicious Applications by Behavioral Similarity on Android Platforms," MS Thesis, National Chiao Tung University, 2012