

移动互联网应用安全分析报告

国家网络信息安全技术研究所

二〇一二年八月

目录

1	前言.....	1
2	移动互联网应用现状.....	3
2.1	移动互联网终端高速增长.....	3
2.2	移动互联网应用程序数量巨大.....	4
2.3	移动互联网应用商店处于无序状态.....	5
2.3.1	应用商店数量多.....	5
2.3.2	应用商店混乱.....	6
2.3.3	非官方商店应用程序数量众多下载量大.....	8
2.3.4	应用软件类型复杂.....	10
3	移动互联网应用安全威胁.....	13
3.1	威胁类型.....	13
3.1.1	恶意行为.....	13
3.1.2	敏感行为.....	15
3.2	分析方法.....	18
3.3	威胁情况.....	19
3.3.1	恶意行为检测结果.....	19
3.3.2	敏感行为检测结果.....	22
3.4	典型案例分析.....	24
3.4.1	一键 VPN.....	24
3.4.2	通话王.....	25
3.4.3	国考大师.....	25
3.4.4	Ok 健康.....	27
4	移动互联网应用安全影响分析.....	28
4.1	内嵌广告造成用户经济损失巨大.....	28
4.2	移动终端普遍感染恶意应用.....	29
4.3	移动互联网应用产业链不健康.....	30
5	结论.....	33
6	附：NINIS 软件安全评估中心.....	35

1 前言

近年来我国移动互联网产业发展迅速，网络用户规模不断扩大。来自 2012 年中国移动互联网产业应用大会数据显示，中国手机网民 2012 年第一季度超过 3.7 亿人，预计年底将达 4.51 亿。同时，移动智能终端市场也发展迅速，来自工业和信息化部报告显示，2012 年第二个季度中国市场移动智能终端销售量已达 4200 万台，成为全球最大移动智能终端市场。

伴随着用户规模和终端市场的发展，移动互联网应用软件产业也在飞速发展。苹果 APPStore 的引领、Android 开放平台的推波助澜，各种官方应用商店和非官方应用商店如雨后春笋般生长出来，每个应用商店都汇聚了巨大的应用软件开发人群，每天都有数千款新的移动应用软件上架，为用户提供各种可下载的支撑工作、生活和娱乐的工具。据统计，目前应用商店的应用软件规模已达上百万款，形成了一种全新产业模式的生态环境，并影响和改变其他相关产业的发展。

然而，随着移动互联网应用加速普及，相关安全威胁也开始逐渐显现。

对用户而言，由于不能有效识别移动应用软件的可信性和功效性，一些恶意软件会乔装成某一类正常应用软件，放置在应用商店，用户下载安装后，会在用户不知情的情形下，从事着恶意扣费、系统破坏、隐私窃取、访问不良信息等恶意行为，给用户带来经济损失和信息安全问题。还有一些软件，本身不实施恶意行为，但在为用户服务过程中会从事一些敏感危险行为，如：获取隐私信息、擅自连接网络或发送短信，这些行为也可能会为用户带来经济损失和风险。

从国家层面而言，通过移动终端多样化的获取敏感信息的方式，再辅助以强大后台的同步分析，很容易获取国家的经济、政治等涉密信息，甚至通过移动智能终端散布谣言、传播危险信息，这就使国家对信息资源生产、传播和监管的能力面临严峻挑战。

鉴于移动互联网应用安全的严峻形势，国家网络信息安全技术研究所专门成立了软件安全评估中心(简称 NINIS 软件安全评估中心)，来开展移动互联网应用软件安全检测与评估业务工作，以实现移动互联网应用安全监测。在国家有关

部门的领导和支持下，现已初步建成面向行业和社会需求的移动互联网应用安全检测和评估的服务能力、技术能力和保障条件。

为总体摸清移动互联网应用及安全状况，从 2011 年下半年开始，NINIS 软件安全评估中心开展了移动互联网应用软件安全检测与分析的工作，取得三个方面的成果：第一，对国内 17 家第三方应用商店的约 50 万款软件进行了采集与分析；第二，对采集到的一部分应用软件进行安全性检测与分析。发现一些应用商店公然存在着大量恶意程序，其下载量已经超过 2000 万次；第三，发现将近 40% 的免费应用软件中存在着在用户不知情情况下耗费流量、窃取隐私等敏感行为。

本报告将详细展开描述这些工作成果，并对这些成果进行分析，最后给出移动互联网应用行业发展建议。

2 移动互联网应用现状

2.1 移动互联网终端高速增长

据工业和信息化部最新报告¹显示，2012 年第二季度，智能手机在所有中国手机出货量中占比 56.9%，在 2012 年的上半年，中国上市手机新品为 2099 款，其中智能手机占 822 款，在这些智能手机中基于 Android 操作系统的移动设备达 801 种（占比超过 97%）。

另据市场研究公司 Canalys 日前发布数据²显示，今年第二季度中国市场智能手机出货量与去年同期相比暴增了 199%，约占全球总出货量的 27%，大大超过美国的 16%。Canalys 的统计数据显示，今年第二季度，中国市场智能手机出货量超 4200 万部，连续第二个季度出现大幅增长。与去年同比增幅为 199%，与上季度环比增幅为 32%。中国已成为全球最大的智能手机市场。

另据腾讯科技转载的尼达姆（Needham & Company）2012 年 7 月 9 日发布的智能手机行业季度研究报告³显示，在操作系统占有率方面，虽然中国最大的移动运营商中国移动还没有开始销售 iPhone 手机，但 iPhone 在中国智能手机市场的份额依然由去年第二季度的 9.9% 增长到今年第二季度的 17.3%。虽然 iPhone 手机的市场份额增幅不小，但 Google 的 Android 还是以 69.5% 的市场份额傲视群雄，诺基亚则以 11.2% 的市场份额位列第三。

该报告还指出，目前苹果公司尚未与拥有超过 6.5 亿用户的中国移动合作，如果能够与中国移动合作，iPhone 在中国的市场份额很有很大的上升空间。

¹ <http://www.199it.com/archives/56155.html>

²

<http://www.canalys.com/newsroom/stellar-growth-sees-china-take-27-global-smart-phone-shipments-powered-domestic-vendors>

³ <http://tech.qq.com/a/20120710/000008.htm>

该报告进一步指出，中国智能手机的销量之所以增长如此迅猛，主要是廉价 Android 智能机的推出让功能机失去了竞争力，华为、中兴等本土品牌的智能手机做出了不小的贡献。

2.2 移动互联网应用程序数量巨大

2012 年 5 月，谷歌宣布 Google Play 的应用下载量已经超过 150 亿次。截止 5 月底，Google Play 的应用总量为 62.7 万。而苹果的 App Store 的应用总量已达到 65.2 万，较 4 月份增长 3.5%，下载量超过 250 亿次。微软的 WP 商城继续保持高速增长态势，应用总量达到 9.8 万款，环比增长高达 10.6%。

下图显示，iOS 和 Android 系统的官方商店应用总数都超过 60 万款，处于领先地位；而 WP 商城的应用总数远远低于上述二者，但其增长速度很快；Nokia 公司的 OVI 商店推出 3 年后应用数量也突破了 10 万大关。

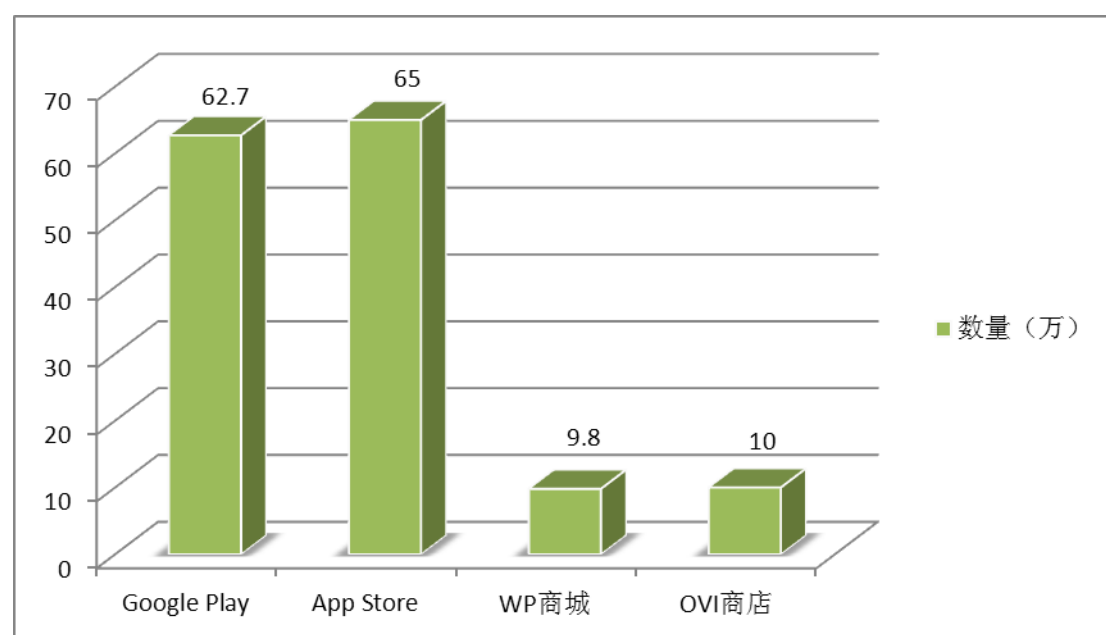


图 2-1 操作系统官方商店应用数量对比

上图主要展示操作系统官方商店的应用软件数量，其实还有大量非官方应用商店也在为用户提供应用软件下载，其应用总数估计已超过官方商店的应用软件数量。

鉴于官方商店的封闭性，本报告主要以非官方应用商店及应用软件为统计分

析对象。

2.3 移动互联网应用商店处于无序状态

在我国除了操作系统官方应用商店之外，还出现大量非官方应用商店，如终端制造商应用商店、电信运营商应用商店、第三方应用商店等等，商店众多，竞争激烈，同质化严重，基本处于无序状态。

2.3.1 应用商店数量多

在移动互联网行业中，与传统 PC 有较大区别的一点就是应用商店。从苹果发布 App Store 开始，到后来谷歌和微软推出的 Google Play 与 Marketplace，移动互联网中的应用程序基本上是通过应用商店下载的。由于 iOS、Android 官方市场，尤其是 Google 市场在国内下载不便等原因，加上“以应用商店抢占国内移动互联网入口”的理念，国内同时出现了很多非官方商店（即第三方商店）。加上 Android 的开放性，Android 平台下的第三方商店数量尤为突出。系统提供商、终端制造商、电信运营商、互联网企业以及其他纯第三方商店纷纷加入用户下载入口的争夺战，应用商店整体格局表现为以上五类商店的混战。

对于国内的应用商店，按照操作系统划分，可以看到：Android 操作系统平台至少有 18 个具有一定规模的应用商店，iOS 操作系统平台有 9 个应用商店，Windows Phone 系统有 5 个，而塞班有 OVI 商店与中移动 MM 商店。这些数据也从侧面反映了各操作系统在中国大陆的占有率和增长态势，如图 2-2 所示：

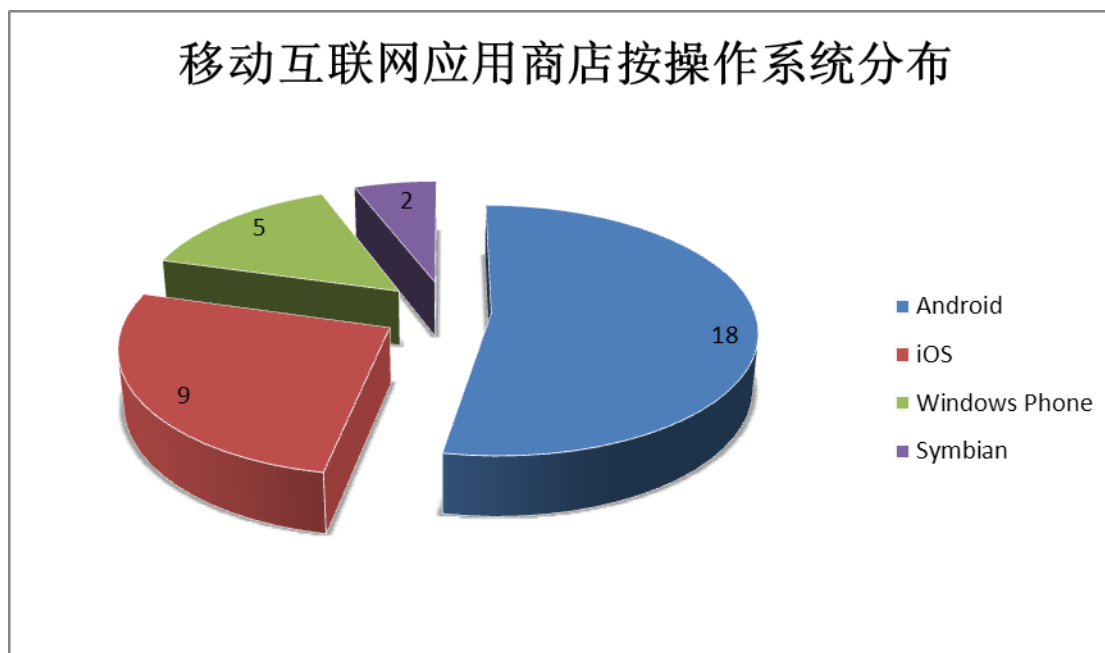


图 2-2 移动互联网应用商店按操作系统分布

从图 2-2 可以看出，在如今的几大手机操作系统中，Android 的应用商店数量最多，这和其庞大的用户量和系统开放性有关。其次数量多的是 iOS 系统的应用商店，这也和智能手机终端操作系统的占比相吻合。

2.3.2 应用商店混乱

据统计，除 Android Google Play、Apple AppStore、Windows Marketplace、Symbian OVI 官方商店外，国内主要的应用程序来源有以下几个途径：

- (1) 第三方应用市场：如机锋市场、安卓市场等；
- (2) 电信运营商商店：如移动 MM 商店、联通沃商店、电信天翼商店；
- (3) 互联网企业商店：如百度应用、搜狐手机应用等；
- (4) 终端制造商：如 HTC、三星、联想、华为、中兴等；
- (5) 移动应用管理厂商：豌豆荚、91 助手等；
- (6) 系统提供商：如华为、中兴、小米等。

此外，除了以上途径之外，还有部分应用程序来自于安全厂商、手机应用开发商、个体开发者等。应用软件传播途径除了应用商店和第三方市场外，还有论坛或者好友群传播等方式。

由此可以看出，不同层次的厂商和开发者都可从事同样的活动，甚至有些厂商同时扮演着多种角色，造成了整个行业的混杂。

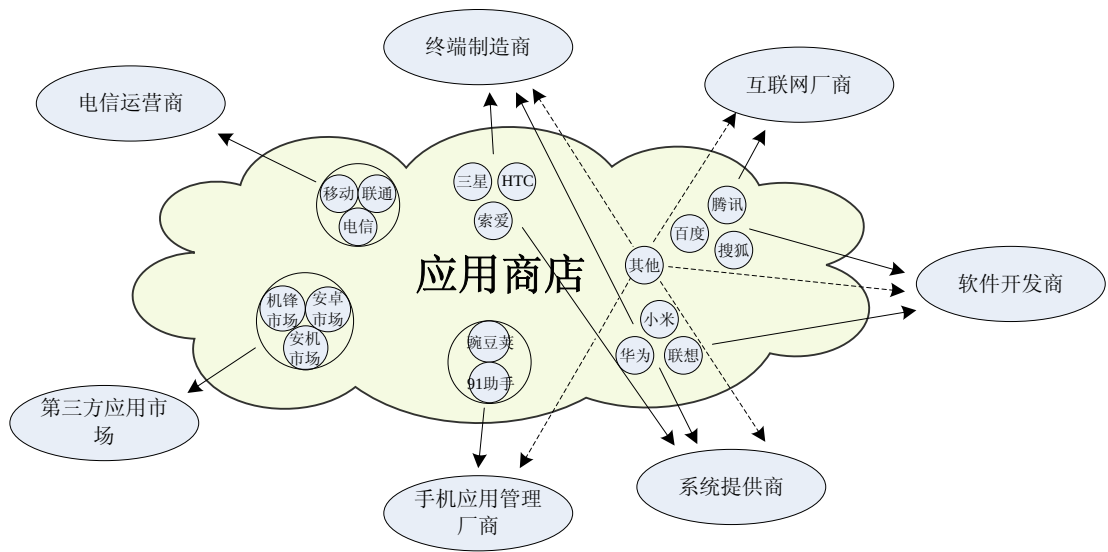


图 2-3 移动互联网应用行业混杂

通过图 2-3 可以看出，有些厂商同时既是软件开发商又是互联网厂商，软件开发商将自己的软件提供给终端制造商、第三方应用市场、系统供应商等，系统供应商又会将运营商应用、第三方市场的应用加入到自己的系统中……而最重要的是，这些厂商都可能成为一个用户应用程序的来源。

如图 2-4 所示，按应用商店类型分布，可以看到，61%的软件商店是纯第三方应用商店，在这些所有商店中占据了一半以上的份额；排名第二是终端制造商，htc、三星、联想等都属于这一类，约占 12%；互联网企业、电信运营商、以及系统提供商的官方商店，各占 9%；纯第三方商店占据了软件商店的大多数，中国境内的移动互联网应用下载被大量第三方商店分流。

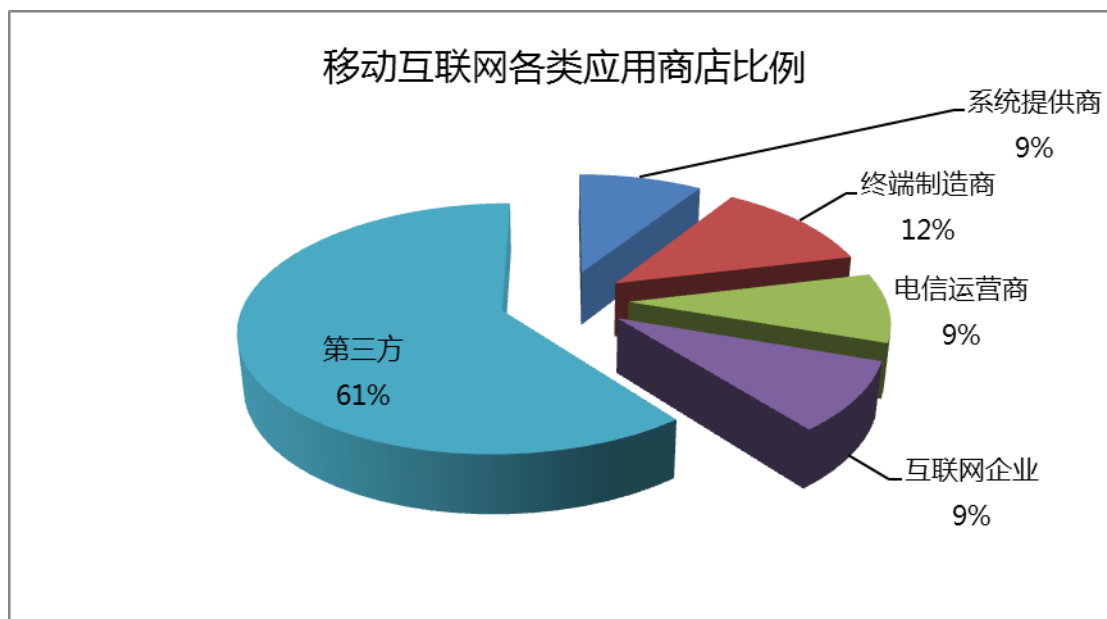


图 2-4 应用商店比例图

此外，除了行业混乱之外，应用商店及第三方应用市场对于应用程序的准入制度没有严格的标准、法规，以确保开发者提交的应用是值得推广的应用。开发者可能为了达到自己的利益，通过某些手段绕过应用商店及第三方应用市场对应用程序的测评，最终让自己的垃圾软件被传播到了网上，直接应用了整个移动互联网的大环境。

2.3.3 非官方商店应用程序数量众多下载量大

从艾瑞咨询的报告⁴可以看出，Android 官方应用商店相对来说用户粘性较差，导致用户易被非官方应用商店大量分流。

⁴ <http://www.iresearch.com.cn/Report/1688.html>

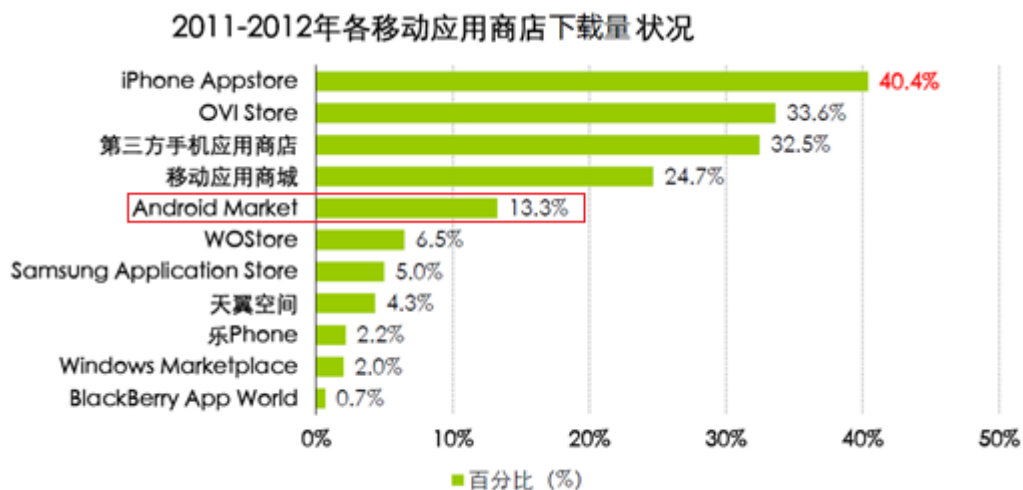


图 2-5 移动应用商店下载量

图 2-5 显示，在 Android Market 中以 13.3% 的比例远低于 AppStore 中应用的数量，由此可以看出，应用商店及第三方市场对 Android 的分流作用非常明显。

截止 2012 年 7 月，本中心从 17 个 Android 应用商店中选择了有下载量数据的 33 万余应用程序进行统计，下载量超过 1000 万的应用程序仅有 80 个(去重)，绝大部分应用程序的下载量少于 1 万次，如图 2-6 所示。

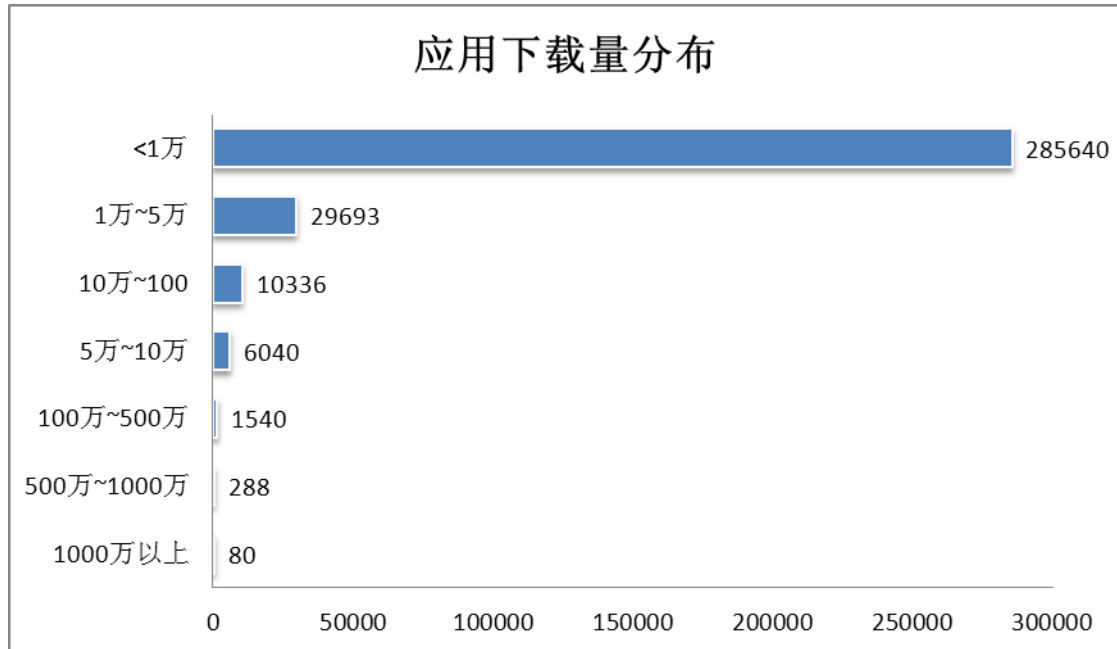


图 2-6 样本应用下载量分布图

第三方应用商店的数量在所有应用商店中接近 2/3。其中，最大的第三方商店应用数量接近 10 万个。本中心收集了 Android 系统的部分第三方近 50 万应用

程序。在这些应用商店中，按照应用软件数量排名，前 10 名的商店如下：

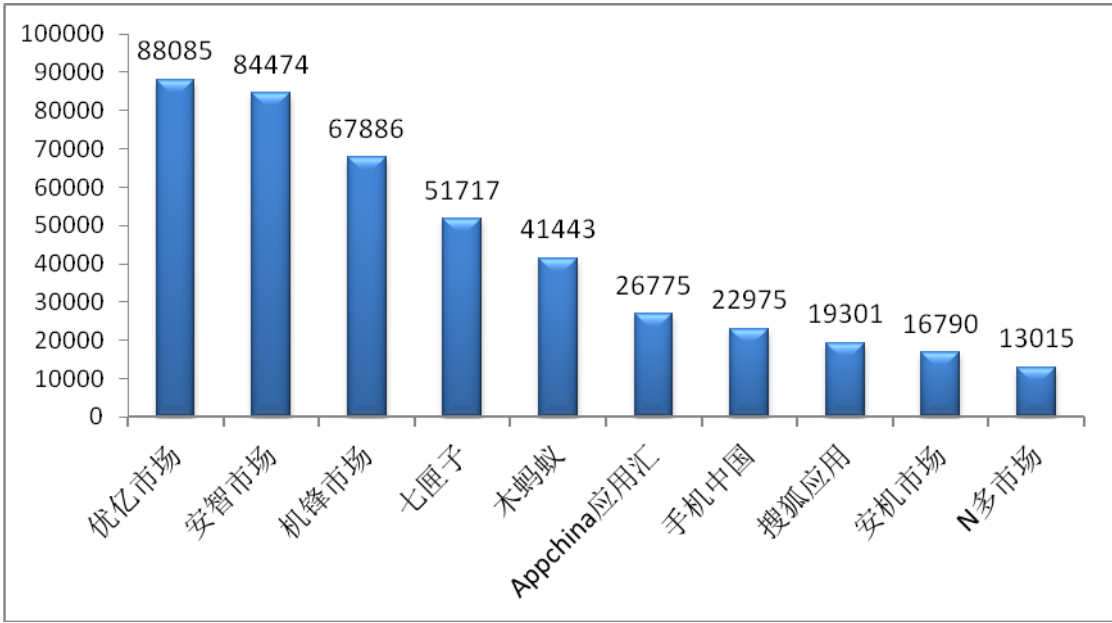


图 2-7 样本应用市场分布图

从图 2-7 可知，国内第三方商店数量众多，且商店内应用数量都巨大。截至 2012 年 7 月，本中心所采集的非官方应用数量已超过 48 万个，若加上未采集的应用数，其总量预计可以超过官方商店的应用数量。

2.3.4 应用软件类型复杂

移动互联网应用程序类型众多，如系统工具类、娱乐类、生活工具类、使用工具类、学习类、游戏类、资讯类、通信类等。iOS 官方应用商店和 Android 第三方商店中，游戏类应用程序仍然是占据着极大的比例，其次是生活类软件。学习类软件、系统工具类软件和娱乐类软件排在后三位，但在两种系统中的占比和排位各不相同。其中，系统工具类主要包括系统设置、安全软件、浏览器输入法和主题桌面类等软件。实用工具类主要包括天气类、交通地图类和摄影类等软件。生活类包括理财、健康、办公和通信类等软件。学习类软件主要包括教育类等软件。娱乐类包括阅读、社交网络、购物、音乐视频和休闲类等软件。

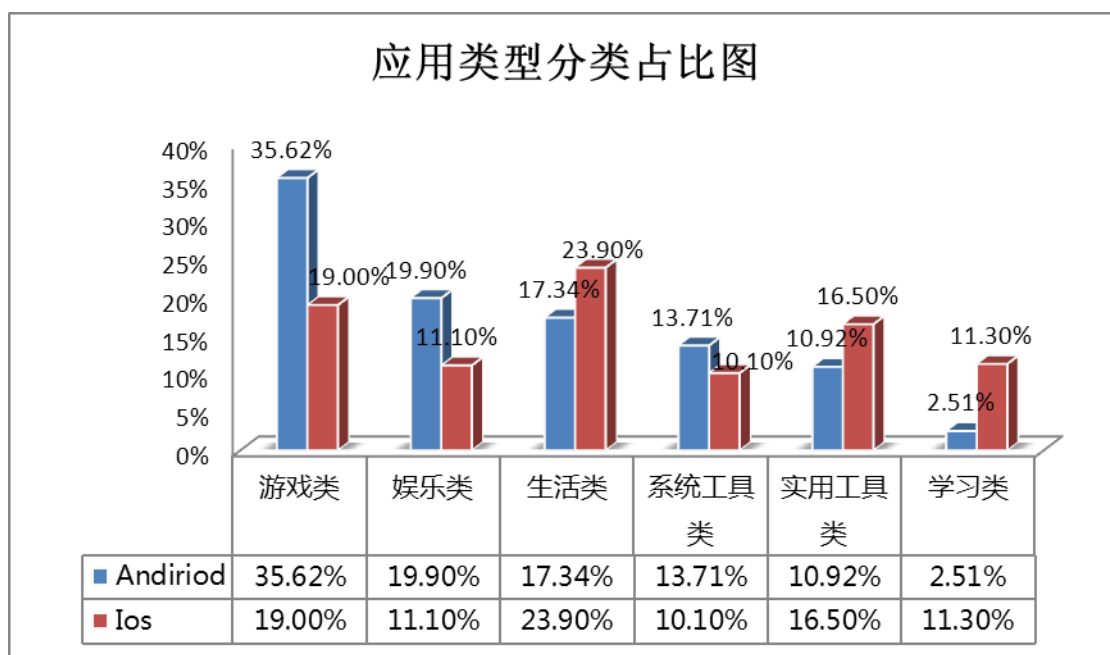


图 2-8 应用类型占比图

从图 2-8 可以看出，Android 和 iOS 两种操作系统中的应用类别是有一些区别的：系统工具类、学习类和游戏类应用占比是 Android 系统高于 iOS 系统，而实用工具类和娱乐类的软件，则是在苹果商店中占比高于 Android 系统。

从用户下载软件数量上看，移动互联网用户下载最多的是游戏类软件，占比达到 31.57%。除了游戏类软件之外，国内移动互联网的用户仍然以娱乐类软件下载为主，占比达到 25.53%。系统工具类软件下载排行第三，下载量占比为 18.78%，生活类、实用工具类和学习类软件下载量占比分别为 12.30%、7.57%和 4.25%，如图 2-9 所示。

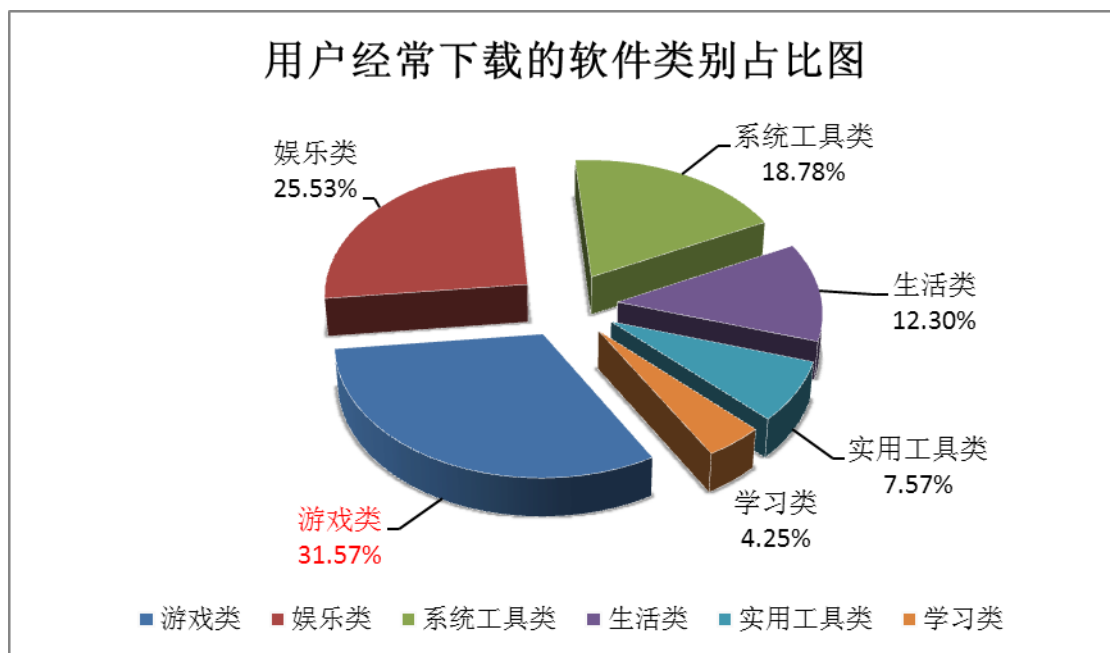


图 2-9 用户下载软件类别占比图

3 移动互联网应用安全威胁

3.1 威胁类型

按照应用程序的威胁程度，将应用程序行为归纳出两大类行为：恶意行为和敏感行为。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；敏感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。

部分含有敏感行为的应用程序可能会对用户的利益造成间接的影响，称其为灰色应用程序。

3.1.1 恶意行为

按照目前业界通用的方式，可以对恶意应用行为进行命名和分类，典型的恶意应用行为按照行为类型和威胁级别对其分类如下：

表 3-1 移动智能终端应用程序典型恶意行为

恶意行为分类	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”
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 exploit 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。

3.1.2 敏感行为

除以上恶意行为外，移动智能终端软件还存在一部分行为，不属于恶意行为范畴，但是使用不当也会对用户的利益造成侵犯，此行为即敏感行为。本中心总结并归纳出可将移动智能终端数十种敏感行为，并按照对用户的隐私和经济利益造成侵害的程度对其进行分级，典型敏感行为如下表所示：

表 3-2 移动智能终端应用程序典型敏感行为

可能造成 的危害	敏感行为	行为威 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 号码来作为唯一的识别码，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 费消耗	自动发送短/彩 信	高	在用户不知情的情况下后台发送短信，属于敏感行为中最为危险的一种，因为这种短信或者彩信往往就是向 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、蠕虫是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。

3.2 分析方法

为了解移动互联网应用程序安全状况，并建立相应的检测分析能力，本中心已完成对 17 个应用商店的应用软件及其相关信息的自动化采集工作，其中包含 Google App 官方商店及 16 个第三方应用商店。在这些商店内共采集了第三方应用商店超过 481459 个应用软件。本次主要针对所有第三方商店的应用程序进行检测分析。

本中心依据应用采集、应用检测、深度分析及综合评估四步对移动互联网应用程序进行检测与分析，如图 3-1 所示：

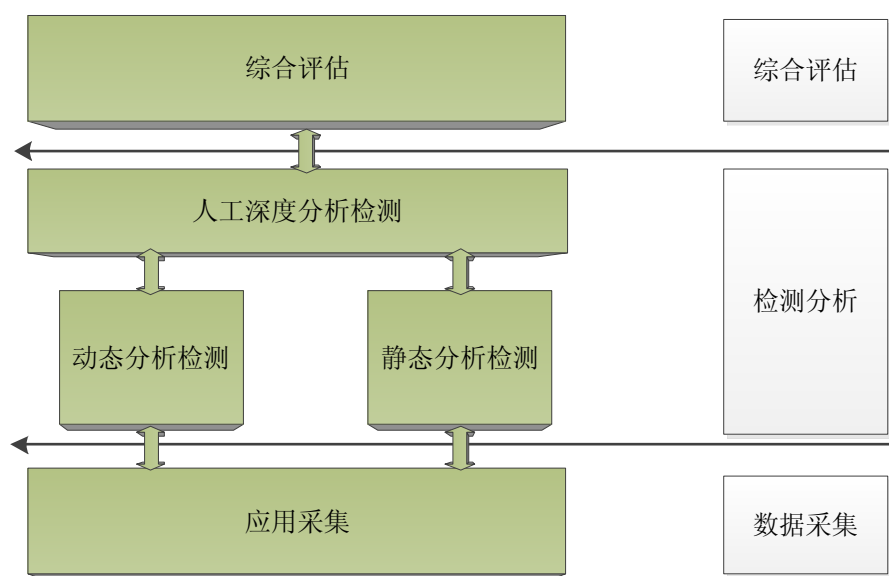


图 3-1 分析方法

应用主动采集是对国内外常见的软件商店内容进行分析、下载。应用采集的覆盖范围包括 Google 的官方市场以及国内部分第三方市场。采集的应用程序及其基本信息保存在应用程序样本库中，供自动分析平台进行分析。

应用检测是对应用程序样本库中的应用程序进行自动化的行为分析，根据由敏感行为制定的规则进行分析，发现存在敏感行为的可疑应用程序。本中心研发了一套针对应用程序行为特征分析的主动式发现工具，根据初始的二十余个敏感行为规则，对应用程序样本进行初步分析与筛选。

深度分析步骤主要由经验丰富的工程师，通过人工安装、运行可疑应用程序，并借助相关工具分析应用程序运行时的网络消息收发、资源占用等特征，最终确认可疑应用程序的危害方式、危害等级并将其归类。

依据移动智能终端信息安全评估指标体系，根据应用筛选和深度分析的结果，建立信息安全评估模型。针对单个应用程序，评估其传播范围（目前主要通过应用程序在各商店的下载量统计），有害应用程序影响的严重程度，以及针对此类有害应用程序的对策建议。对移动移动智能终端应用程序监管方面，评估目前有害应用程序的综合态势，总结当前有害应用程序技术分类，分析当前使用各种有害技术的应用分布，为整体监管提供建设性建议。

3.3 威胁情况

3.3.1 恶意行为检测结果

本中心从样本库中挑选出 206882 个应用进行统计，涵盖主流第三方商店，各商店样本数量具体情况如图 3-2 所示（图中仅展示样本数量前 10 的商店）：

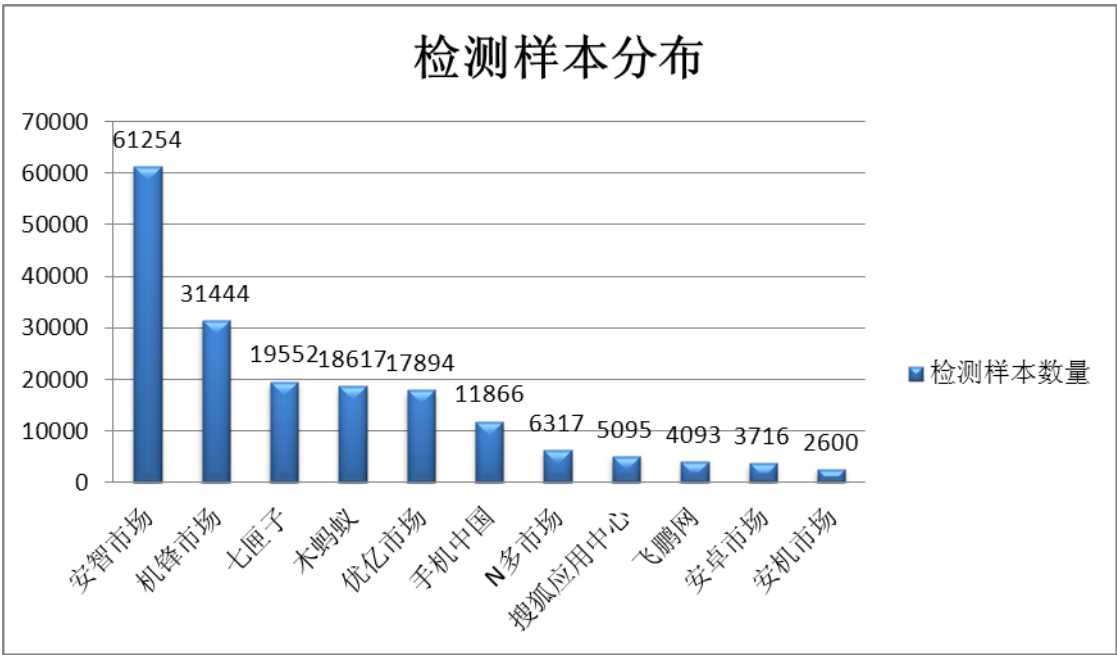


图 3-2 检测样本分布

经过恶意行为检测分析发现，各应用商店中均含有恶意应用程序，具体检测结果如图 3-3 所示：

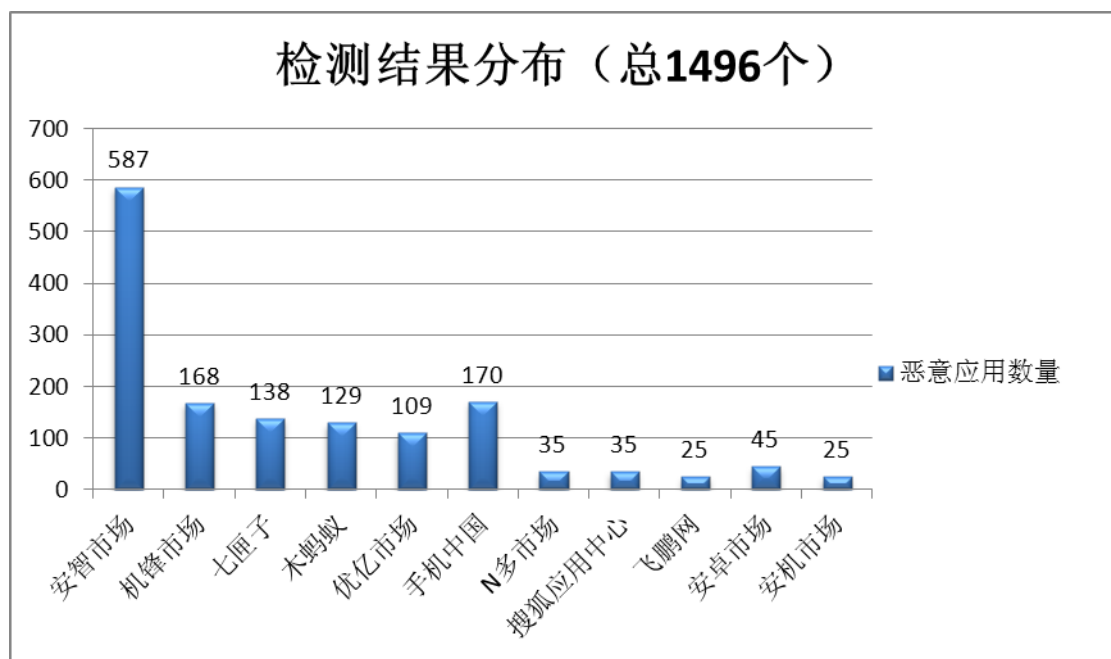


图 3-3 检测结果分布

从检测结果可以看出，移动互联网应用商店中的恶意应用程序的比例已经在千分之五至百分之一之间，经统计，这 1496 个恶意程序的总下载量已经超过了两千万（图 3-4），这已经是一个非常巨大的数字，在这些第三方商店中，恶意应用程序就这样公开放在商店中供用户下载，成为当前移动互联网病毒传播的主要方式之一，移动互联网第三方应用商店中恶意程序的问题应该引起足够的重视。

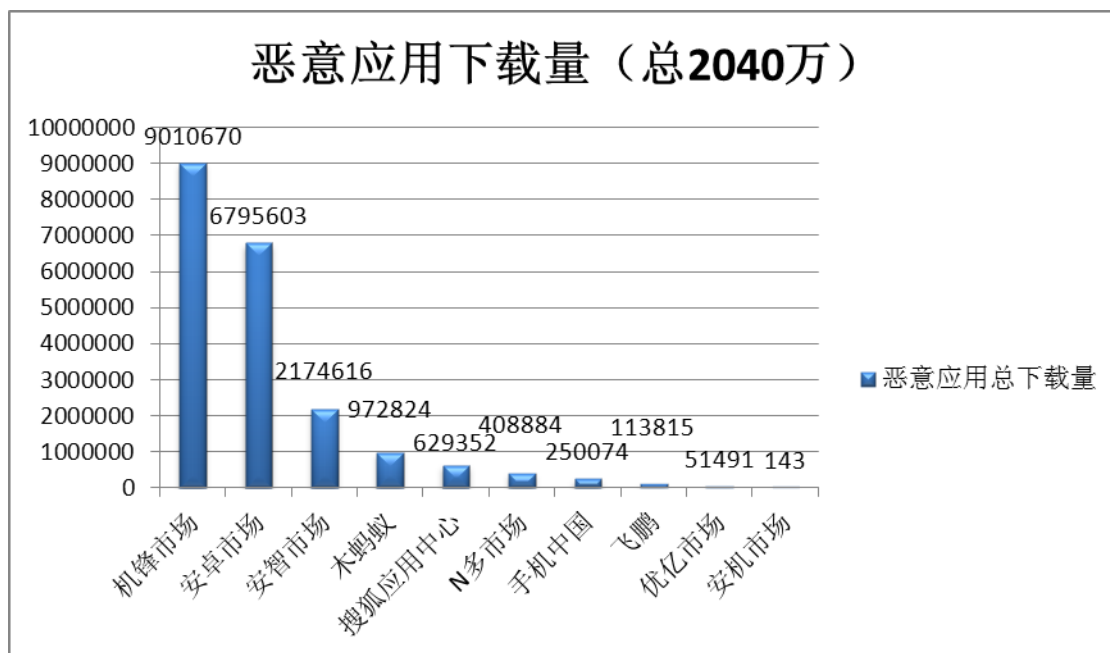


图 3-4 恶意应用程序下载量（七匣子市场由于未公开下载量数据而没有被统计）

本中心本次统计的恶意应用程序的总量为 1496 个，按照现在安全厂商的通用分类标准，可以分为如下几类，其中最多的是 Kungfu 病毒，其次是 Ginmaster 及 Updtkiller 病毒，如图 3-5 所示。

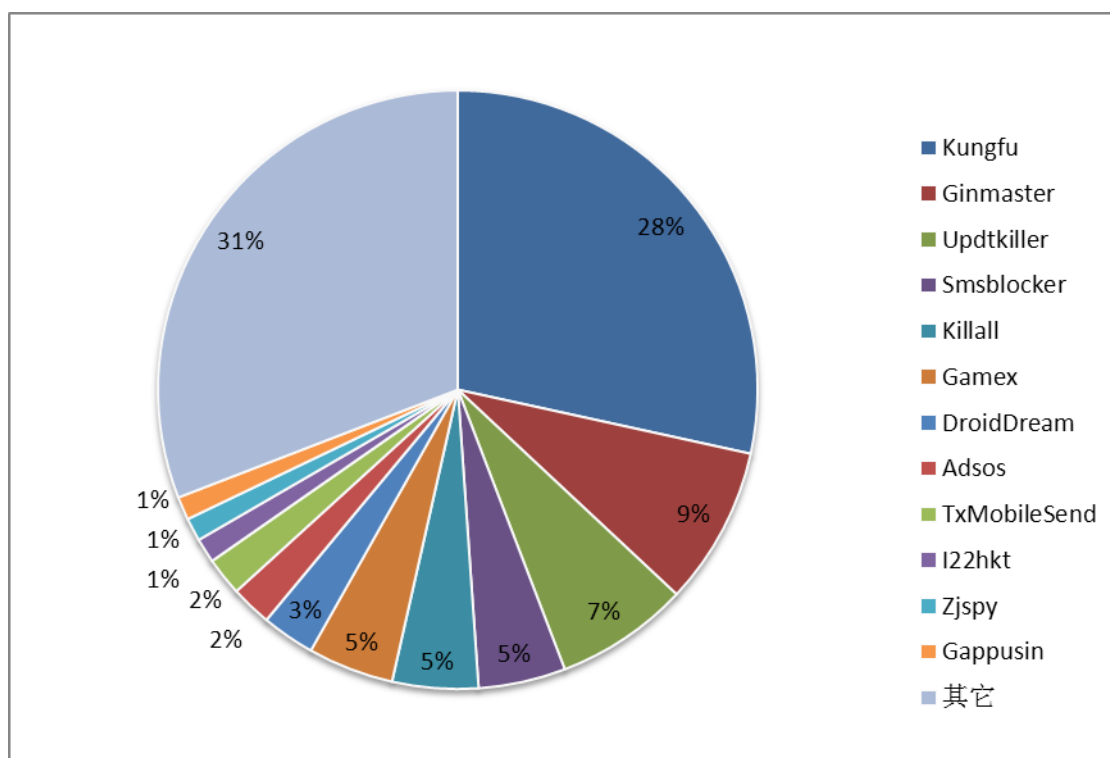


图 3-5 恶意应用程序比例

3.3.2 敏感行为检测结果

本中心从采集的应用程序中，随机抽选 19442 个应用程序，使用行为分析工具对其进行分析，从检测结果来看，超过 50% 的应用程序存在敏感行为（所有的这些敏感行为均为在用户不知情的情况下发生，即没有经过用户允许而触发），而这些敏感行为在防病毒软件的检测中，通常是被忽略的一种。具体的统计如图 3-6 所示：

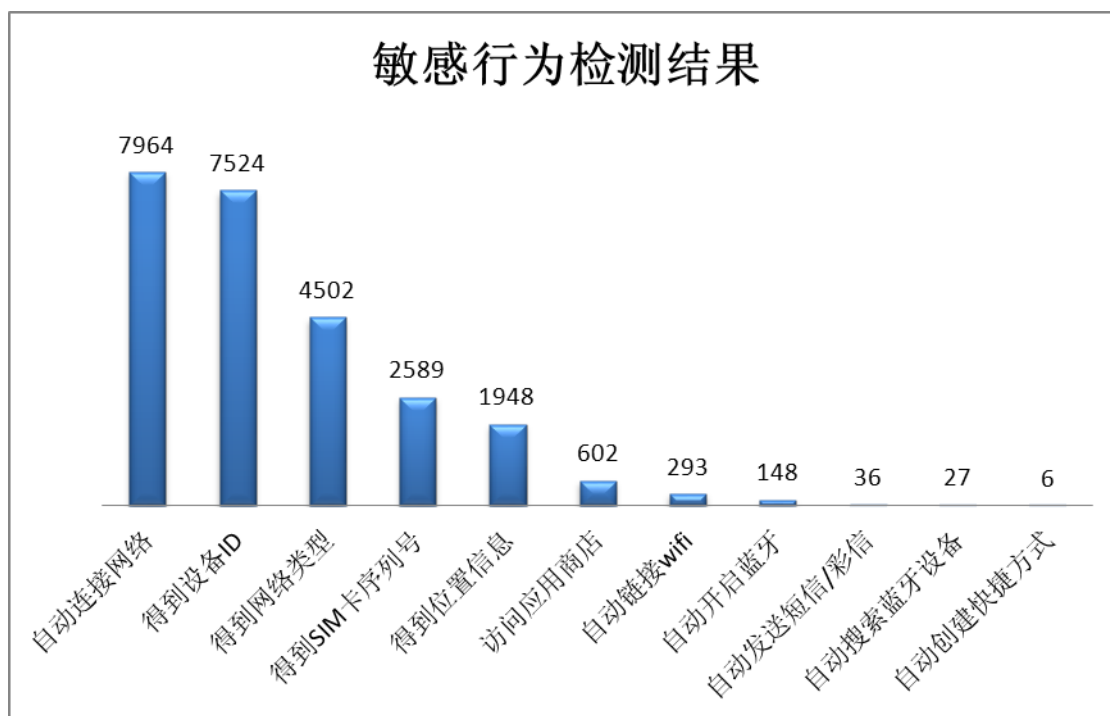


图 3-6 敏感行为检测结果

其中，通过对自动连接网络类进一步的分析，发现大部分软件自动连接到广告网站，并且这种行为没有经过用户允许。这意味着，大量的广告访问意味着会消耗用户大量的流量。软件中插入广告的行为是免费软件的潜规则，现在并没有安全厂商将其划为恶意软件，但是其对用户流量的吞噬也不容小觑。按照威胁类型的分类，这种自动连接网络获取广告的应用程序属于灰色应用程序，这种程序会间接侵害用户利益。

表 3-3 自动连接网络的应用程序中，广告商统计

域名	广告商	应用程序数量（个）
admob.com	Google 广告	1692
umeng.com	友盟统计	1347
adsmogo.com/net/org/mobi	芒果聚合	1269
munion.baidu.com	百度联盟	1217
domob.cn	多盟	1163
adwo.com	安沃	912

youmi.net	有米广告	388
adview.cn	adview	220
wooboo.com	哇棒广告	216
lmmob.com	力美广告	122

3.4 典型案例分析

3.4.1 一键 VPN

所属类别：恶意行为 Kungfu。

在一款名为“一键 VPN”的软件中，存在 kungfu 病毒。感染 Kungfu 病毒的手机会自动在后台利用系统漏洞静默获取 root 权限，释放安装它所指定的应用程序并接收控制命令。其释放安装的软件名称通常为 Google update，以此迷惑用户（如图 3-7 所示）。当手机感染此病毒后使用常规安全软件无法彻底清除，甚至将手机恢复至出厂设置也无法解决问题。



图 3-7 “一键 VPN”软件中释放的恶意应用程序安装截图

在总共五个应用商店中存在这款应用，手机中国、2265 商店和百度应用商店的三款应用都存在问题。

表 3-4 一键 VPN 应用分布及下载量

应用名称	来源市场	下载链接	下载量
一键 VPN	手机中国	http://app.cnmo.com/android/105449/	9000+
	2265 商店	http://www.2265.com/soft_16/42/android_2162.html	400+
	百度应用	http://as.baidu.com/a/item?docid=332315295&f=hao	60+

3.4.2 通话王

所属类别：敏感行为。

自动发送短信不仅消耗了用户的通信费用，而且设备标识和地区标识等信息的泄露可能会导致用户受到垃圾短信和垃圾电话的骚扰。一款名为“通话王”的软件，在用户不知情的情况下，会向 15919479044 这个号码发送设备标识和地区标识，属于用户隐私信息的窃取行为。

表 3-5 通话王应用分布及下载量

应用名称	来源市场	下载链接	下载量
通话王	优亿市场	http://www.eoemarket.com/apps/60161	800+
	安智市场	http://www.anzhi.com/soft_90441.html	2200+

3.4.3 国考大师

所属类别：敏感行为。

一款名为“国考大师”的软件会向 18601796923 发送软件的注册信息，用户的用户名密码等敏感信息的泄露会对用户的个人隐私和信息安全造成严重威胁。由于一些用户出于便于记忆的出发点，存在各个网站注册用户名和密码一致的习

惯，不法分子可能利用得到的用户注册信息尝试破解用户的其他重要账户，甚至是与财产密切有关的网银和第三方支付账户，对用户的信息安全和财产安全都造成了严重的潜在危害。值得注意的是，位于“机锋市场”和“AppChina 应用汇”中，存在同名但不同区域的数个版本，其中 5 款应用程序不发送信息至固定号码，而另外 9 款应用程序存在此敏感行为。

表 3-6 应用分布及下载量

应用名称	来源市场	下载链接	下载量
国考大师	机锋市场	http://apk.gfan.com/Product/App253731.html （重庆卷）	2300+
	机锋市场	http://apk.gfan.com/Product/App253358.html （广西卷）	900+
	机锋市场	http://apk.gfan.com/Product/App253770.html （深圳卷）	2300+
	机锋市场	http://apk.gfan.com/Product/App253348.html （广东卷）	1000+
	AppChina	http://www.appchina.com/app/com.hyt.android.examin_chongqing.view/ （重庆卷）	100+
	AppChina	http://www.appchina.com/app/com.hyt.android.examin_guangdong.view/ （广东卷）	300+
	AppChina	http://www.appchina.com/app/com.hyt.android.examin_guangxi.view/ （广西卷）	200+
	AppChina	http://www.appchina.com/app/com.hyt.android.examin_guangzhou.view/ （广州卷）	300+
	AppChina	http://www.appchina.com/app/com.hyt.android.examin_shenzhen.view/ （深圳）	300+

3.4.4 Ok 健康

所属类别：敏感行为。

名为“OK 健康”的软件会将用户填写的健康数据通过短信方式发送到13683618663。用户健康信息作为用户的个人隐私，应受到严格的保护。泄露的健康信息会被不法分子利用或者非法传播，严重危害用户的个人信息安全。一些与健康相关的不良机构还可能会利用这类信息对用户发送垃圾短信和拨打垃圾语音电话（见图 3-8、图 3-9）。

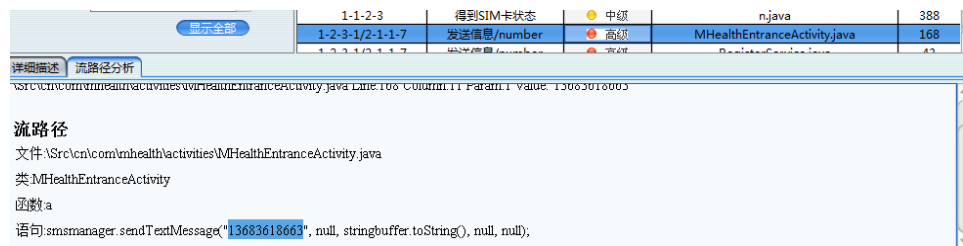


图 3-8 检测工具所检测的发送短信行为

序号	短信内容	发送时间	接收号码	发送号码
20	国内短信	2012-08-11 11:30:59	13683618663	0.10
21	国内短信	2012-08-11 14:58:46	13683618663	0.10

图 3-9 运营商话费详单

表 3-7 OK 健康应用分布及下载量

应用名称	来源市场	下载链接	下载量
OK 健康	安智市场	http://www.anzhi.com/soft_278753.html	2300+
	安机市场	http://www.anshouji.com/bencandy.php?fid=66&aid=3 4786(v1.0.4)	10+
	N 多	http://www.nduoa.com/apk/detail/252473(v1.0.4)	1000+
	机锋市场	http://apk.gfan.com/Product/App226146.html###(v1.1.3)	3600+
	木蚂蚁	http://www.mumayi.com/android-83075.html(v1.1.3)	2300+

4 移动互联网应用安全影响分析

4.1 内嵌广告造成用户经济损失巨大

出于国内用户的使用习惯，以及整体环境影响，相对花钱购买软件，用户更愿意选择免费软件。孰不知天下没有免费的午餐，使用免费软件的用户，可能会在不知情的情况下花费比购买付费软件更多的费用。

针对检测出的存在敏感行为的应用程序，本中心选取了其中 7964 个自动连接网络的应用程序进行数据流量消耗统计。统计结果表明，这些应用每个小时由于自动连接下载广告会消耗 200KB-500KB 的数据流量，平均流量约为每小时 300KB。

依据艾瑞 2011-2012 年中国移动应用商店用户行为研究报告⁵，手机上网时间一般每天在 5 小时以内，假设按照每个 Android 手机用户平均每天有 4 个小时的时间使用手机应用程序，同时，按照所检测的应用程序中会自动连接网络的应用程序数量占所统计的 19442 个应用程序的 40.96%，由此，可以粗略估算，每个 Android 用户的手机每天广告刷新的时间将约有 $4 \times 40.96\% = 1.64$ 个小时。按平均每个小时耗费的流量是 300KB 统计（这些流量均非用户主动连接网络耗费），这样，每个用户每天因为广告刷新就会耗费 0.5MB 的数据流量。累计下来，每个用户每月会耗费 15MB 数据流量。

按照现有移动运营商收费标准，即使最便宜的 3G 用户在套餐外也需要花费 0.3 元/MB。不算运营商的流量套餐，每个用户每月的话费中，约有 4-5 元是被免费软件所携带的广告所耗费。

另据 91 无线统计数据⁶，截止 2012 年第一季度国内的 Android 智能终端用

⁵ <http://www.iresearch.com.cn/Report/1688.html>

⁶ <http://news.cntv.cn/20120516/106479.shtml>

户数量达 6000 万。仅从这 6000 万 Android 手机用户计算，每个月因广告耗费 9 亿 MB 流量，也就是全国 Android 用户每个月通过这些后台广告就要消耗近 3 亿人民币！

参考官方应用商店的标价，iOS 和 Android 应用商店中应用程序的价格为 3-10 元一个，即用户每月被广告消费的流量，差不多支撑其购买一个不含广告的应用程序。

相对于 iOS 的应用程序开发者的主要收入来源为苹果公司的分成，而在 Android 平台下，鉴于混乱的市场环境与第三方商店的大量分流，应用开发者不得不采取另一种模式来获得经济收入，即植入广告。移动应用中植入广告的模式起源于美国的 Admob 手机广告平台，它通过与开发者合作，在程序中嵌入广告插件代码，以便能绕开运营商对用户所收到的内容进行控制。广告能通过这种方式更精准而直接地触达消费者，为广告主带来效益，然而，无止境的广告对用户的流量也造成了大量的损耗。用户看起来享受到免费服务，但受伤害最大的恰恰是用户本身。植入的广告需要在应用程序执行时自动联网下载广告信息，无形中对终端使用者的经济利益造成了侵犯。

4.2 移动终端普遍感染恶意应用

从检测结果来看，恶意应用的应用数量之巨大、传播面之广远超预期。根据 3.3 节统计结果表明恶意应用程序的总下载量已经突破了两千万次，这是从 20 万应用软件样本中统计出的恶意应用下载量，如果按照第三方商店 50 万个应用软件的规模来推算，将超过 5000 万次恶意应用下载量。而根据上一小节引用的“91 无线”数据，2012 年第一季度国内的 Android 智能终端数量达 6000 万。假设一台智能终端下载到一次恶意应用，就会有超过 80% 的智能终端已被感染或曾被感染。

在这些恶意应用程序中，含有 kungfu 病毒的应用程序数量占比 28%，其下载量约为一百万。即至少有百万级别的用户感染了这种恶意程序。Kungfu 会后台利用系统漏洞静默获取 root 权限，释放安装它所指定的应用程序并接收控制命令。感染这种病毒的移动智能终端除了用户隐私被窃取以外，还有被控制作为

移动僵尸网络的风险。

另一种包含泄露隐私的病毒 Killall 的应用程序总下载量也超过了 50 万。感染此病毒的终端用户隐私会被大量泄露，同时会被诱导下载并安装其它恶意应用程序，以达到攻击者远程控制或造成用户资费消耗的目的。

总的来看，这些移动互联网恶意程序窃听用户电话、窃取用户信息、破坏用户数据、擅自使用付费业务、发送垃圾信息、推送广告或欺诈信息、影响移动终端运行，一旦入侵支付和网上账户等系统，更会带来无法估量的经济损失。同时，这些恶意应用程序已经达到了一个如此巨大的下载量，如不及时处置，用户的隐私和利益得不到有效的保障，最终将会危害整个移动互联网环境安全。

4.3 移动互联网应用产业链不健康

在移动互联网产业链中，手机用户、软件下载渠道、软件开发者、广告联盟商、电信运营商等扮演着重要的角色，其关系如图 4-1 所示：

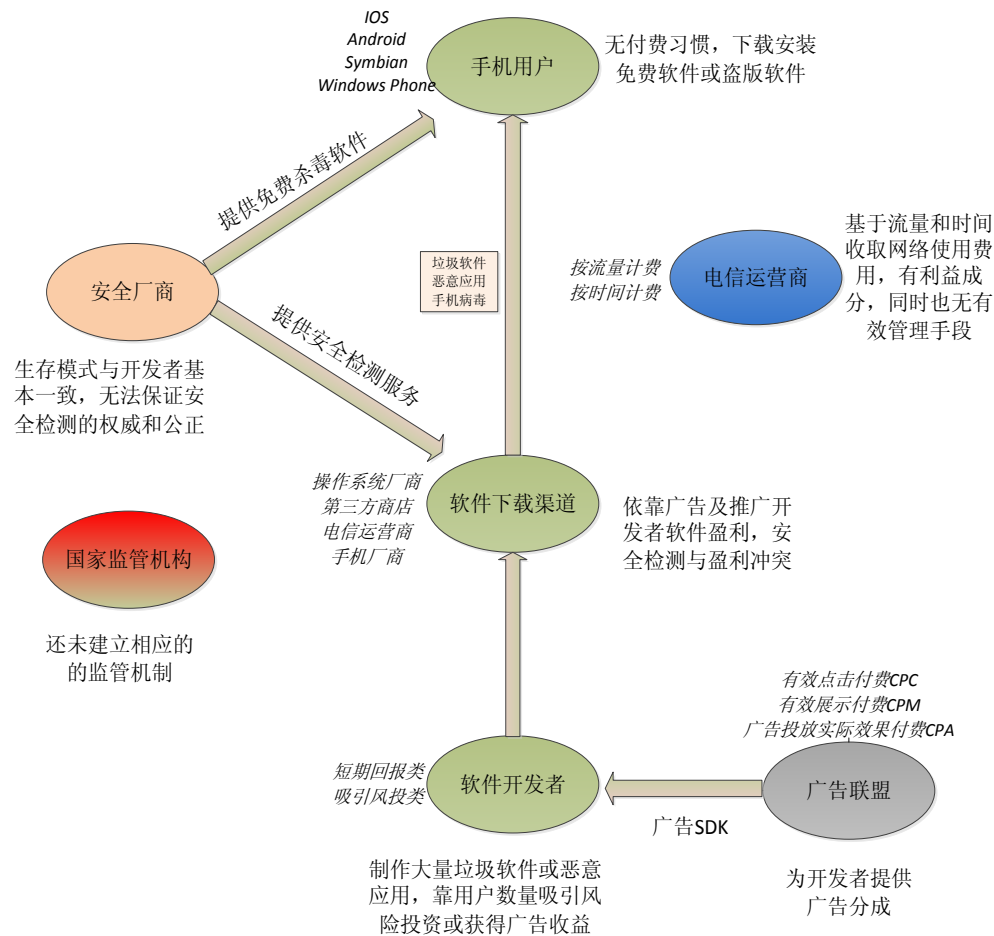


图 4-1 移动互联网产业链

手机用户：

因国内用户使用应用软件大都没有付费习惯，导致除了苹果 appstore 外，其他软件商店只能为用户提供免费的软件，用户从商店中下载免费的软件安装并使用。

软件开发者：

开发者为了生存，往往采取两种模式，一种是积累用户数量吸引风险投资；另一种是短期内制造大量垃圾及恶意应用，吸引用户下载并安装，利用其内嵌的广告用于盈利。

软件下载渠道：

下载渠道主要靠软件推广和发布广告盈利，成功推广一个软件可获得 1-3 元，在首页为一个软件打广告一天收费 5000-15000 元人民币不等，大型的软件下载渠道每年可盈利数千万。

广告联盟：

往往与开发者合作，为开发者提供广告 SDK，与开发者按照 3:7 或其他比例分成，根据 CPM、CPC、CPA 等多种广告投放效果结算，软件被下载、安装次数越多，使用时间越长，广告收益越大。

电信运营商：

为软件下载提供通信线路，如 2G/3G、WIFI、ADSL 等接入方式，通过流量、时间等方式收取费用，不会对用户下载软件中是否存在病毒、木马或恶意应用进行检测。

安全厂商：

为手机用户提供了免费的杀毒软件，并可以为软件下载渠道提供软件安全检测服务，但是目前生存模式存在问题：

- 1、免费杀毒的模式与其他软件开发者生存模式一致，都是靠用户数量盈利，无法保证其权威与公正；
- 2、为软件下载渠道提供的安全检测服务与软件下载渠道的盈利模式冲突，可能导致该渠道软件来源减少进而影响收入，渠道商没有进行安全检测

的动力和积极性。

国家监管机构:

因目前我国在移动互联网安全监管方面的工作刚刚起步,目前没有适用的政策、标准等监管要求,也缺乏相关监管手段进行支撑,对移动互联网应用安全现状“有心无力”。

综上所述,虽然用户可以免费的下载和使用大量应用软件,表面看“占了便宜”,但是从产业链分析看,这样的模式导致我国移动互联网产业目前的不健康状态。

为了生存,开发者如此只能依赖广告及风险投资,开发者无法专注做好的产品,只能每天乐此不彼地开发大量的垃圾及恶意应用;渠道商因无法与开发者分成,只能依靠软件推广盈利,无法保证软件的质量和安全;因利益问题电信运营商、安全厂商等也无法通过市场手段阻止恶意软件的下载和使用。

最终结果导致我国的移动互联网应用产业基本处于混乱和无序状态,损害的是最终用户的利益。

5 结论

根据本报告分析工作，移动互联网应用软件产业势头是非常良好的，但存在的安全问题以及由此带来的影响并不乐观。

经过仔细分析，我们认为导致目前移动互联网应用安全困局的原因主要有以下几方面：

一是目前移动互联网大多数应用软件的盈利模式主要是来自广告点击，而非用户安装使用，这样，应用软件开发商就会与广告商形成利益联盟，在不告知用户的情况下，做出损害用户利益的行为。而要使移动互联网应用成为一个健康的产业生态环境，这种盈利模式是必须能够得到有效管制。

二是移动互联网应用软件数量巨大，每天不断有几千款新应用上架，应用商店和用户目前还没有建立有效机制识别应用软件的可靠性和效能性，因此难免有一些开发者基于恶意应用软件，来损害消费者利益以谋取非法收益。

三是移动互联网应用软件产业还刚显露出一个雏形，暴露出的都是全新的问题，没有现成的监管机制和手段能够直接拿来使用，还处在一个不能有效监管的阶段，这当然给一些恶意应用提供了机会。

基于以上移动互联网应用安全问题的原因分析，我们认为目前是解决这些问题的关键时机，解决的有效方法就是：由工业和信息化部牵头，组织各方力量，专门建立移动互联网应用安全监管体系。

而应用互联网应用监管体系可以通过如下途径来构建：

首先，需要建立移动互联网应用软件安全要求和评测规范体系，指导移动互联网应用开发、使用和监管。

其次，通过应用商店来实现对应用软件的安全管理，对应用软件商店建立实现准入制，只有满足一定资质条件的应用商店，才能开展营运服务。

再次，建立移动互联网应用安全第三方测评机制，由可信赖的第三方测评机构，对应用商店以及应用商店的软件进行安全性测评和评价，而主管部门只需对

第三方测评机构进行监管即可。

总之，面对我国目前移动互联网应用发展和安全现状，必须尽快建立起一个规范有效的监管体系，才能促进其有序和良性发展，这不仅仅对移动互联网应用产业本身有利，对整个移动互联网产业乃至 IT 产业发展都至关重要。

6 附：NINIS 软件安全评估中心

为实现对移动互联网应用安全监测，国家网络信息安全技术研究所专门成立软件安全评估中心(简称 NINIS 软件安全评估中心)，来开展移动互联网应用软件安全检测与评估业务工作。

为使 NINIS 软件安全评估中心发挥更大社会效能，我们将进一步面向社会提供移动互联网应用安全检测服务，进而为国家主管部门实现对移动互联网应用行业监管提供支撑。

在国家有关部门的领导和支持下，经过多年的努力和建设，现已初步建成面向行业和社会需求的移动互联网应用安全检测和评估的服务能力、技术能力和保障条件。

一、具备的移动互联网应用软件安全检测服务能力

(1) 检测服务功能

NINIS 软件安全评估中心提供的移动互联网应用软件安全检测服务，主要是面向移动终端操作系统和应用程序提供如下三个方面的检测功能：

- ✓ **检测应用恶意行为：**包括恶意扣费、远程控制、隐私窃取、恶意传播、资费消耗。
- ✓ **检测应用有害行为：**包括穿透行为、传播有害信息行为
- ✓ **检测软件安全缺陷：**包括异常输入处理、不安全 API 调用、权限管理漏洞、程序漏洞、安全功能误用。

(2) 检测服务对象

我们可以面向国家监管机构、应用商店、应用软件开发、终端制造商、应用使用者五类客户提供移动互联网应用安全检测和评估服务：

i) 面向监管机构，提供：

- 移动终端操作系统安全态势分析服务
- 移动应用安全标准符合性检测服务
- 管理体系建设咨询服务
- 安全整改咨询服务

ii) 面向应用商店、应用软件开发和使用者，提供：

- 应用软件安全检测服务
- 安全合规性咨询服务

iii) 面向终端制造商，提供：

- 移动终端操作系统安全检测服务
- 移动终端存储系统安全检测服务
- 安全技术相关咨询服务
- 安全合规性咨询服务

(3) 检测服务效能

根据目前已建成的检测服务平台和保障条件，我们的检测能力和效能可达到：

检测能力	并发能力
检测 300 个应用程序/每日	100 个应用程序/小时
检测 10 万个程序/每年	每款应用程序处理时间小于 1 小时
含人工参与深度分析	无人工参与

基本能够支撑目前产业服务需求。

二、建成的移动互联网应用安全检测技术和组织保障条件

为支撑移动互联网应用安全检查服务，目前我们建成的技术和组织保障条件如下图所示，包括三部分：

一是我们已初步建立移动互联网应用安全测评规范体系，包括：移动终端操作系统安全技术要求和测评规范、移动终端应用安全技术要求和测评规范、移动应用商店安全技术要求和测评规范、移动终端信息安全要求与测评规范、移动互

联网恶意代码描述规范，该规范体系涵盖移动互联网应用各个层面，是构建移动互联网应用软件安全检测服务的基础保障。

二是移动互联网应用安全测评技术平台，主要是由我们自主开发的技术、工具、特征库、系统构成。根据目前业界目前应用安全检测状况，我们的技术平台目前应该处于业界领先水平。

该技术平台是我们构建移动互联网应用软件安全检测服务的重要支撑。

三是我们建立了一支达 60 人的测评服务队伍，包括一支由博士、硕士组成的、从技术研究到开发到应用服务全覆盖的高水平人才队伍，同时，还建立了专门的服务经营和市场营销队伍，具备了面向社会服务的组织保障条件。

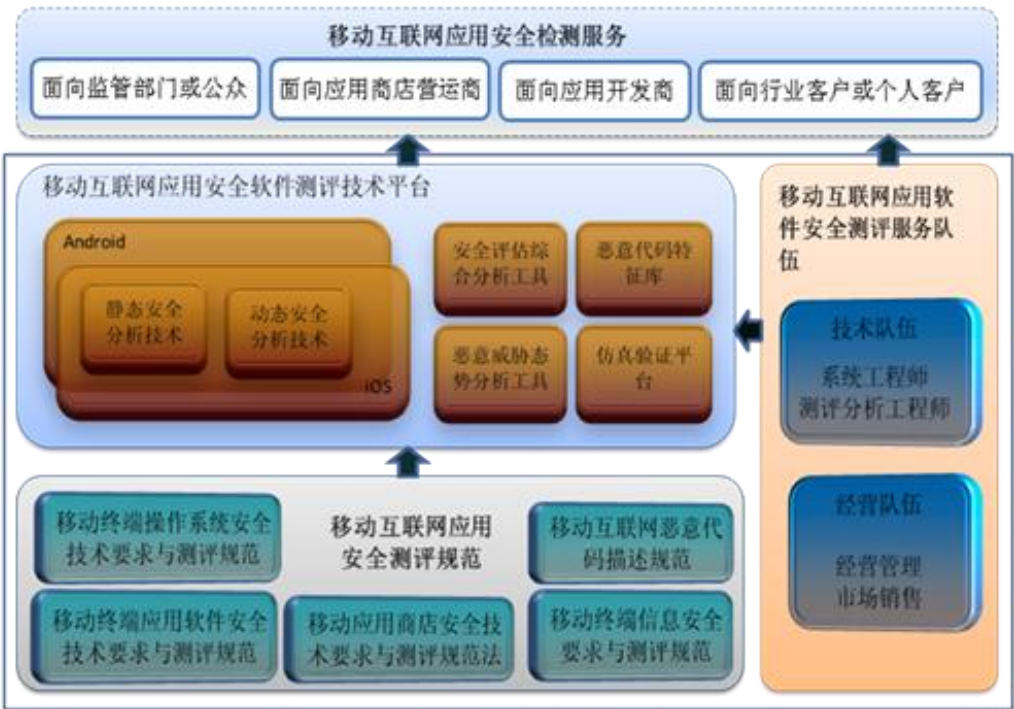


图 6-1 移动互联网安全检测服务

三、强有力的支撑单位服务支持

北京邮电大学和北京软件科技有限公司是我们构建移动互联网应用安全检测服务的重要支撑单位。

北京邮电大学在移动互联网及安全领域拥有高水平的人才资源和科学研究能力，是我们的人才队伍和基础技术研究的后台保障。

北京软安科技有限公司是依托北邮信息安全中心建立的公司，专门从事移动互联网应用软件安全检测业务，具有很好的相关技术积累。我们的移动互联网应

用安全测评服务技术平台就是与软安公司合作建立起来的。

有了这些支撑单位支持，使我们的竞争力持续得到保障。

四、已开展工作

可以说，我们的移动互联网应用安全测评服务能力和测评技术体系是在开展如下国家重大项目技术攻关过程中建立起来的，它们是：

1、2012 年工信部重大专项：智能终端安全检测关键技术研究

2、2011 年工信部重大专项：移动互联网安全关键技术研究

正是这些项目的技术积累，厚积薄发，使我们能构建现有的移动互联网应用安全测评服务体系。

同时，为检验我们的技术服务能力和水平，我们还开展了联想乐 phone 应用商店的检测服务示范工作，主要为：联想乐 phone 应用商店安全检测及防护

(1) 帮助建立严格的手机软件上线前测评工作

- ✓ 源码分析

- ✓ 动态检测

(2) 检测总数超过五万个软件

- ✓ 发现安全问题超过 100 种

- ✓ 恶意应用 30 个左右

联系方式：

电子邮件：ninis@cert.org.cn