Android 恶意软件特征研究

边 悦,戴 航,慕德俊
(西北工业大学 自动化学院,陕西 西安 710072)

摘 要:智能手机的广泛应用导致手机恶意软件的数量急速增加,尤其是近几年,基于 Android 操作系统的手机在智能手机市场占据主导地位,针对 Android 系统的恶意软件数量快速增加。手机恶意软件主要收集手机用户地理位置、语音通信、短信等个人隐私信息,或进行恶意扣费、耗费系统资源等行为,给用户自身和手机系统带来很大危害。准确分析恶意软件行为特征可以为后续清除恶意软件提供有力依据。传统的恶意软件分析技术主要包括静态分析与动态分析,文中介绍了当前存在的一些手机恶意软件分析检测技术及其缺陷,并从安装、激活、恶意负载三方面对已知 Android 恶意软件主要行为特征进行详细分析。

关键词:智能手机安全;Android 恶意软件;行为分析
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2014)11-0178-04
doi:10.3969/j.issn.1673-629X.2014.11.045

Research on Android Malware Characteristic

BIAN Yue, DAI Hang, MU De-jun
(School of Automation, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: The wide use of smart phones results in a sharp increase in the number of phone malicious code, especially in recent years, phone with Android operating system dominates the smartphone market, malicious code to the Android system increases rapidly. Malicious software on mobile phones mainly collects personal privacy information such as user location, telephone calls, text messages and so on, those software may also engage in malicious payment, costing of system resources, bringing great harm to the user and cell phone system. Accurate analysis of malware behavior characteristics can provide powerful basis for the subsequent removal of malicious software. Traditional malware analysis techniques include static analysis and dynamic analysis, some analysis and detection technology and its defects are introduced, analyzing the main behavior characteristic of existing Android malware from three sides, inclusive of the installation, activation and malicious load in detail.

Key words: smartphone security; Android malware; behavior analysis

0 引 言

恶意代码对 PC 的威胁存在已久,随着智能手机的普及,针对手机的恶意代码也陆续出现,并呈现爆炸式的增长。根据移动安全服务厂商网秦对外公布的一份手机安全报告显示,2013 年第一季度查杀到手机恶意软件 25 140 款,同比 2012 年增长 353.05%;感染手机 1 040 万部,同比 2012 年增长 99.23%。由于 Android 平台快速扩张,已超过 IOS 和 Symbian 平台占据市场主导地位,同时 Android 系统具有高开放性,导致 Android 平台受到较多恶意攻击,据统计,超过 8 成的恶意软件来自 Android 平台。这些恶意软件主要为游戏类或者工具类软件,如“神庙逃亡”、“航班查询”等热门软件都曾被伪装或修改过[1]。

手机恶意软件的危害主要有恶意扣费、窃取用户隐私、耗费系统资源、破坏系统、恶意传播等[2-3]。大多数恶意软件包含多种恶意行为,其中,附加窃取用户隐私行为的占总数比例超过九成。这些恶意软件隐藏在后台非法收集用户地理位置、通讯录、短信或其他信息上传到指定服务器,一旦存有恶意目的的人获取这些信息,造成的损害将无法估计。

然而,由于缺乏对这些新型恶意软件机理的认识,缺少相关代码样本,同时由于智能手机内存和电池容

收稿日期:2013-12-09 **修回日期**:2014-03-16 **网络出版时间**:2014-07-28
基金项目:2012 教育部博士点基金(20126102110036)
作者简介:边 悦(1989-),女,陕西人,硕士研究生,研究方向为网络与信息安全;戴 航,硕士生导师,研究方向为网络与信息安全;慕德俊,博士生导师,研究方向为控制理论、网络信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140728.1228.045.html

量限制反病毒软件的效率,手机不能时刻联网,不能及时获知新病毒的出现,目前能够应对手机病毒的解决方案少之又少。

1　相关技术

目前,恶意代码分析与检测主要存在两种方法—静态分析与动态分析[4]。防病毒厂商大多采用静态分析技术,静态分析主要分析源代码或二进制代码,查找可疑行为[5-7]。尽管存在一些成功的分析方法,但对于采用模糊变性技术的代码,静态分析存在很大缺陷。基于行为的动态分析是指在受控或独立的环境中运行样本,从而分析其执行过程[8-9],文献[10]介绍了恶意代码动态分析技术的总体概况。

静态与动态分析方法都已被引入到手机恶意代码分析。但是由于手机资源、电池容量和内存限制,单个手机上的分析效果并不理想。

手机恶意代码出现初期,采用最多的检测技术是计算电池电量消耗。这种技术通过监视手机电量消耗,并与正常电量消耗比对,来确定是否存在异常。

鉴于智能手机内存、运行速度等资源限制,研究者们提出一些协作分析技术[11-12]。协作系统通常有一台核心服务器,该服务器用于收集手机恶意代码,并进行分析,最后将分析结果发送系统中各个手机上。

也有研究者提出一些 Android 安全模型,其中一个重要的模型是基于许可的安全模型[13]。根据该模型,每个应用程序有不同的设备资源使用需求,由手机用户同意或拒绝安装程序。已经有很多文章在分析和使用 Android 许可安全模型。然而即使用户在安装陌生程序前收到警告信息,手机上的恶意程序传播依然迅速,因为恶意程序通常采用欺骗用户的方式,使用户相信其所有应用的可靠性,并在手机上进行安装。

另外还有研究者提出 Android 应用检测沙盒。首先将静态分析程序伪装成 apk 文件,以便检测恶意行为。然后,在一个安全的环境中模拟用户操作,运行 Android 应用程序,程序执行期间,设备发生的所有事件(打开文件、存取文件、电池消耗等)都被监视并记录以备后续分析。然而该技术仍存在缺陷,即用户交互仿真器不可能模拟真实用户所有行为。

2　Android 恶意软件

文献[14]的作者收集了 2010 年到 2011 年间 1 260个恶意软件,基本涵盖当前已知恶意代码家族。分析这些代码,可以发现超过 80% 的样本对合法应用程序进行重包装,添加恶意负载。同时,越来越多的恶意代码采用升级攻击或过路式下载方式感染手机用户,此外,大约三分之一的样本采用提高权限的方式以获得 Android 安全模型的完整许可。这些恶意软件给 Android 手机用户带来了极大的安全威胁。

总体来说,从安装方法、激活方式、恶意负载三方面来看,Android 恶意软件主要行为特征详见下文。

2.1　恶意软件安装

已知的 Android 恶意软件安装方法主要有重包装、软件升级、路过式下载。这些方法并不独立,通常某个恶意软件会采用多种方法诱骗用户下载。

2.1.1　重包装

重包装是病毒编写者采用较多的方式。病毒编写者查找并下载热门 app,进行反汇编,嵌入恶意负载,然后重新上传至官方或其他安卓市场,并诱骗手机用户下载安装这些被感染的 app。

通常恶意软件编写者使用有误导性的文件名,以使恶意软件看起来是合法软件。如早期的 DroidKungFu 家族软件使用文件名 com. google. search,伪装成 Google 搜索模块,之后的版本使用 com. google. update,伪装成 Google 官方升级模块。

另外,Android 安全模型允许 app 部署相同的手机固件平台密钥来获取许可,许可中包含一条:不用经过用户同意,即可安装额外 app。一些著名的固件拥有默认密钥,并公布在 Android 公开资源工程 AOSP。于是部分恶意软件利用在 AOSP 上公开获取的私有密钥获得安全模型许可,从而被感染的 app 能够轻松获取操作系统的某些权限而不被用户知晓。

2.1.2　软件升级

恶意软件重包装将恶意负载直接加入 app 中,容易暴露其本性。不同于将负载作为一个具体功能,升级攻击只在 app 中加入更新模块,当被感染的 app 运行时,自动下载恶意负载。该技术使得升级攻击更难检测。升级攻击有以下几个手段:

(1)检测是否有更新会话,若有,则提示有新的版本可以更新,用户自主选择安装新版本,但是这个新版本是增加恶意负载的。

(2)由第三方数据库提供合法的更新提示功能,这个功能类似于 Google 信息自动提示模型。通过第三方数据库给用户发送更新提示,用户在网络上远程下载一个带恶意负载的新版本软件。

(3)不经过用户同意,偷偷更新部分组件。

2.1.3　路过式下载

不同于传统 PC 路过式下载技术主动挖掘浏览器漏洞,手机路过式下载攻击采用在 app 嵌入广告,引诱用户下载“感兴趣”的 app。当用户点击广告,就可能被引导到一个恶意网站或一个虚假的 Android 市场。另一种路过式下载方式是,当用户使用 PC 某个软件时,可能会被推荐下载相关手机 app,然而下载的这个

app 很可能是一个恶意软件。

2.2 恶意软件激活方式

通过记录相关系统事件,Android 恶意软件借助内嵌自动事件通知和 Android 回调函数,灵活触发其恶意行为。Android 系统常见的系统事件如表 1 所示。

表 1 Android 常用系统事件

缩写	事件
BOOT	BOOT_COMPLETED
CALL	PHONE_STATE
	NEW_OUTGOING CALL
PKG	PACKAGE_ADDED
	PACKAGE_REMOVED
	PACKAGE_CHANGED
	PACKAGE_REPLACED
	PACKAGE_RESTARTED
	PACKAGE_INSTALL
SMS	SMS_RECEIVED
USB	UMS_CONNECTED
	UMS_DISCONNECTED
BATT	ACTION_POWER_CONNECTED
	ACTION_POWER_DISCONNECTED
	BATTERY_LOW
	BATTERY_OKAY
	BATTERY_CHANGED_ACTION
NET	CONNECTIVITY_CHANGE
	PICK_WIFI_WORK
MAIN	ACTION_MAIN
SYS	USER_PRESENT
	INPUT_METHOD_CHANGED
	SIG_STR
	SIM_FULL

其中,大部分 Android 恶意软件有监听 BOOT_COMPLETED 事件的行为。系统启动的同时是运行恶意软件的最好时机。系统启动后,BOOT_COMPLETED 事件被触发,因此恶意软件一旦检测到该事件,就开始自动运行。此外,SMS_RECEIVED 也经常被恶意软件监听,通过监听该事件,恶意软件能够拦截或回应收到的 SMS 信息。

特定恶意软件监听多种系统事件,例如,AnserverBot 监听 10 种事件的回调函数,BaseBridge 监听 9 种事件。通过这些事件,恶意软件可以较稳定地开启其恶意行为。另外,还有一些恶意软件直接拦截所有事件,于是恶意软件能够在手机原始 app 运行前快速启动。

2.3 恶意负载

根据具体行为,可以将 Android 软件划分为四类:权限提升、远程控制、经济消费、隐私窃取。

2.3.1 权限提升

Android 平台是由 Linux 内核和超过 90 个开源数据库构成的复杂系统,系统的复杂性带来的问题就是,平台漏洞将可能导致系统权限提升。表 2 列出了目前已知可用于提升权限的 Android 平台漏洞和采用该漏洞的恶意软件。

表 2 Android 平台漏洞及恶意软件

平台漏洞	采用漏洞的恶意软件
Linux kernel	Asroot
init	DroidDream,zHash
	DroidKungFu
adbd	DroidDream, BaseBridge
	DroidKungFu[1235]
zygote	DroidDeluxe
	DroidCoupon
vold	GingerMaster

同样的,某个恶意软件会利用两种或两种以上的漏洞以最大化多平台下成功提升权限的机会。

早期的恶意软件仅简单利用已知漏洞用于提升权限。随后,技术发生变化,部分恶意软件先将漏洞挖掘程序加密存储为资源文件,运行时,动态解码这些挖掘程序。另外还有些恶意软件将发掘程序文件伪装成其他正常文件。

2.3.2 远程控制

大多数有远程控制功能的恶意软件通常把被感染的手机变成僵尸手机以便远程控制。有些家族的恶意软件使用基于 HTTP 的网站通信功能接收控制指令,还有一些恶意软件尝试加密远程 C&C(命令与控制)服务的 URL。

攻击者多在其控制的域中注册 C&C 服务器;也有些攻击者在公用云中建立 C&C 服务器,例如 Plankton 间谍软件从亚马逊的云端动态获取并运行其负载;甚至有些攻击者将共用博客服务器当作他们的 C&C 服务器,如 AnserverBot 使用新浪和百度博客服务器。

2.3.3 经济消费

攻击者大多从经济角度出发制造恶意软件,因此伴有恶意扣费的手机恶意软件十分常见。扣费方式通常包括发送高昂费用的短信、私下订制收费服务、自动网络连接等。

许可函数 sendTextMessage,允许不需用户知晓就能在后台发送 SMS 信息。有时,自动订购收费服务需要回复服务提供商的确认 SMS 信息以激活服务。为避免用户知晓这一行为,恶意软件自行回复这些确认信息。同样的,为避免用户发现账单消息,恶意软件自动过滤掉账单 SMS 消息。

除了订购收费项目,恶意软件还可能向其他手机发送消息,尽管没有前一个方式那么严重,但若是在用

户不知晓的情况下无限制发送信息,造成的经济损失也不可估量。

2.3.4　隐私窃取

绝大多数恶意软件都含有隐私窃取行为,可能窃取的用户隐私多种多样,包括 SMS 消息、手机号码、用户账户、密码等。由于 SMS 信息中可能含有用户证书,所以凡是收集 SMS 信息的行为都应高度关注。

3　结束语

通过分析总结已知 Android 平台下恶意代码行为特征,可以看出,Android 恶意软件行为多种多样。八成以上恶意软件重包装其他合法 app。然而,检测每天出现的大量 app 是否经过重包装是一个巨大挑战,同时大量第三方 Android 市场上众多 app 的出现也增加了检测难度。超过三分之一的 Android 恶意软件发掘平台漏洞来提升它们的权限。此外,由于缺乏对相关 API 的良好控制,半数左右的恶意软件在后台通过 SMS 信息订购收费服务。

当前 Android 市场存在众多问题,然而现存的手机安全防护软件依然落后于恶意代码技术的发展,不能提供有力保障。传统的基于签名方法并不适用于手机恶意软件检测,同时由于手机资源和电池容量约束,在手机上部署复杂的监测技术也不现实。因此,提出有效的手机恶意软件检测技术与模型至关重要。

参考文献:

[1] 王　伟. Android 病毒行为自动分析工具的设计与实现[D]. 天津:南开大学,2012.

[2] 吕海军,陈前斌,吴小平. 智能手机病毒的发展及其对策研究[J]. 信息安全与通信保密,2008(1):80-82.

[3] 杨卫军,余彦峰,张佩军. Android 手机恶意软件取证技术研究[J]. 警察技术,2012(5):8-11.

[4] 翁雪城,场零江. 恶意代码的分析与检测技术的研究[J]. 科技资讯,2012(5):19-20.

[5] Christodorescu M,Jha S. Static analysis of executables to detect malicious patterns[C]//Proceedings of the 12th conference on USENIX security. Berkeley,CA,USA:[s. n.],2003.

[6] 孙润康,展　娴,邵玉如,等. Android 手机安全检测与取证分析系统[J]. 信息网络安全,2013(3):71-74.

[7] 童振飞,杨　庚. Android 平台恶意软件的静态行为检测[J]. 江苏通信,2011,5(1):39-42.

[8] Rieck K,Holz T,Willems C,et al. Learning and classification of malware behavior[C]//Proc of detection of intrusions and malware,and vulnerability assessment. [s. l.]:[s. n.],2008:108-125.

[9] Christodorescu M,Jha S,Kruegel C. Mining specifications of malicious behavior[C]//Proceedings of the 1st India software engineering conference. [s. l.]:[s. n.],2008:5-14.

[10] Egele M,Scholte T,Kirda E,et al. A survey on automated dynamic malware analysis techniques and tools[J]. ACM Computing Surveys,2012,44(2):6-47.

[11] Burguera I,Zurutuza U,Nadjm-Tehrani S. Crowdroid:behavior-based malware detection system for Android[C]//Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices. Chicago:ACM,2011:15-26.

[12] Schmidt A D,Bye R,Schmidt H G,et al. Static analysis of executables for collaborative malware detection on Android[C]//Proc of IEEE international conference on communications. Dresden:IEEE,2009:1-5.

[13] 吴俊昌,骆培杰,程绍银,等. 基于权限分类的 Android 应用程序的静态分析[C]//第四届信息安全漏洞分析与风险评估大会. 北京:出版者不详,2011:41-48.

[14] Zhou Yajin,Jiang Xuxian. Dissecting Android malware:characterization and evolution[C]//Proc of IEEE symposium on security and privacy. San Francisco,CA:IEEE,2012:95-109.

(上接第 177 页)

签名方案[J]. 电子学报,2004,32(7):1062-1065.

[4] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory,1985,31(4):469-472.

[5] Ateniese G,Song D,Tsudik G. Quasi-efficient revocation of group signatures[J]. LNCS,2003,2357:183-197.

[6] Rivest R L,Shamir A,Adleman L. A method for obtaining digital signatures and public key cryptosystems[J]. Communications of ACM,1978,21(2):120-126.

[7] 史来婧. 基于中国剩余定理的群签名方案的研究[D]. 西安:西安电子科技大学,2012.

[8] 李新社. 群签名安全性分析与改进研究[C]. 西安:西安电子科技大学,2009.

[9] 邓宇乔. 基于动态属性的数字签名方案[J]. 计算机工程与应用,2013,49(15):19-22.

[10] 陈辉焱,李　巍,苏艳芳. 一种基于证书的代理环签名方案[J]. 计算机工程,2012,38(16):149-152.

[11] 程小刚,王　箭,杜吉祥. 群签名综述[J]. 计算机应用研究,2013,30(10):2881-2886.

[12] 陈道伟,施荣华,樊翔宇. 存在可实施强制签名特权集的门限群签名方案[J]. 计算机应用研究,2012,29(1):319-321.

[13] 黄　斌,史　亮,邓小鸿. 一个群签名方案的安全性分析[J]. 计算机工程,2013,39(4):151-153.

[14] Diffie W,Hellman M E. New directions in cryptograph[J]. IEEE Transactions on Information Theory,1976,22(6):644-654.

Android恶意软件特征研究

作者： 边悦， 戴航， 慕德俊， BIAN Yue， DAI Hang， MU De-jun
作者单位： 西北工业大学 自动化学院,陕西 西安,710072
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(11)