2012年第四季度中国移动互联网应用安全检测与分析报告

国家计算机网络应急技术处理协调中心

国家网络信息安全技术研究所软件安全评估中心

2013年2月

版权声明

国家网络信息安全技术研究所

2013 年 2 月

目 录

1 中国移动应用安全概况

1.1 安全概况

第四季度，移动互联网的应用总数持续增加，应用下载量也保持高速增长。据 2013 年 1 月 8 日苹果官方最新统计，App Store 应用总数已超过 77 万款，累积下载量高达 400 亿次（注：不包括重复下载和升级次数），其中 2012 年下载量达到了 200 亿次，仅 12 月单月下载量达到了 20 亿次；谷歌应用商店 Google Play 应用数量超过 80 万，用户总下载量超过 250 亿次；我国活跃的 24 家 Android 非官方应用商店中发布的应用总数已超过 160 万款（注：该数据没有考虑重复情况）。

截至 2013 年 1 月 8 日，即本期报告撰稿日期，国家网络信息安全技术研究所软件安全评估中心（以下简称“本中心”）对我国 4 家官方商店、24 家 Android 非官方商店和 7 家 IOS 非官方商店进行了安全检测分析，相比上期报告统计结果[1]，我国第四季度移动应用安全状况出现了新的发展迹象，主要体现在如下几方面：

1）**Android 非官方应用商店中仍然发现较多的恶意应用，本期从新采集的 97250 款应用样本中检测发现 860 款恶意应用，且下载量惊人，超过 850 万次。**本季度统计的数据大部分来自于 Android 国内非官方应用商店，在本期检测的样本中，对 97250 款应用程序进行了恶意检测，97250 款应用中检测出 860 个恶意应用，其中共发现 910 个手机病毒，下载量超过了 850 万，安全形势不容乐观。在统计范围

[1] 2012 年第三季度中国移动互联网应用安全分析报告，
http://www.cert.org.cn/publish/main/47/2012/20121231133721780244799/20121231133721780244799_.html

内的各个应用商店中，仍然能发现大量新增的恶意应用，截止撰稿日期，本期发现的 860 款应用仍有 600 款尚未下架，且下载量继续增加。

2）**Google Play 恶意应用仍有 4 款尚未下架。**在上期报告中，本中心发现有 12 款恶意应用存在于谷歌官方商店 Google Play 中，并且截止上期报告撰稿日期，12 款应用中尚有 4 款还未下架，且累积下载量高达 650 万。这 4 款恶意应用分别是 EAGLE NEST - Sniper training(v1.26)、Basketball Tour GOLD(v2.0)、iStreet Basketball PRO(v2.0)、Ball Tennis Gold(v1.0)。

3）**部分国内应用商店调整应用安全审核机制。**本季度，安机网的应用商店整体下线，不再作为应用商店的形式提供下载，转而发布自己的 Android 终端检测平台，从应用平台过渡到安全检测平台。豌豆荚在审核机制上作了一些调整，逐渐限制开发者直接上传应用，并向搜索其他官方和非官方应用商店的聚合引擎方向发展。针对目前 Android 应用的混乱现状，豌豆荚在应用信息中加入了“绿色标签”机制；此外，豌豆荚在 12 月中旬开设了“优质开发者专区”，进一步筛选推荐安全优质的应用，而对优质应用的审核细则还在修改调整当中。

4）**Windows Phone Store 成为移动互联网领域近期关注的新焦点。**由于微软加大了在 Windows Phone 上的投入力度，本季度 Windows Phone Store 有了较大的发展。现在的 **Windows Phone Store 拥有比其他应用商店更严格的审核机制和安全机制，**审核机制包括**开发者中心账户验证机制、软件审查机制**和**应用商店下载机制**三方面。这种严格的安全审核机制，可能成为部分非官方应用商店效仿的对象，

也可供相关管理部门参考借鉴。

1.2 报告依据

1.2.1 涉及应用商店

本报告将涉及的移动应用商店分为两大类：官方应用商店和非官方应用商店。具体涉及的官方应用商店如下表所示。

公司	应用商店	网址	平台
苹果	App Store	itunes.apple.com	IOS
谷歌	Google Play	play.google.com/store	Android
微软	Windows Phone Store	www.windowsphone.com	Windows Phone
诺基亚	诺基亚 OVI	store.ovi.com.cn	Symbian

非官方应用商店主要包括第三方应用市场、电信运营商应用商店、终端制造商、定制系统提供商等。

本报告针对应用总数和下载量较大的应用商店，选取了包括上述官方和非官方在内的 30 多家应用商店作为检测分析对象。其中，本报告重点检测分析 24 家 Android 第三方应用商店，其具体信息如下表所示。

表 1-1 本报告重点检测分析的 24 家 Android 第三方应用商店简介

公司	应用商店	网址	类型	应用量
百度	百度应用中心	as.baidu.com	第三方	28490
腾讯公司	应用宝	android.myapp.com/	第三方	24026
华为技术有限公司	智汇云应用市场	app.hicloud.com/	终端制造商/定制系统提供商	6853
奇虎 360	360 应用中心	zhushou.360.cn	第三方	5539
机锋网	机锋市场	apk.gfan.com/	第三方	3758
搜狐公司	搜狐应用中心	download.sohu.com/	第三方	3617
飞鹏网	飞鹏网	www.fpwap.com/	第三方	3183
网易公司	网易应用中心	m.163.com/android/i	第三方	2789

		ndex.html		
N 多网	N 多市场	www.nduoa.com/	第三方	2742
当乐网	当乐网	www.d.cn/	第三方	2681
安粉网	安粉网	www.appfun.cn/	第三方	2291
七匣子	七匣子市场	www.7xz.com/	第三方	1679
小米网	小米应用商店	app.xiaomi.com/	终端制造商/定制系统提供商	1536
木蚂蚁	木蚂蚁市场	www.mumayi.com/	第三方	1291
天网手机软件下载站	天网安卓专区	android.waptw.com/	第三方	1090
中关村在线	ZOL 应用中心	sj.zol.com.cn/	第三方	574
阿里巴巴集团	淘宝应用市场	app.taobao.com/index.htm	第三方	186
手机中国	手机中国	app.cnmo.com/	第三方	111
福建网龙计算机网络信息技术有限公司	91 手机娱乐	sj.91.com/download/	第三方	91
安卓网	安卓市场	apk.hiapk.com/	第三方	77
安机网	安机市场	www.anshouji.com/	第三方	77
北京掌汇天下科技有限公司	AppChina 应用汇	www.appchina.com	第三方	61
优亿网	优亿市场	www.eoemarket.com/	第三方	14
北京力天无限网络技术有限公司	安智市场	www.anzhi.com	第三方	4

1.2.2 不良行为分类

本中心制定了一套严格的应用行为分类方法，根据应用行为的安全威胁程度将其分为恶意行为、可疑行为和灰色行为，这三类行为统称为不良行为。其中，恶意行为指明确带有恶意目的并且会对系统和用户利益造成直接侵害的行为；可疑行为是指存在一定风险，但不能直接被确认为恶意行为的行为；灰色行为是指通过后台进行特定网络访问，但又难以判断是否具备恶意目的的行为，主要指的是嵌入广告的流氓行为。

1.2.2.1 恶意行为

本报告提及的“恶意行为”具体类型、威胁级别等信息详见下表：

表 1-2 恶意行为分类具体信息

恶意行为类型	典型代表	威胁级别	说明
损害系统	Kungfu	极高	后台释放应用程序，修改系统分区嵌入至 ROM、感染后极难查杀，同时会主动连接控制服务器接收控制命令。是目前为止危险性最高的流行病毒。
	Updtkiller	极高	诱导用户激活设备管理器，导致用户无法卸载。破坏安全软件功能，给手机带来了安全威胁。
资费消耗	Gappusin	高	首次运行后在后台会访问网址 www.xxandroid.com，获取用来下载其他程序的 URL 列表保存在本地。样本在每隔一段时间通过 URL 列表下载 apk 文件，每次下载一个，并伪造“系统更新”通知，骗取用户点击安装所下的程序。样本每隔一段固定的时间会访问 www.00android.com 更新 url 列表。

	Gamex	极高	诱导用户获取 ROOT 权限，在未经用户允许情况下，私自静默安装携带的多款恶意安装包，这些安装包又会私自联网、偷偷下载其他恶意应用，并从云端配置推广软件列表，让用户手机彻底变成病毒的“天堂”。
	FakeInstall	高	会向收费服务的电话号码发送消息，无需用户同意，便可将自身伪装成合法的安装程序。
	SmsSend	高	具有不经用户同意，通过后台向收费服务电话号码发送消息。
隐私泄露	Smsblocker	高	具有拦截电话、短信息行为，并且可以私下记录用户 MobileMarket 登录账户密码，并发送到指定号码，远程指令控制用户手机下载指定程序。
	Ginmaster	高	会将中毒手机的手机号、IMEI 串号等信息传送到病毒作者指定的服务器。
综合危害	ADRD	极高	开启多项系统服务；每 6 小时向控制服务器发送被感染手机的 IMEI、IMSI、版本等信息；接收控制服务器传回的指令；从数据服务器取回 30 个 URL；依次访问这些 URL，得到 30 个搜索引擎结果链接；在后台逐一访问这些链接；下载一个 apk 安装文件到 SD 卡指定目录。感染该木马的手机将产生大量网络数据流量，从而被收取流量费用。攻击者通过增加搜索链接的访问量而获益。
	BgServ	极高	具有向控制服务器发送手机隐私信息、发送扣费短信、拦截中国移动和中国联通客服短信等能力。
	DroidDream	高	通过 Android 已知的 exploid 和 rageagainstthecage 漏洞提取 root 权限并且在后台静默安装了一个内嵌的 com.android.providers.downloadsmanager 的包，搜集手机部分信息发送到特定的服务器并在后台下载一些其他的恶意安装包，将给用户手机带来严重的安全威胁。

	Killall	高	会自启动上传手机 IMEI、手机号码、SD 卡容量等信息到指定服务器并伪造系统升级诱骗用户下载安装指定 apk。
	Geinimi	高	启动后，将通过其含有的恶意插件后台联网，并泄露用户手机隐私信息，同时会在后台下载其它恶意软件保存到 sdcard/system/app 目录和其他目录。不但消耗用户资费，更可能通过下载其它恶意程序，给用户造成进一步的损失。

1.2.2.2 敏感行为

本报告提及的“可疑行为”具体类型、威胁级别等信息详见下表：

表 1-3 移动智能终端应用程序典型可疑行为

可疑行为类型	行为内容	威胁级别	说明
隐私泄露	得到设备 ID	中	部分应用程序使用设备的 IMEI 号码来做为唯一的识别码，类似网站的 cookies 使用。甄别其是否为恶意行为的关键在于应用程序是否将设备 id 泄漏。
	得到位置信息	中	大部分基于 LBS 的应用程序会主动获取应用程序的位置信息，是否为甄别为恶意行为的关键是分析应用程序获取位置信息之后是否有泄露用户隐私的嫌疑。
	得到 SIM 卡序列号	中	此行为本身并不存在恶意性，但是恶意程序通常都会通过该行为得到 SIM 卡序列号，从而得知可以在该设备上进行哪些操作，之后进一步进行其他的恶意行为。实践说明，很多恶意程序都会事先得到 SIM 卡序列号，得知可以进行的操作，之后在进行真正的恶意行为。
隐私泄露/资费消	自动发送短信/彩信	高	在用户不知情的情况下后台发送短信，属于可疑行为中最为危险的一种，因为这种短信或者

耗			彩信往往就是向 sp 订制的信息，或者就是泄漏用户的隐私信息。
资费消耗	自动连接网络	中	在用户不知情的情况下连接网络，会耗费用户流量。通常情况下，自动连接网络的行为为访问广告提供商的网站，也存在访问钓鱼网站的情况。
	访问应用商店	中	一部分应用程序会在后台访问应用商店，获取其中的一些版本信息甚至是一个新的应用程序。这种行为一方面损耗了用户的流量，另一方面，也有一部分恶意应用程序在访问应用商店后直接进行后台下载、安装。
其他	创建快捷方式	低	有一部分应用程序会在运行后自动在桌面创建快捷方式，以引起用户的注意。此类行为虽然不会造成用户的直接损失，但是却并非用户本意。
	自动连接 wifi	低	程序会自动将 wifi 设置为可用，并且尝试连接可用的 wifi。此行为不会造成直接经济损失，但是会造成用户设备电量损耗等其他负面影响。
	得到网络类型	低	对于一个正常的网络应用程序，对网络类型的判断是极为正常的行为。鉴别此行为是否为恶意行为的关键在于是否将网络类型信息通过某种手段发送到网络上或者其他用户的设备上。
	自动开启蓝牙	低	此行为不会造成直接的经济损失，但是存在一定的危害。一方面，蓝牙对设备电量的损耗比较大，容易使用户设备待机时间变短；另一方面，有一部分手机木马、蠕虫则通过蓝牙进行短距离传播。判断此行为是否为恶意行为的关键是判断之后是否执行了网络命令，或者进行了蓝牙传输。
	自动搜索蓝牙设备	低	此行为主要会损耗用户设备电量。另外一部分恶意程序在这个行为之后，将一部分数据、信息乃至应用程序发送到已经连接的设备上，造成用户信息损失。

1.2.3 检测分析样本

一、本中心从 24 家应用商店中随机抽取 **97250 款应用作为恶意行为检测分析样本**，样本涵盖游戏、娱乐、工具等主要类型的应用，并侧重几家应用商店进行采样，本次采样的样本分布如下图所示。

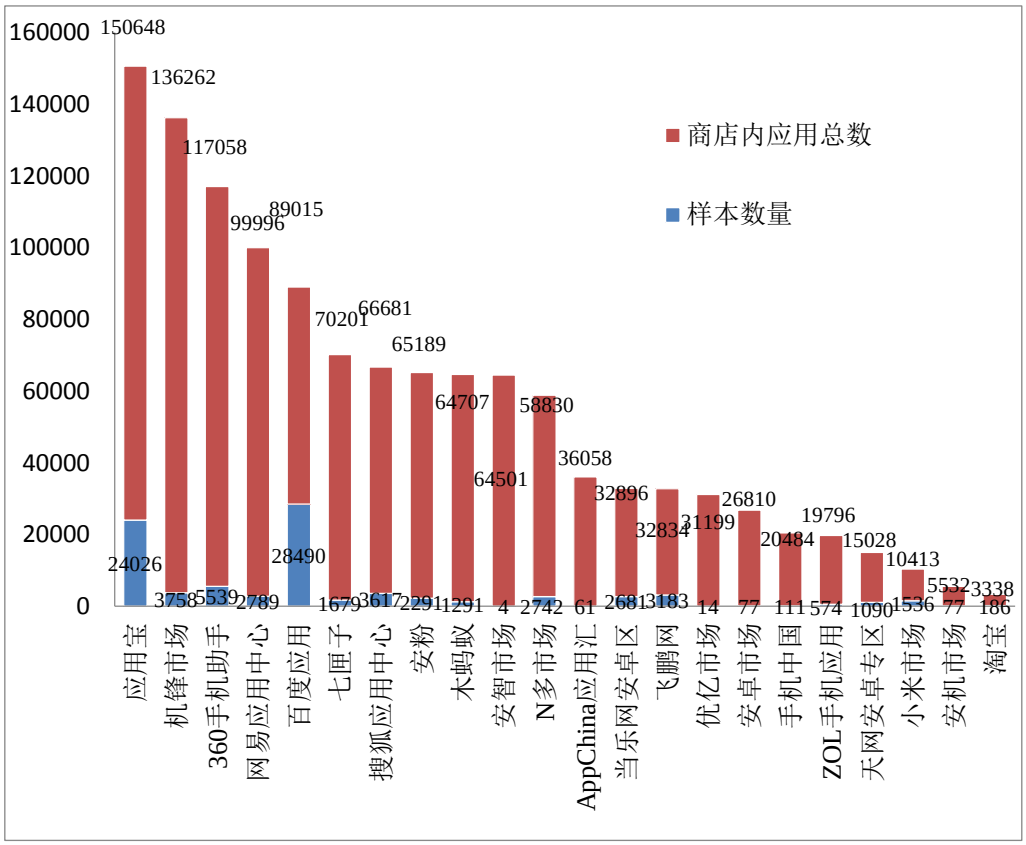


图 1-1 应用样本分布 1

本期报告主要抽取几家应用商店进行重点检测与分析，后续发布的报告会逐渐均衡各家应用商店的应用采样比例。

二、本中心从 24 家应用商店中随机抽取超过 157363 款应用作为**可疑行为检测分析样本**，样本同样涵盖了游戏、娱乐、工具等主要类型的应用，本次采样的样本分布如下图所示。

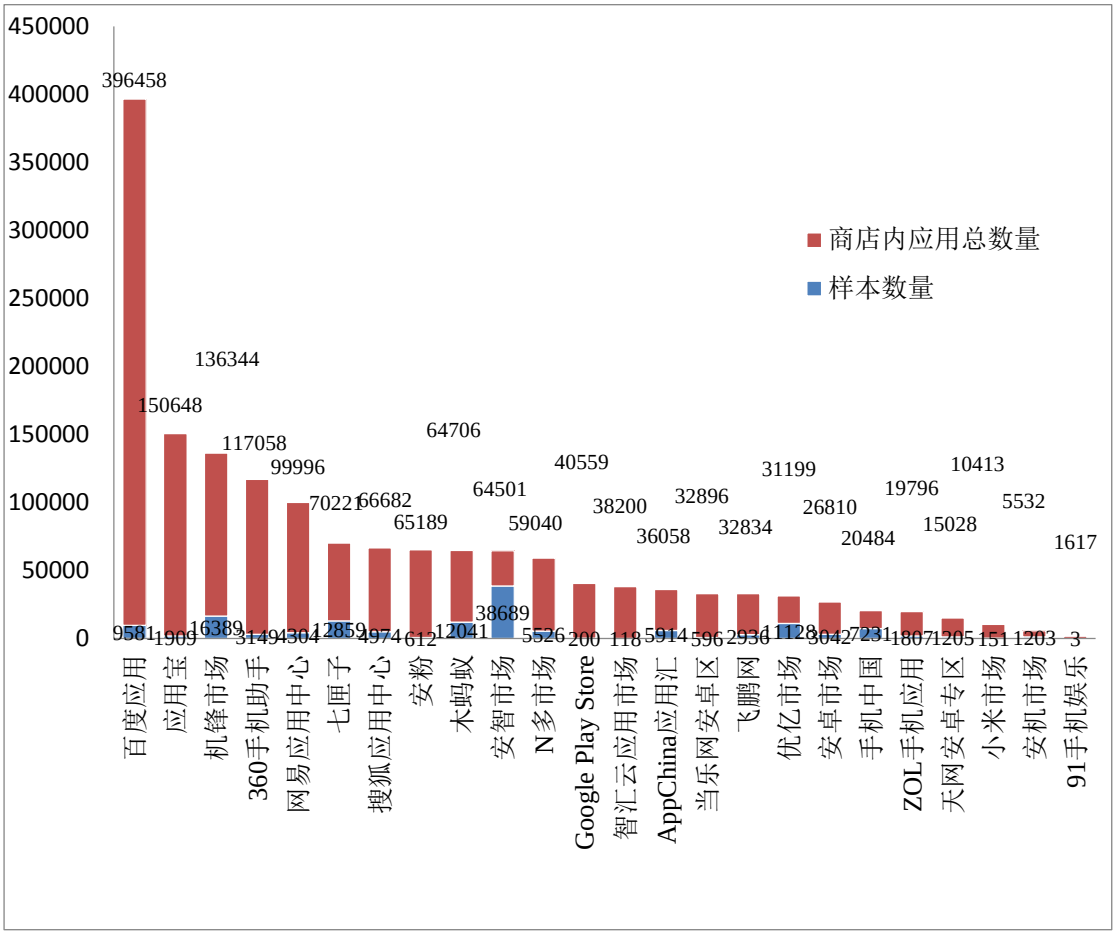


图 1-2 应用样本分布 2

如图所示，百度应用总量远高于其他应用商店，这是因为百度应用聚合了其他应用商店的应用链接，在接近 40 万的应用中，仅有 9 余万应用是百度应用自己的链接，其他链接则来自于聚合的其他应用商店。

2 安全数据展示与解读

2.1 应用商店管理现状

2.1.1 Google Play 等官方应用商店继续完善安全审核机制

谷歌在 2012 年第二季度发布了 Google play 最新的开发人员应用政策[2]，涉及到应用程序命名、应用程序图标、支付、隐私、垃圾邮件和广告等多方面的审核标准，如果开发者违反这些规则并且没有在 30 天改正期内进行更正，那么他们将被 Google Play 除名。

苹果的 App Store 官方应用商店一直执行着严格的审核机制，开发商在任何时候都必须严格遵守苹果商店的各项规定，对于被审核人员认为存在不恰当或违法内容的应用，苹果绝对不会将其发布到商店中，即使是因为运行错误、Bug 等技术问题，苹果也不会允许应用出现在应用商店中。

诺基亚的 OVI 商店也提供了一套完整且简单易懂的内容发布指南供参考，所有发布在 OVI 商店里的内容将会由诺基亚的质检部门严格把关。

2.1.2 Windows Phone Store 具有目前最为严格的安全审核机制

微软的官方商店 Windows Phone Store 厚积薄发，提出了目前最为严格的安全审核机制，包括如下三个方面：**开发者中心账户验证机制**、**软件审查机制**和**应用商店下载机制**。

[2] http://support.google.com/googleplay/android-developer/answer/2519872?hl=zh-Hant

http://support.google.com/googleplay/android-developer/answer/113469?hl=zh-Hant&ref_topic=2897388

(1)开发者中心账户验证机制

Windows Phone 开发者如果想开发并发布应用到官方商店，那么他首先需要注册创建 Microsoft 账户，之后在微软的开发者中心注册账户。开发者中心的账户分为公司账户和个人/学生账户两种，学生账户需要提供学生身份证明，企业账户需要进行身份验证，开通账户需要通过 Symantec 的验证。Windows Phone 开发者中心对开发者注册账户进行验证，一方面有助于保护公司和个人的身份信息，防止其在不知情的情况下被使用，并加强购买应用程序者对公司的信任；另一方面有助于对上传应用的审查，避免非法账户上传应用，保护被购买应用程序的利益。

(2)软件审查机制

Windows Phone Store 对应用软件采用与苹果 App Store 一样的人工审查机制，一款应用程序从开发者上传、商店审查至在商店发布，大概需要五至七天的时间。应用商店将根据应用认证要求[3]中的策略和要求，对所有应用及应用内产品进行验证，只有符合要求，才能够在 Windows Phone Store 中发布。

(3)应用商店下载机制

目前 Windows Phone 官方商店应用主要的下载的方式是通过 Windows Phone Store 的手机客户端直接下载并安装应用到手机上，此外 Windows Phone 也支持通过计算机端进行应用下载，然后通过 SD

[3] 具体标准 http://help.wandoujia.com/entries/22854241

卡将软件安装到手机的方式。

Windows Phone Store 为了保护开发者的利益，保证应用和游戏软件的正版版权，采用了**内容数字版权加密保护技术(以下简称 DRM 技术)**和**加壳混淆**技术以防止对他人对 Windows Phone 可执行应用程序的逆向工程。用户下载应用软件时，官方商店会在应用下载传输通道过程中使用 DRM 技术对下载的文件进行加密，有效地保护了应用软件的版权。对于使用过 DRM 技术的应用软件，用户只能将其复制到 SD 卡中，通过与微软官方商店通信的手段才能将应用安装到手机上使用。

IOS 应用破解原理是在已破解的 IOS 设备中安装应用，在解密完成之后把应用提取出来，得到破解的应用。而 Windows Phone 在下载的时候，加入的数字加密，需要手机实时与服务器通信，多次交换设备密钥。目前还没有黑客可以破解 Windows Phone，也没法把 Windows Phone 应用程序 xap 的数字加密给破解。

由此可见，目前已成为大家关注焦点的 **Windows Phone Store 采取了比苹果、谷歌和诺基亚更为严格的安全手段，不仅具备严格的安全审核机制，同时还有效地保护了开发者的版权**。

2.1.3 豌豆荚率先完善安全审核

本季度豌豆荚在审核机制上进行一些调整，使用了更严格的应用审核机制。目前豌豆荚逐渐限制开发者直接上传应用，并转向搜索其他官方和非官方应用商店的聚合引擎方向发展。

图 2-1 豌豆荚审核情况 1

图 2-2 豌豆荚审核情况 2

如上图 2-1、2-2 所示，所有以前在豌豆荚注册的开发者账户现在都不能正常使用，提示原因：“豌豆荚开发者中心内测已结束，根据国家相关政策规定及通知，开发者在注册开发者中心审核标准有所变动[4]，因此您需要重新提交注册申请，等待资质审核，同时您也可以在第三方应用商店上传管理您的应用，同样可以被豌豆荚搜索聚合，不会影响您的分发量。”

开发者在注册开发中心审核标准有所变动，具体审核标准包括以下多点：开发/代理商的基本资料及法律要件、应用元数据与资料、功能、推送通知、商标与商业外观、用户界面、渠道和聚合、人身攻击、暴力、不当内容、隐私、色情、宗教文化与种族、博彩与用户激励购买行为、激励下载与广告、其他。

此外，如下图 2-3 所示，豌豆荚发布了新版本的应用搜索，引入“绿色标签”机制，对应用的安全性、是否包含广告插件、正版与否、

[4] 具体标准 http://help.wandoujia.com/entries/22854241

以及对敏感权限的调用情况进行检测，以保障用户安全放心的下载体验。

图 2-3 豌豆荚“绿色标签”

针对 Android 应用质量良莠难辨，仿冒和山寨应用层出不穷、第三方广告和敏感权限滥用难以规范等混乱现状，豌豆荚在最新的应用搜索里引入了“绿色标签”机制，在搜索结果里为扫描检测合格的应用打上安全、无广告、Google 验证、以及信任权限标签。如下所示，为多款应用在豌豆荚中的显示情况。

图 2-4 豌豆荚应用样例 1

安全标签（无病毒）：接入腾讯、360、LBE 等厂商的安全引擎，针对手机病毒、扣费代码等风险进行全面扫描。豌豆荚在聚合每一款应用程序时，都会通过上述几款杀毒工具进行检测，如果没有检测到病毒或木马，那么豌豆荚就会将该应用聚合到自己的应用发布平台，并且加入响应的检测标签。用户在下载安装应用时，可以通过这个标签判断应用是否安全。

图 2-5 豌豆荚应用样例 2

无广告标签：检测广告平台模块，针对通知栏广告和内嵌广告有明显提醒。目前 Android 应用程序的盈利手段主要就是通过广告来营销的，因此大部分应用软件都会被嵌入广告。豌豆荚在聚合应用软件时，会通过自己的检测，获知该应用程序中是否有广告，并为其加上相应的检测标签。用户在选择应用程序时，可以通过这个标签判断应用中是否有广告，进而决定是否要下载该应用。

图 2-6 豌豆荚应用样例 3

信任权限标签：对没有经过认证信任的应用调用敏感权限的情况进行警示，预防通讯录等用户隐私信息的泄漏。用户在选择应用程序时，可以通过该标签判断该应用是否会对个人的隐私信息进行访问。对于新型病毒或木马，各大杀毒厂商有可能没有及时更新病毒库，而导致安全检测标签出现暂时性失效，而该标签则可就此为使用者提供一个判断依据。

图 2-7 豌豆荚应用样例 4

Google 验证标签：检验应用签名与 Google Play 中的是否一致，

如果一致则会判定为官方版，以确保应用没有被第三方篡改。Android 应用程序可以被第三方随意修改，然后重新打包、签名、上传。恶意用户可通过这种手段对 Google 官方应用进行重新深度定制修改，嵌入新型病毒或木马，伪装成 Google 官方应用程序，以逃避杀毒厂商的检测。但是重新打包容易，伪造 Google 官方签名却很难，而豌豆荚通过这种签名检测，可以明确地告诉用户，该应用是否是伪装的应用。

图 2-8 豌豆荚应用样例 5

豌豆荚中安全性被判为危险的应用会直接下架，被判为可疑的、或者有通知栏广告的应用绝不会出现在首页的各个推荐榜单，应用搜索的排名也会依据绿色标签进行优化。

此外，豌豆荚还针对优质开发者设立了“优质应用开发者”标签，并在 12 月中旬开设了“优质开发者专区”，进一步筛选推荐安全优质的应用，而对优质应用的审核细则还在修改调整当中。

2.2 应用安全威胁现状

2.2.1 官方应用商店应用保有量持续增加

截至到 2013 年 1 月，苹果公司 App Store 收到的应用提交总数达到 100 万，审核通过应用总数 77.5 万款，用户下载量超 400 亿次；谷歌应用商店 Google Play 应用数量为 80 万款，用户总下载量超过 250 亿次；WP 应用商店中现有应用已有超过 15 万款，相比 2012 年 11 月份增加 2.5 万。Nokia 公司的 OVI 商店的应用总数约 12 万款。结合 2012 年 11 月统计数据对比，如图 2-9 所示。

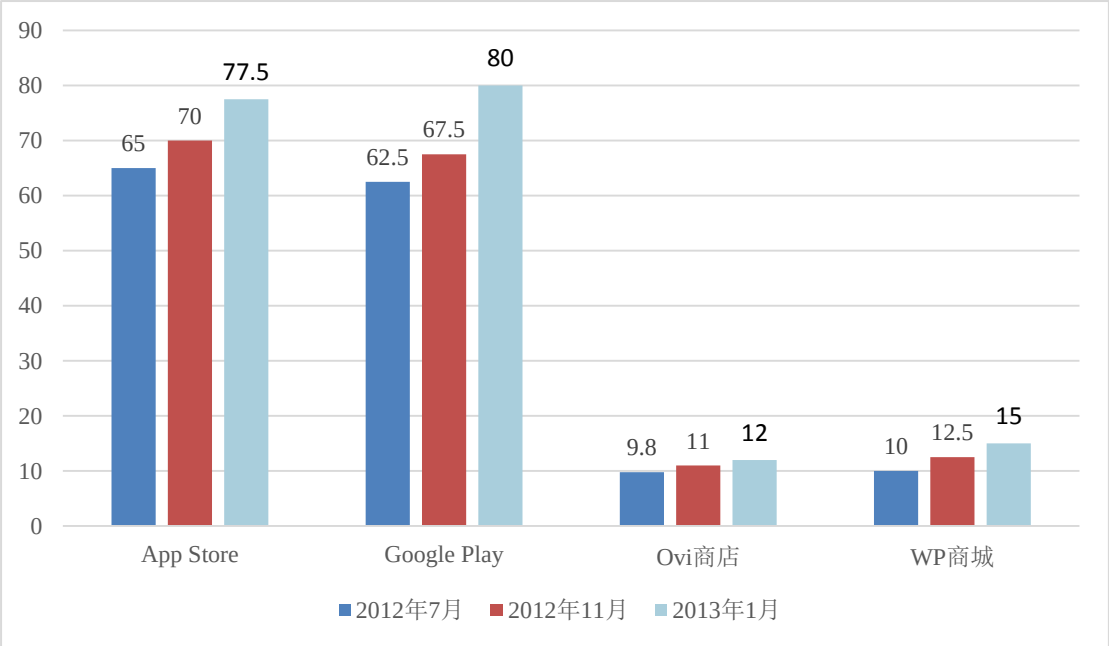


图 2-9 官方应用商店情况

App Store 和 Google Play 应用商店的应用数量远远超过其他两家应用商店的应用数量。因此，本报告主要针对 IOS 和 Android 两大平台的应用情况进行分析。

2.2.2 非官方应用商店应用保有量惊人

1. IOS 平台

本报告分别统计了猫人吧、手机中国等 7 家非官方 IOS 应用商店的应用保有量，截至 2013 年 1 月，这 7 家应用商店的应用数量超过 31 万款，具体分布情况如下图 2-10 所示。

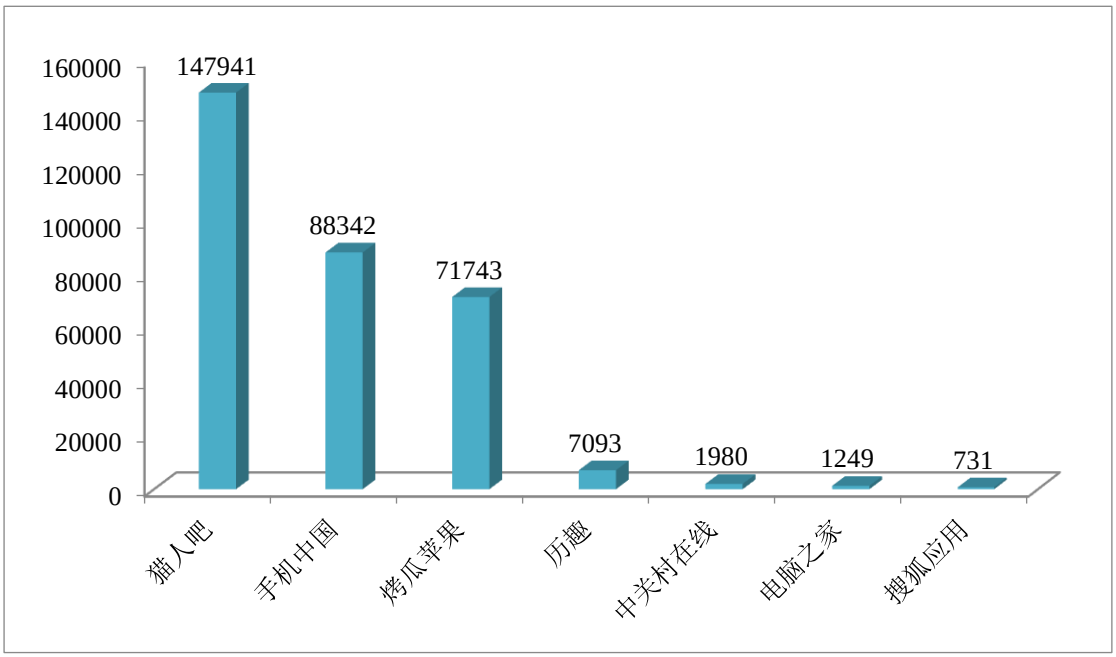


图 2-10 IOS 非官方应用商店应用数量

从上图 2-10 可以看出，目前有些主流的非官方 IOS 应用商店内应用数量已经相当庞大，譬如猫人吧的应用数量已经超过 14 余万款。由于本中心对部分 IOS 应用商店的信息收集工作刚刚起步，所以本中心平台中 IOS 应用数量还相对较少，譬如电脑之家的 IOS 应用数量只有 1000 余款，而搜狐应用的 IOS 应用数量甚至不及 1000 款。但是总体来看，和 Android 第三方应用商店相比来说，IOS 非官方应用商店数量较少，这和 IOS 更为封闭的系统特点有关。

2. Android 平台

2012 年 11 月，本中心在《2012 年第三季度中国移动互联网应用安全分析报告》中曾对机锋市场、安智市场等 22 个非官方 Android

应用商店的应用进行了统计分析。本报告中，除了上述 22 家非官方 Android 应用商店，本中心还增加了对 91 手机娱乐、智汇云应用市场 2 家应用商店的统计分析。在已统计的应用商店中，应用总数也由 11 月份的 140 多万款增长到 1 月份的 160 多万款。具体如下图 2-11 所示。

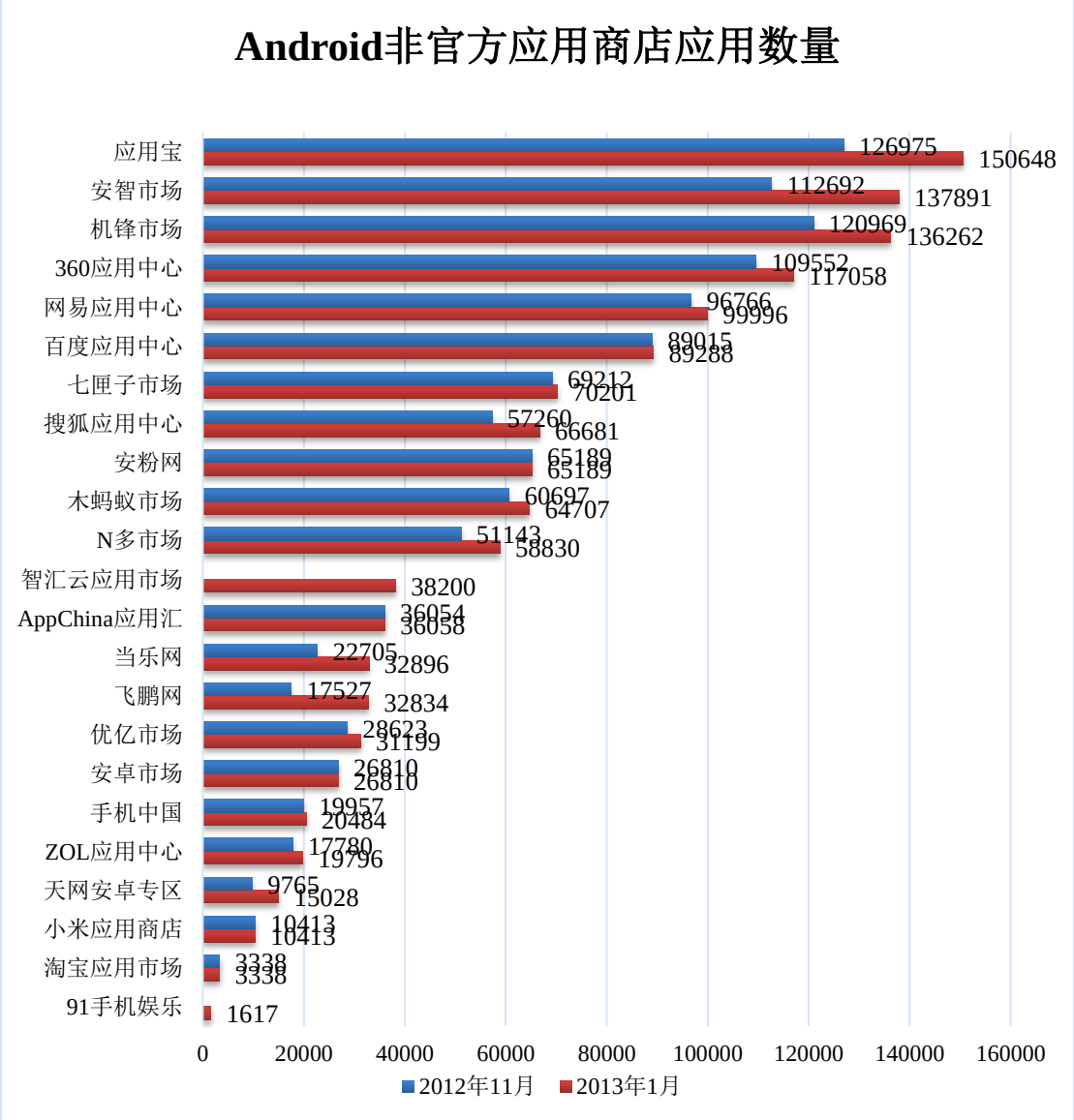


图 2-11 非官方 Android 应用商店应用数量

在本期统计中，由于安机市场从第三方应用商店转型成为 Android 手机验证网站，不再对外提供应用上传及下载等服务，因此

本期报告检测数据中不含安机市场应用数据。

2.2.3 Android 应用下载分布极度不均

截至本报告撰写日期，本中心从 Google Play 官方商店和 24 个第三方应用商店中选择了有下载量数据的 160 余万应用程序进行了下载量的统计，去除同一应用不同版本的重复情况，结果显示，**下载量超过 1 亿的应用程序只有 21 款；下载量高于 100 万次的软件不到一万款，只占应用总数的 0.4%；，88.5%的应用程序的下载量低于 5000 次，其中超过 72 万应用的下载量为零，约占总数的 45%。**应用下载量分段统计结果如图 2-12 所示。

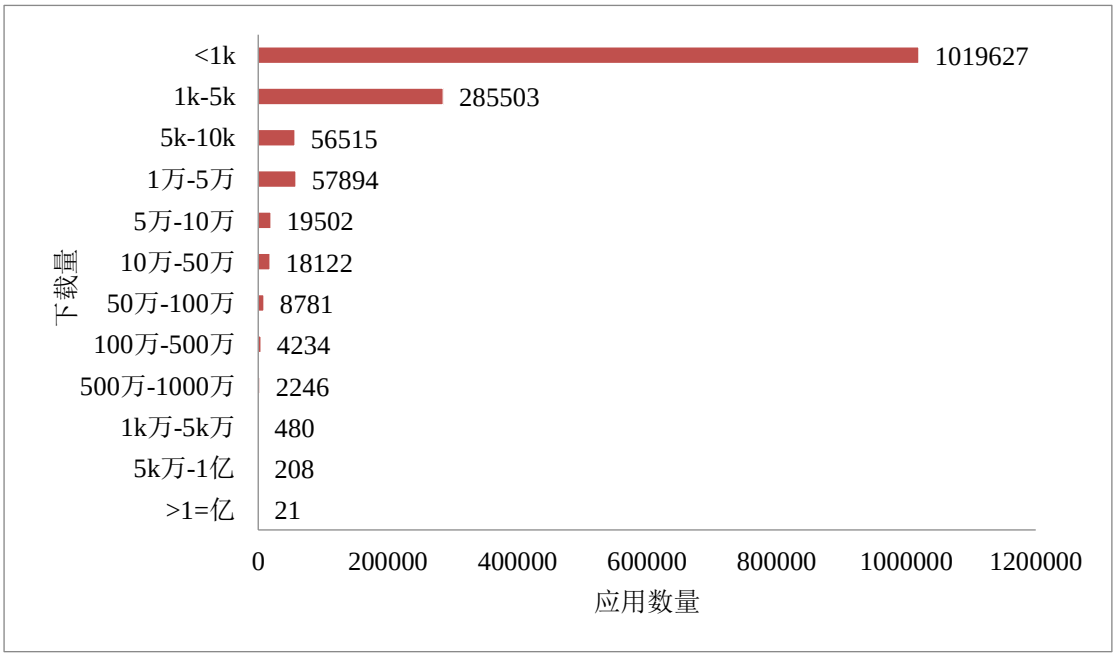


图 2-12 应用下载情况分布表(含 Google Play)

此外，本中心对上述应用统计数据进行了进一步分析，去除了统计应用中 Google Play 官方应用商店的应用程序，得到数据如下图图 2-13 所示。

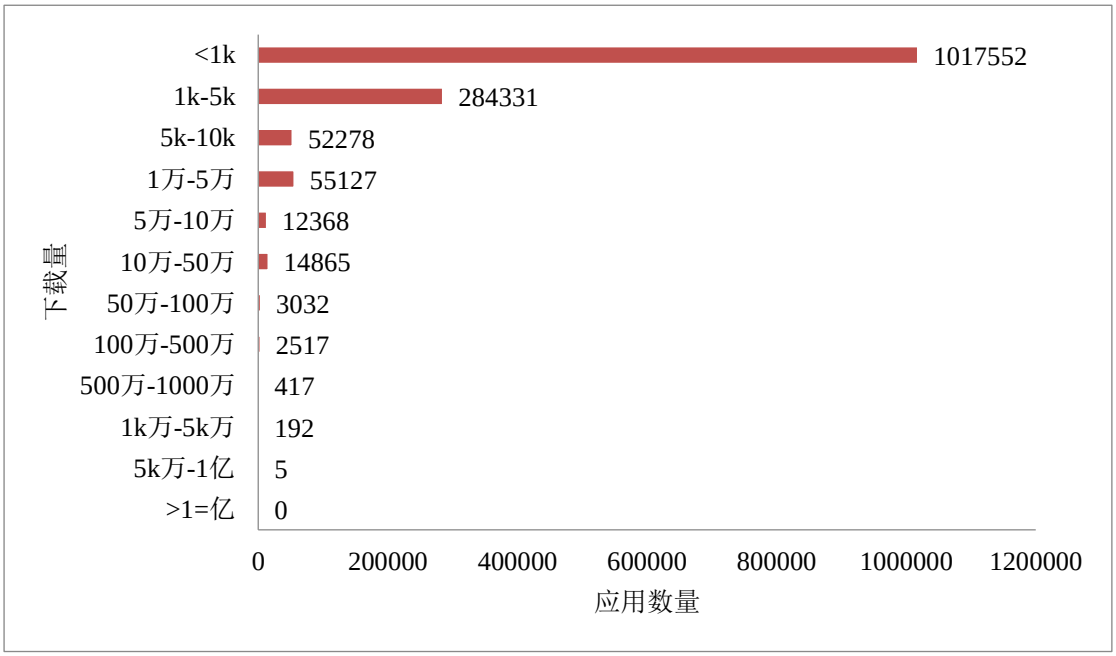


图 2-13 应用下载情况分布表(不含 Google Play)

从上图可以看出，**在国内第三方市场中，**超过 1000 万下载量的应用仅有 192 款，**超过 5000 万下载量的应用仅仅只有 5 款**。这 5 款应用全部出现在腾讯应用宝中，分别是腾讯微信（下载量为 8000 万次）、QQ 浏览器（下载量为 5000 万次）、手机 QQ2012（下载量为 7000 万次）、腾讯手机管家（下载量为 8000 万次）、腾讯应用宝（下载量为 8000 万次）。

2.2.4 抽查的 Android 应用商店均含恶意应用

本期报告从 24 家 Android 非官方应用商店中随机抽取超过 9 万应用样本进行安全检测，应用样本分布如下图 2-14 所示。

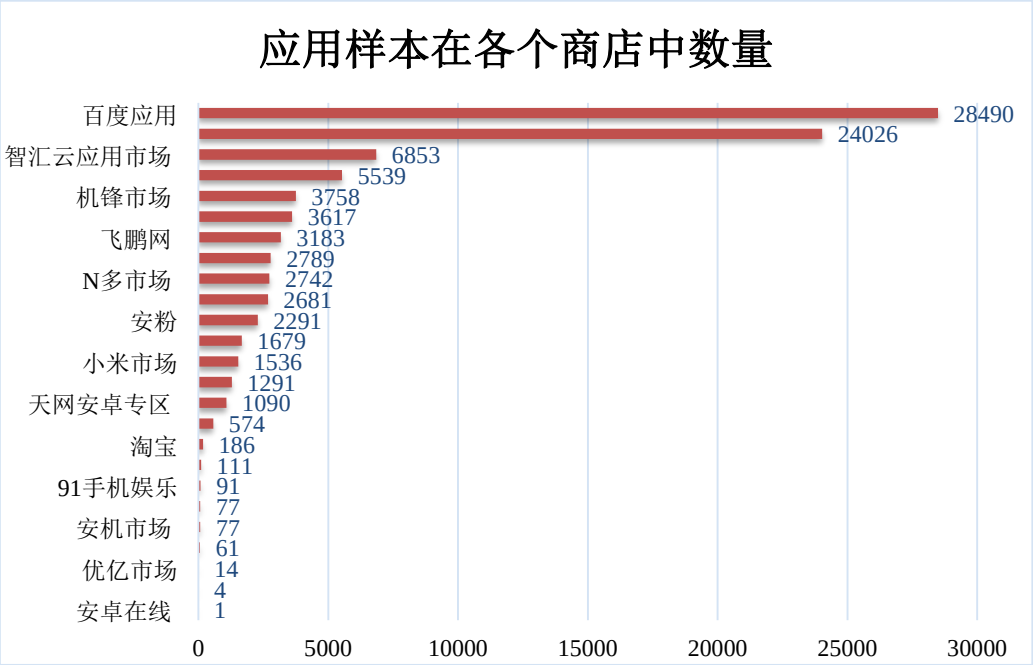


图 2-14 应用样本分布

分析结果显示，从 9 万应用样本中共发现恶意应用软件 860 款，恶意应用比例将近 9.5‰，且这 860 余款恶意应用的下载量超过 850 万次，平均每款恶意应用被下载接近 1 万次。截止撰稿日期，上述 860 款应用仍有 609 款仍然在架。各个应用商店内的恶意应用数据如图 2-15 所示。

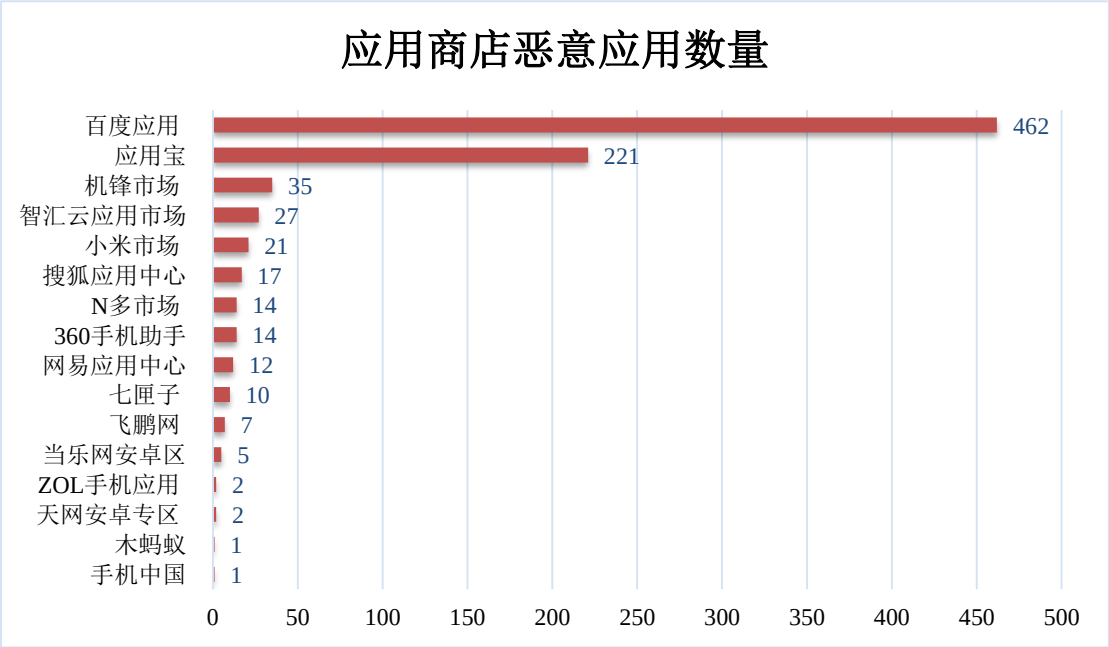


图 2-15 应用商店恶意应用数量图

下图 2-16 为各个应用商店中恶意应用的下载量统计结果。

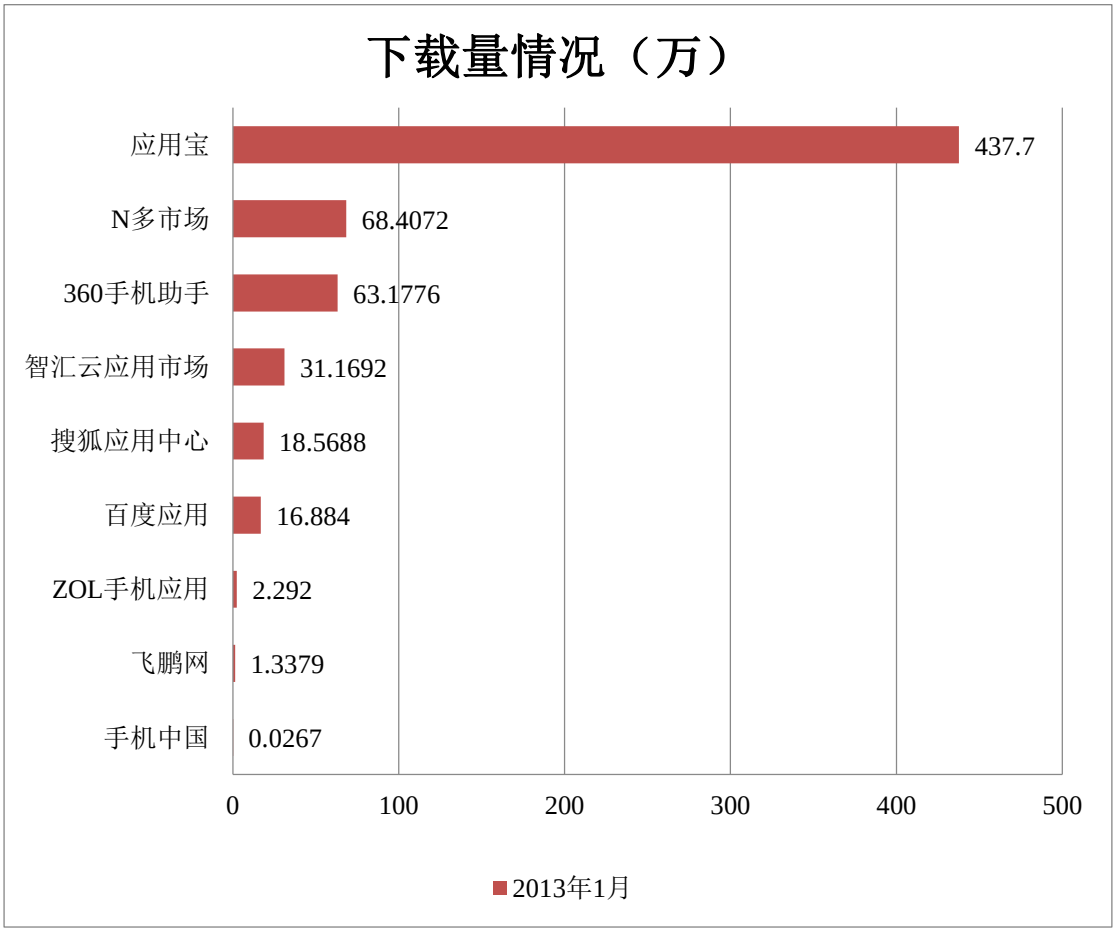


图 2-16 恶意应用下载量变化图

在上图中可以看出，在本季度统计中，腾讯应用宝中的恶意应用下载量巨大。需要注意的是，腾讯应用宝中有款名为“3D 狂暴赛车”的游戏，存在 android.troj.mdk 恶意威胁，下载量高达 400 万。此外，本季度，由于优亿市场和机锋市场不再对外提供应用下载量统计数据，因此这两个应用商店的恶意应用下载量为 0。

根据安全厂商的通用分类标准，本期报告发现的 860 个恶意应用的分类如下图所示。

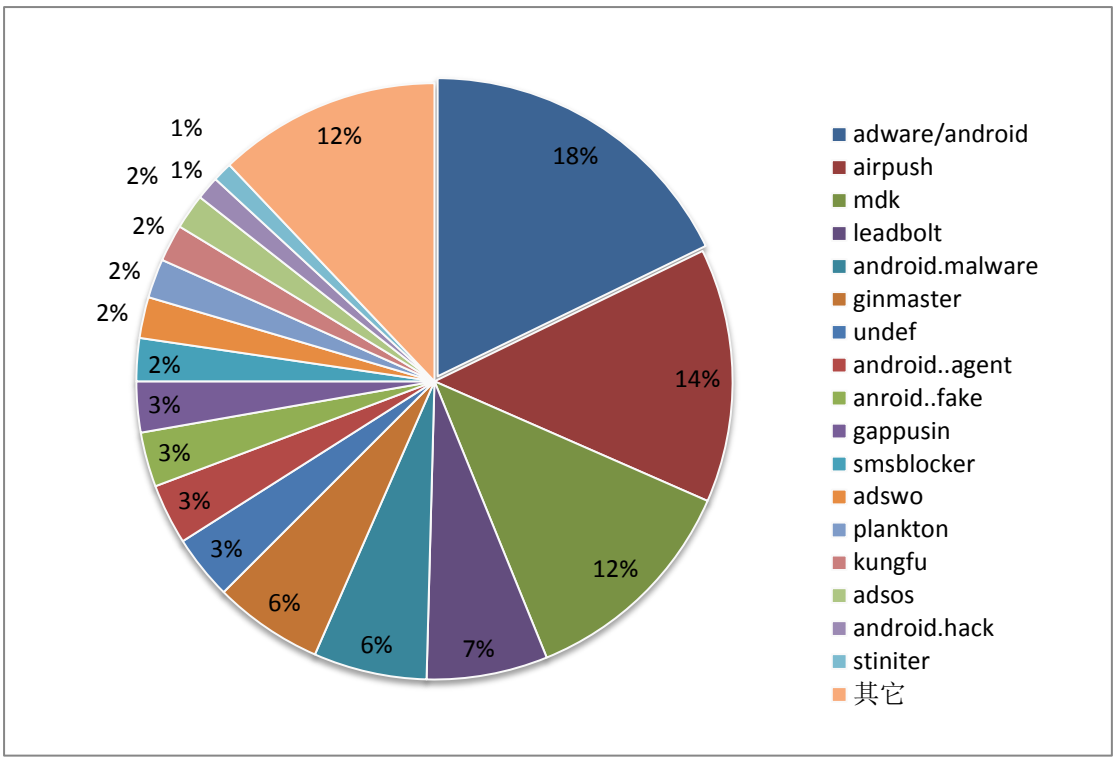


图 2-17 恶意应用程序比例图

如上图所示，**比例最大的三类恶意应用分别是 adware/android 病毒、airpush 病毒和 mdk 病毒，占总数的 44%。**图中各类病毒的介绍可参见本报告 1.2.2.1 小结。

在上期报告中，kongfu 病毒的感染率最高。而本期报告中，kongfu 病毒感染率明显下降了。本中心认为，在病毒公布之后，杀毒厂商一般都会尽快更新病毒引擎，致使之前活跃的 kongfu 病毒逐渐被控制。然而，从病毒出现到有效查杀工具使用之间的时间，已有部分恶意应用被下载并传播。此外，本报告数据显示，新的手机病毒已出现并开始广泛传播。

2.2.5 近半数已知 Android 恶意应用仍然在架

本中心在《2012 年第三季度中国移动互联网应用安全分析报告》

中从样本库中随机抽取约 30 万个应用进行统计，共计检测出恶意应用程序 3017 个(含 Google Play 中 12 款)，截止第三季度撰稿日期，3017 款恶意应用程序中仍有 1964 款(含 Google Play 中 4 款)。

截至本期报告撰写日期，本中心对这 1964 个恶意应用程序进行复查，调查结果显示，1964 个恶意应用程序中仍有 1245 款(含 Google Play 中 4 款)在应用商店可公开下载。具体对比数据如下图所示。

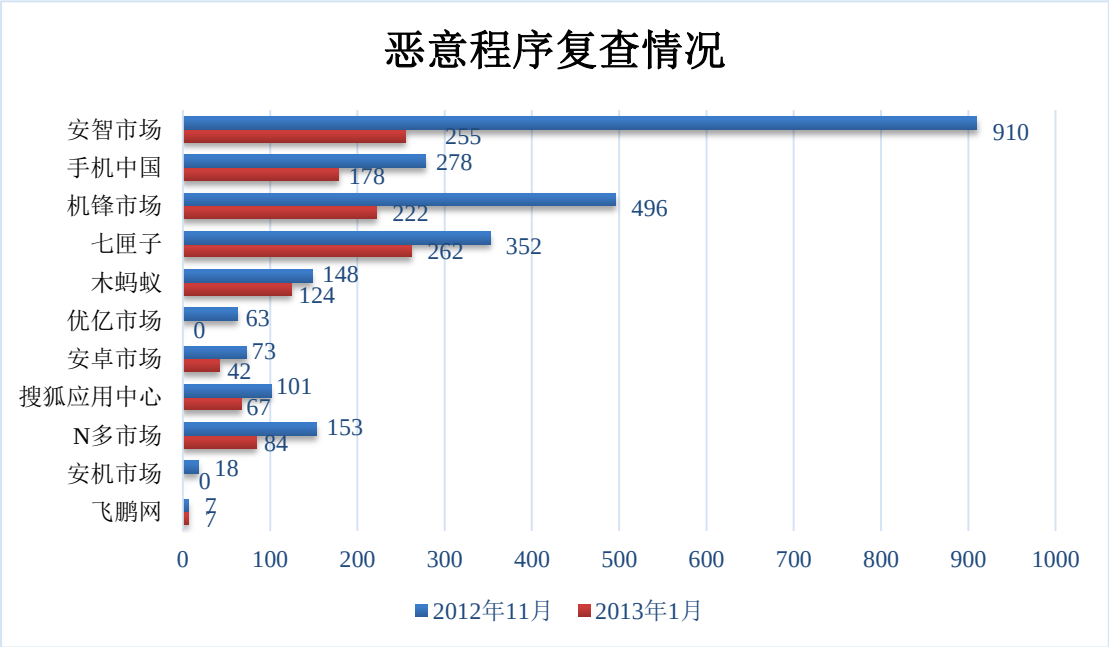


图 2-18 恶意程序复查情况

从图 2-18 中可以看出，1 月份发现的恶意应用软件至今仍然有将近 50%的应用仍然在架，有些应用商店的恶意应用甚至仍然全部在架，由此可以看出这些应用商店的审核制度仍然存在明显缺陷。在众多第三方应用商店内，应用审核制度都存在或大或小的漏洞，这些漏洞给恶意应用软件提供了传播的温床。已知 Android 恶意应用下载量已增加到 2728 万。

2.2.6 Google Play 中已发现的 4 款恶意应用仍然在架

截止本报告撰稿日期，本中心从 Android 官方应用商店 Google play 中发现 4 款恶意应用，这 4 款应用也是上期报告中提到的 4 款恶意应用。这 4 款恶意应用在 2012 年后半年一直在架供用户下载，目前下载量已达 650 万。

Google Play 中的 4 款恶意应用名称及下载量如下表所示。

表 2-1 Google Play 应用商店中检测出的 4 款恶意应用列表

应用名	下载量（万）	应用类型	感染病毒
EAGLE NEST - Sniper training	500	游戏类	android/airpush.b
Basketball Tour GOLD	50	游戏类	android.hack.ginmaster.a.v.(kcloud)
iStreet Basketball PRO	50	游戏类	android.troj.kungfu.b.(kcloud)
Ball Tennis Gold	50	游戏类	android.troj.ginmaster.e.(kcloud)

2.2.7 近半数 Android 应用具有可疑行为

本报告从应用样本中随机抽取 147362 个应用程序，对其进行可疑行为检测分析。结果显示，**接近 50%的应用程序存在可疑行为**。这些可疑行为均为在用户不知情的情况下触发，且这些可疑行为可以顺利通过防病毒软件的检测。根据本报告 1.2.2.2 小结对可疑行为的分类，按照单一规则命中进行统计，结果如下图 2-19 所示。

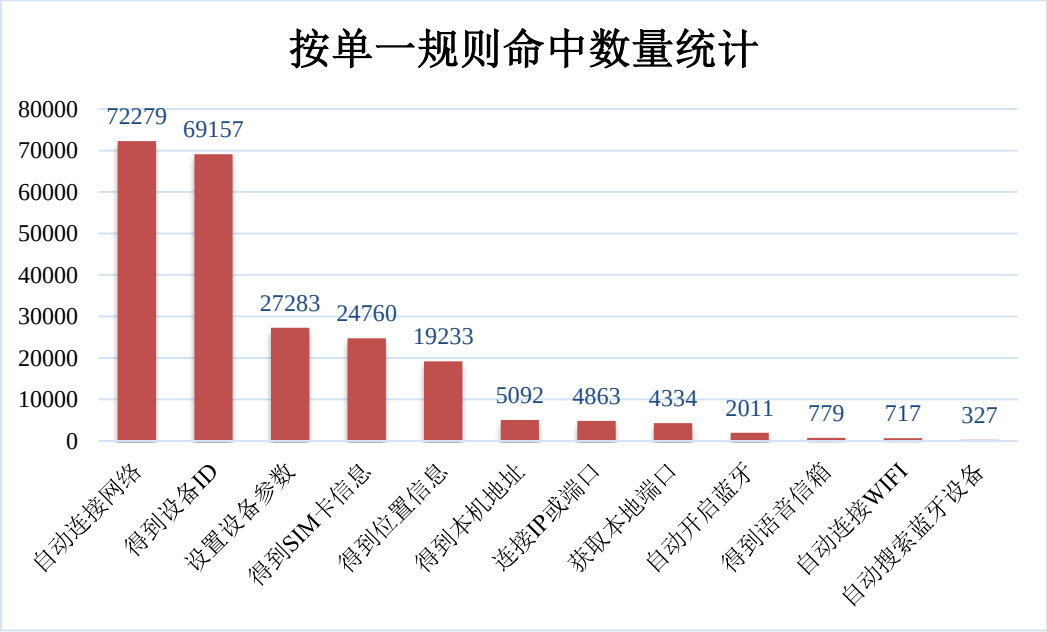


图 2-19 按单一规则命中数量统计图

由上图可知，未通知用户便在后台自动连接网络的行为是出现最多的可疑行为。自动连接网络行为和得到设备 ID 行为始终是触发次数最多的两种行为。

本中心对自动连接网络类进行了深入的分析，发现大部分自动连接网络类行为是访问广告网站行为，具体如下图所示。

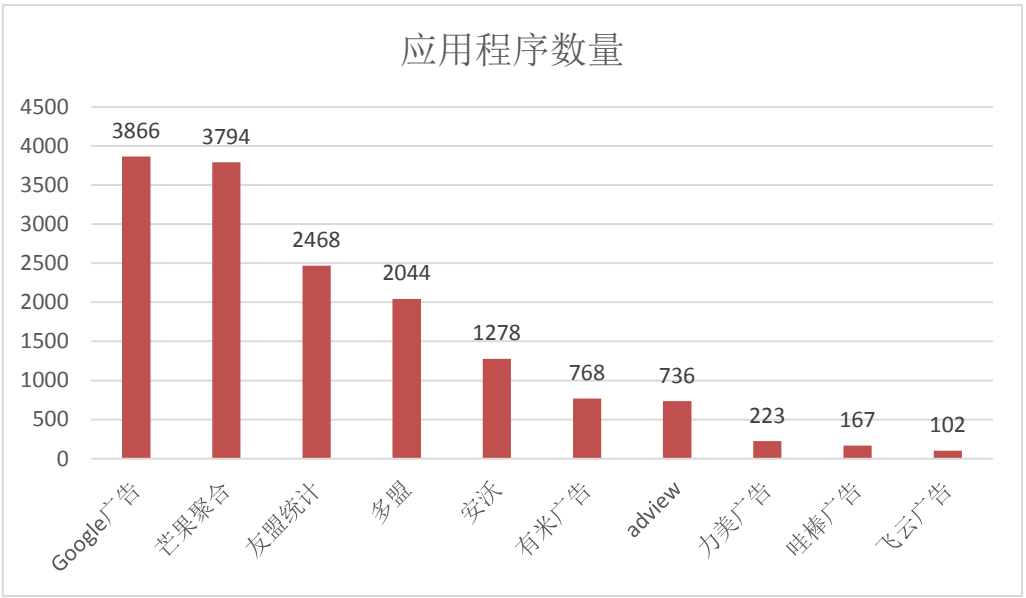


图 2-20 广告网站分布图

3 问题及对策

3.1 安全问题

3.1.1 Android 商店的应用感染病毒比例上升

从本季度的统计报告中可以看到，样本中恶意应用的比例从 9.0‰ 增加至 9.5‰，第四季度恶意应用复查情况也比第三季度恶意应用复查情况进一步恶化。第三季度，本中心一共发现 3017 款恶意应用，截止第三季度撰稿日期，仍有 1964 款应用在架可下载，占比 65.09%；本季度，本中心一共发现了 860 款恶意应用，截止撰稿日期，其中仍有 609 款应用在架可下载，占比增长到 70.81%。第三季度，本中心对第二季度发现的 1496 个恶意应用程序进行复查，发现其中仍有 717 款在架可下载，占比 47.92%；而本季度，本中心对第三季度的 1964 款恶意应用程序进行复查，发现仍有 1245 款在架可下载，占比增长到 63.39%。

从上述这些数据可以说明，目前国内外移动互联网的安全形势不容乐观，移动互联网行业安全态势正在不断恶化。需要注意的是，受欢迎的应用并不代表它是安全的。在 Google Play 商店前 500 名受欢迎的应用中，“高风险”应用被下载的次数超过了 1.75 亿次[5]。而在非官方应用商店中，恶意应用被下载的情况更为严重。

3.1.2 移动互联网恶意威胁更广泛

此外，谷歌官方应用商店 Google Play 在第三季度发现的恶意应用，第四季度仍然没有下架，且下载量持续增长。第三季度在 Google

[5] http://www.36kr.com/p/163742.html

Play 中发现的恶意应用主要是恶意广告类木马，目前恶意广告类木马技术有了进一步的发展，更高也更隐蔽，恶意广告类木马将进一步泛滥。

Google Play 官方应用商店中发现的 4 款恶意应用程序，感染了 Apperhand 恶意广告类木马，目前下载量已经达到 650 万；腾讯公司在 2012 年 10 月发布的一份安全数据报告中提到，腾讯手机管家拦截到 a.expense.fakeKernel 恶意广告类木马，此木马在 10 月份已感染了 2 万用户，107 款软件被感染，攻击约 1.9 万个 Android 应用程序包。按照一个用户被推广 2-4 个软件来算，每个软件的推广费从 1-1.5 元不等，病毒制造者最高可获利 14 万左右。高盈利、低成本、快速批量感染使得恶意广告类木马进一步泛滥。

3.2 对策建议

3.2.1 强烈建议非官方应用商店加强监管

国内大部分非官方应用商店的审核机制尚不完善，给恶意应用开发者大开方便之门。因此，本中心强烈建议应用商店，特别是非官方应用商店（包括手机同步工具类的应用商店）加强自身对应用提交及更新的安全审核能力，可以采用如下几种方式：

1）依托权威的第三方测评机构对应用商店进行安全性测评；

2）从技术层面上对应用进行安全加固并完善安全防护措施，对已经确保安全的应用程序通过特定技术手段进行特定认证，防止恶意应用对应用程序进行恶意篡改；

3）建立评价开发者实名制制度和恶意应用开发者黑名单制度，

确保从开发者这个源头上保障应用安全。

3.2.2 建议用户养成安全使用智能终端的习惯

如今，手机等智能终端上存储了众多用户的个人隐私信息或重要数据，养成安全使用智能终端的习惯可以明显降低手机、平板电脑等个人设备感染病毒、木马等恶意软件的概率。为此，本报告建议用户养成如下以下几点安全使用习惯：

1、下载官方发布或认证的应用。最近，许多应用商店在应用的下载页面上都增加了“标签”，例如官方版、无病毒、无广告等，如下图所示。

图 3-1 应用认证标签举例

建议用户首选具有标签的应用商店下载应用，并在下载应用前看清应用的标签内容，尽量选择下载官方认证的、无病毒广告、无窃取隐私的应用。

2、安装软件时留意提示信息。手动安装软件时，系统会显示该软件安装后将使用的权限，如下图所示。

图 3-2 安装应用时权限提示举例

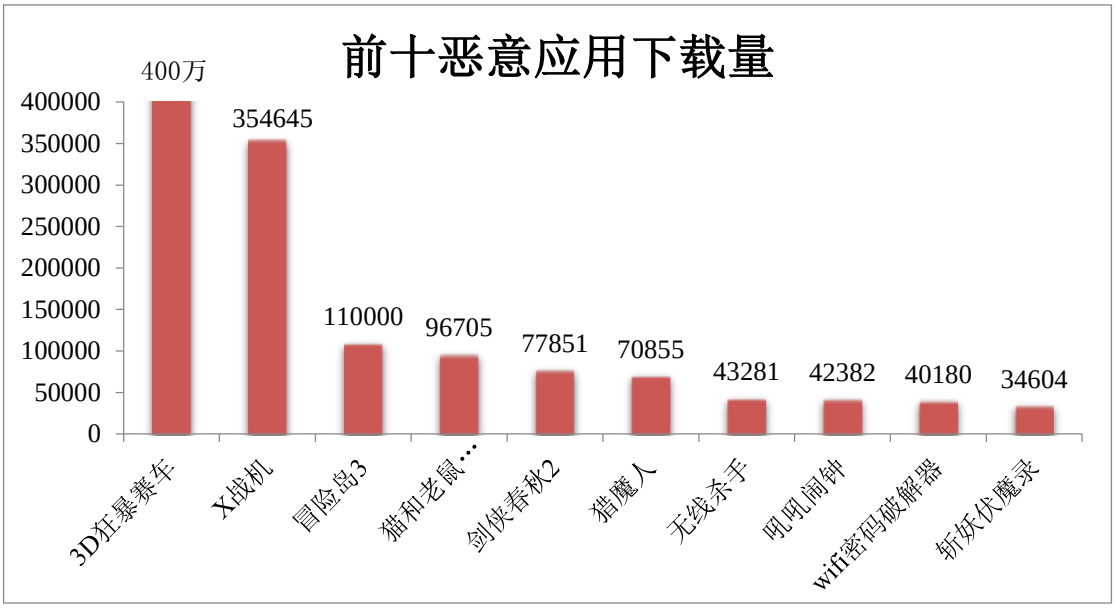
建议用户在安装时一定留意系统提示的权限内容，如发现软件使用了与其功能不符合的权限，则该软件可能具有恶意行为，建议放弃安装该软件，选择其他软件代替。例如，安装某游戏时系统提示该游戏将使用访问通讯录权限，或安装某新闻阅读器时系统提示该软件将使用访问短信权限，遇到此类情况建议用户放弃安装。

3、安装防病毒软件并及时更新病毒库。防病毒软件是检测并清除已知手机病毒的必备工具。此外，一些防病毒软件还提供了系统敏感数据的监控功能，可以及时地对系统中的危险操作进行提醒。需要注意的是，要养成及时更新病毒库的习惯，确保防病毒软件的最佳查杀能力。

4、不要轻易 ROOT 自己的设备。设备 ROOT 后将获取系统最高的控制权限。换句话说，ROOT 设备中的所有数据都可以随意读写，容易扩大病毒等恶意软件的破坏范围和力度。

附件 1.　2012 年第四季度十大恶意应用

截至本报告撰写日期，本中心已发现 1960 款恶意应用，其中下载量最大的十款恶意应用的总下载量已高达 1000 万款。其下载量分布如下图所示。



附图 1 前十恶意应用下载量示意图

注：“3D 狂暴赛车”下载量为 400 万。

由上图可知，本期主要的恶意应用类型集中在游戏类和常用工具类。以下是 2012 年第四季度十大恶意应用的详细信息：

序号	名称	版本	下载量	所在商店	病毒种类
1	3D 狂暴赛车	1.2.1	400 万次	应用宝	android.troj.mdk.e.(kcloud)
2	X 战机	1.2.7	354645	360 手机助手	android/plankton.ag
3	冒险岛 3	2.3	110000	应用宝	android/gappusin.s
4	猫和老鼠 (Run Jerry	1.0	96705	搜狐应用中心	android.troj.plankton.a.(kcloud)

	Run)				
5	剑侠春秋 2	1.0	77851	智汇云应用商店	troj.adsos.a.(kcloud)
6	猎魔人	1.0	70855	智汇云应用商店	troj.adsos.a.(kcloud)
7	无线杀手	1.7	43281	百度移动应用	android/wifikill.b
8	吼吼闹钟	1.3	42382	智汇云应用商店	android.troj.undef.(kcloud)
9	wifi 密码破解器	2.12	40180	N 多网	android.hacktool.penetho.a.v.(kcloud)
10	斩妖伏魔录	1.0	34604	智汇云应用商店	troj.adsos.a.(kcloud)

关于我们：NINIS 软件安全评估中心

国家计算机网络信息安全技术研究所（National Institute of Network and Information Security，简称“NINIS”）围绕国家和社会重大网络信息安全需求开展技术攻关和关键平台研究。

为满足国家移动互联网安全需求，实现对移动互联网应用安全的检测、评估与分析，NINIS 专门成立软件安全评估中心开展移动互联网应用软件安全检测与评估业务工作。目前对外提供的服务如下：

- **移动应用恶意行为检测分析服务**：检测分析移动应用具有的恶意扣费、远程控制、隐私窃取、恶意传播、资费消耗等行为。
- **移动应用可疑行为检测分析服务**：检测分析移动应用具有的异常输入处理、不安全 API 调用、权限管理漏洞、程序漏洞、安全功能误用等行为。
- **移动应用商店安全评估服务**：根据应用商店的应用安全情况评估应用商店的安全状况。

联系方式

地址： 北京市朝阳区裕民路甲 3 号　　邮编： 100029

电话： 010-82991530　　邮箱： ninis@cert.org.cn

合作伙伴

北京软安科技有限公司

12321 举报中心

联想乐商店

国家计算机网络应急技术处理协调中心

国家网络信息安全技术研究所软件安全评估中心

地址：北京市朝阳区裕民路甲3号　　邮编：100029

电话：010-82991530　　传真：010-82990073

邮箱：ninis@cert.org.cn

扫描二维码可直接下载电子版报告