免责声明：

该报告综合网秦“云安全”监测平台的统计、研究数据和分析资料，针对 2012 年第一季度全球 Android 手机安全形势发展进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构、厂商作为移动互联网信息安全状况的介绍和研究资料，请相关单位酌情使用，如若本报告阐述之状况、数据与其它机构研究结果有差异，请使用方自行辨别，北京网秦天下科技有限公司不承担与此相关的一切法律责任。

一、安全报告概要

《2012 年第一季度全球 Android 手机安全报告》（以下简称:报告）由领先的移动安全云服务企业 – 北京网秦天下科技有限公司（NYSE：NQ）制作并发布。报告数据显示，据网秦“云安全”监测平台统计，**2012 年第一季度查杀到 Android 手机恶意软件 3523 款，直接感染手机 412 万部。**

2012 年第一季度 Android 平台安全形势图（网秦“云安全”监测平台）

在全球范围内，**中国大陆地区以 26.7%的感染比例位居首位，**美国（15.3%）、俄罗斯（12.6%）、印度（11.4%）位居其后。国内方面，广东省（23.4%）居首，北京（21.5%）、上海（16.3%）紧随其后，山西、海南增长速度较快。

恶意软件特征方面，**隐私窃取类以 24.3%的感染比例位居首位**，远程控制、恶意扣费、系统破坏类、资费消耗类则以 22.6%、21.5%、11.7%、8.4%的比例位居其后。

传播途径方面，数据显示，**应用商店（Google 官方应用商店及第三方应用商店）是恶意软件的主要传**

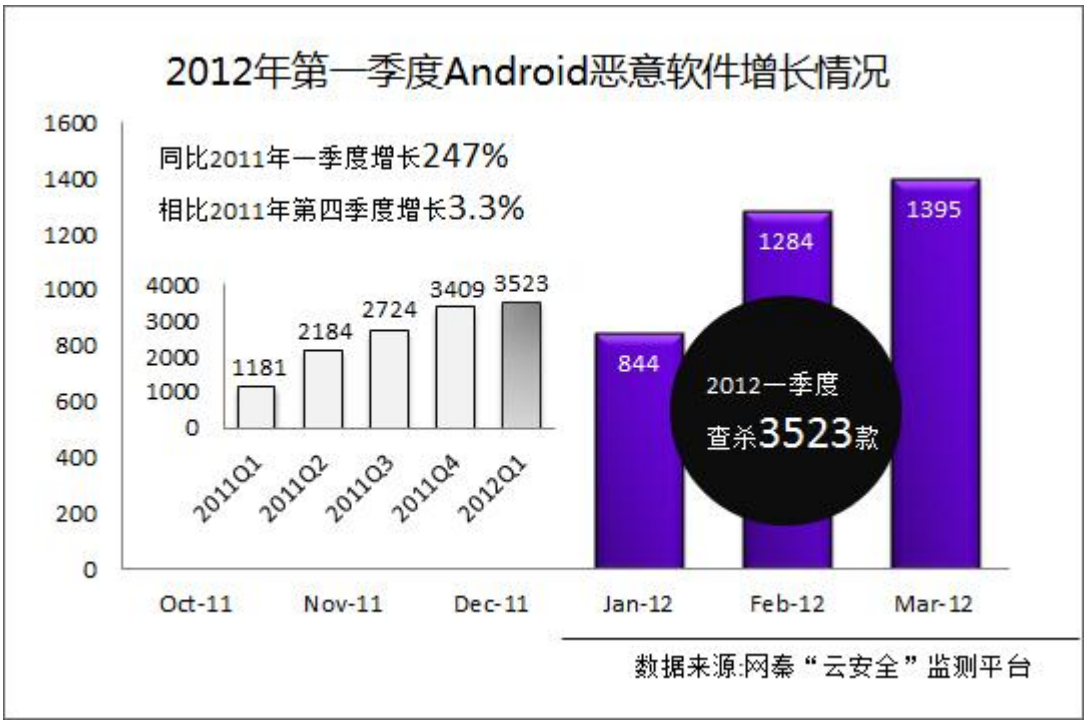
播途径，以 28.4%的传播比例居首，手机论坛、WWW/WAP 网站和刷机包则以 26.3%、13.6%、8.3%紧随其后。

同时，**2012 年一季度中，Google 系列应用正在成为恶意软件的主要伪装对象**，在一季度被伪装次数最多的十款应用中，便有 Google Maps、Google Update、Google Dual Core 三款，其中在中国大陆地区广泛传播的“暗黑推手”便以伪装成 Google 升级来诱骗用户安装用于恶意推广的应用。

此外，本次报告还结合 2012 年一季度的发展情况，对二季度的 Android 安全趋势进行了预测，预测指出，**伴随手机吸费软件在吸费形式、方式、形态上的不断升级，用户的话费安全仍将面临较大威胁**，而**伴随恶意软件开发模式的改变，也将空前增加安全厂商的分析难度**，同时，由于 2012 年基于 Android 系统的智能电视、机顶盒、导航等设备的大规模上市，**恶意软件或将通过变换形式在二季度向其它平台迁徙。**

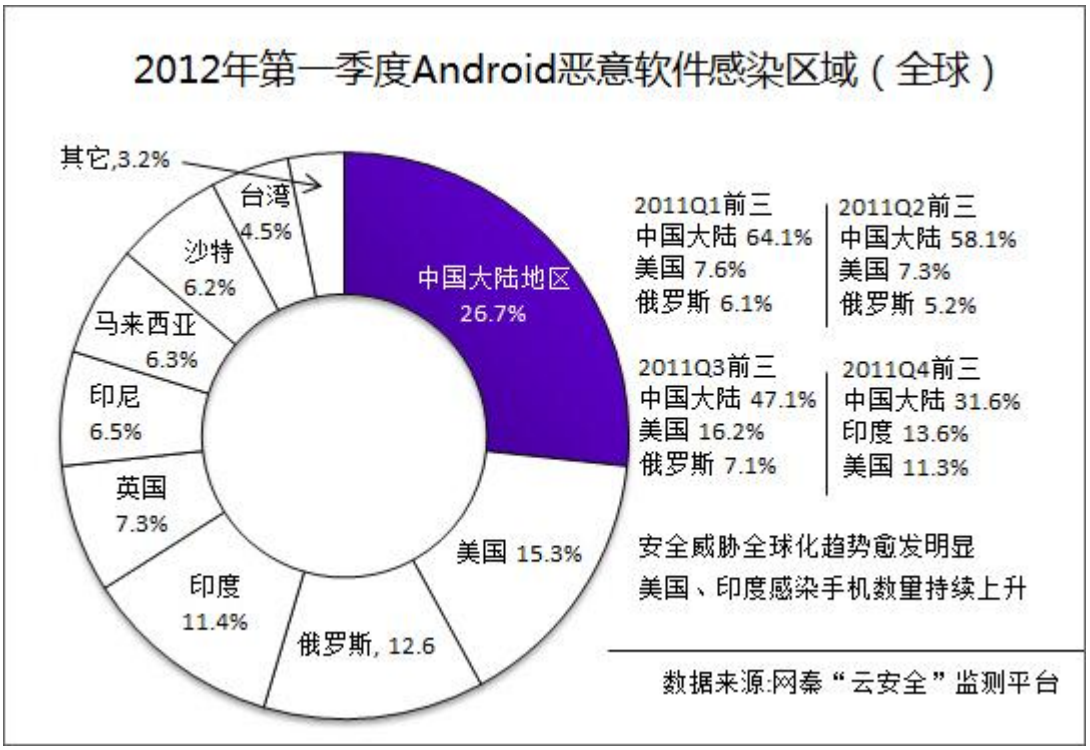
二、平台安全数据

数据显示：2012 年一季度，网秦“云安全”监测平台，**2012 年第一季度查杀到 Android 手机恶意软件 3523 款**，相比 2011 年 4 季度增长 3.3%，同比 2011 年一季度增长 247%。**直接感染 Android 智能手机 412 万部**，相比 2011 年 4 季度增长 90.7%，同比 2011 年一季度增长 200%。



2011 年第一季度 Android 恶意软件增长情况（数据:网秦“云安全”监测平台）

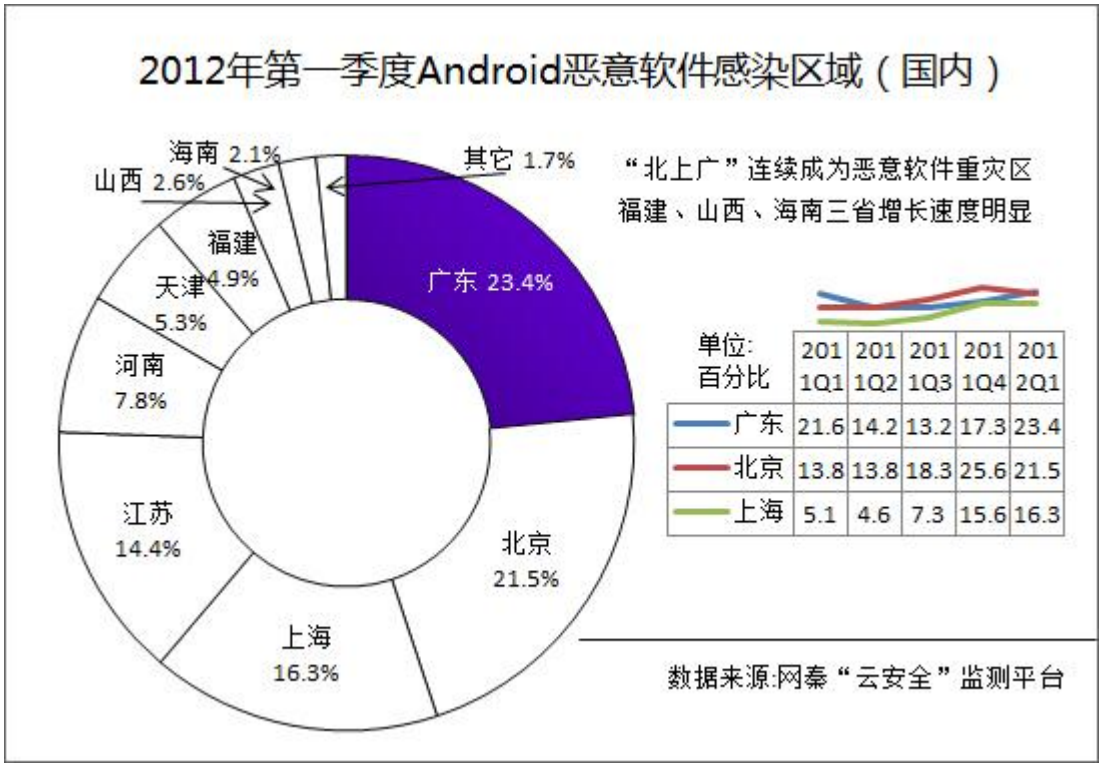
地域分布方面，据网秦“云安全”监测平台数据显示，在全球范围内，**中国大陆地区以 26.7%的感染比例位居首位，**美国（15.3%）、俄罗斯（12.6%）、印度（11.4%）位居其后。



一季度 Android 恶意软件全球感染区域（数据:网秦“云安全”监测平台）

一季度全球 Android 恶意软件重灾区（数据:网秦“云安全”监测平台）

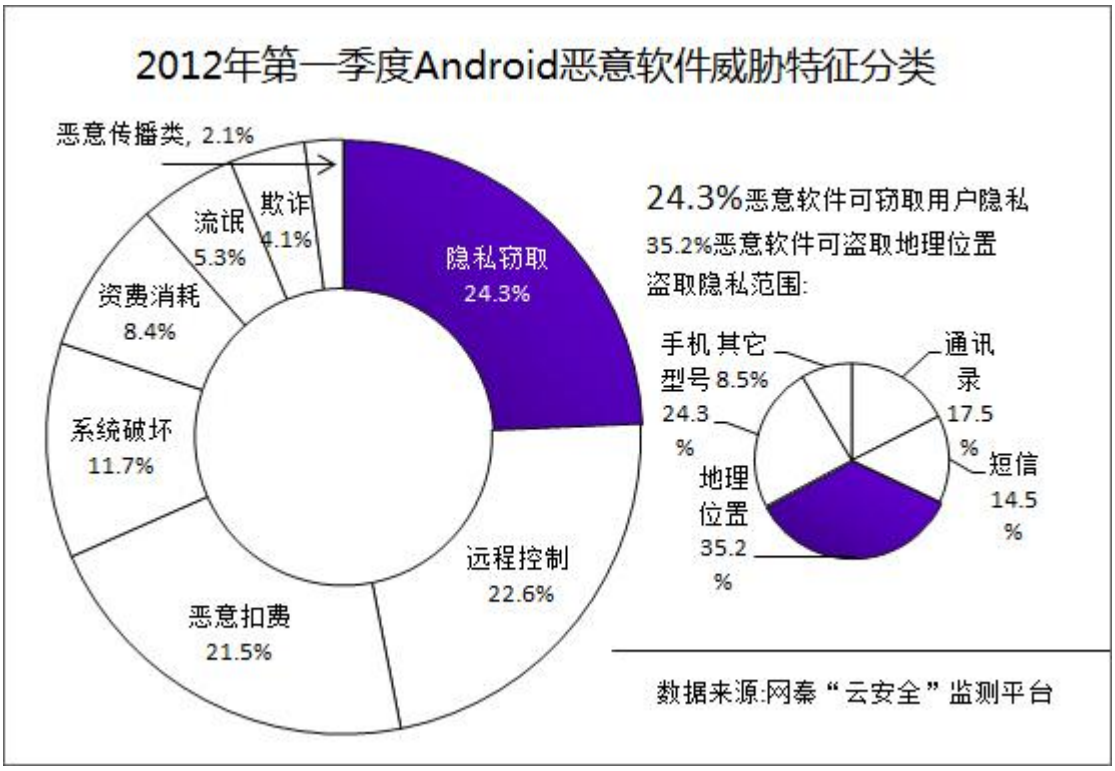
国内方面，广东省（23.4%）居首，北京（21.5%）、上海（16.3%）紧随其后，其中“北上广”地区连续成为恶意软件重灾区，山西、海南增长速度较快。



一季度 Android 恶意软件国内感染区域（数据:网秦“云安全”监测平台）

恶意软件特征方面，**隐私窃取类以 24.3%的感染比例位居首位**，远程控制、恶意扣费、系统破坏类、资费消耗类则以 22.6%、21.5%、11.7%、8.4%的比例位居其后（目前普遍存在一个恶意软件存在多个行为

特征现象，本分类仅以其第一特征为准）。

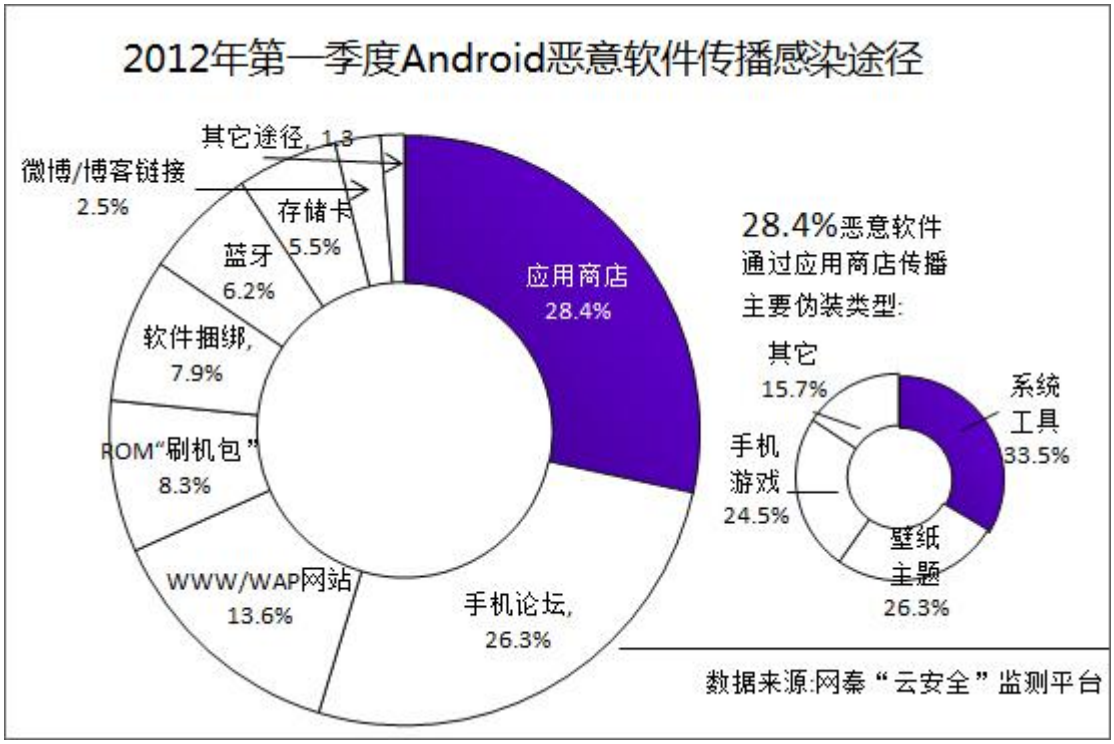


一季度 Android 恶意软件威胁特征分类（数据:网秦“云安全”监测平台）

在隐私窃取类恶意软件中，地理位置成为其主要的窃取目标，**有超过 35%的恶意软件存在盗取用户地理位置的能力**，采用如发送包含地理位置编号的手机短信，并根据卫星地图定位感染目标所在区域的方法窥探用户的位置隐私。

而在恶意软件的传播途径方面，数据显示，**应用商店（Google 官方应用商店及第三方应用商店）是恶意软件的主要传播途径**，以28.4%的传播比例居首，手机论坛、WWW/WAP 网站和刷机包则以26.3%、13.6%、8.3%紧随其后。**其中，Google 应用商店的恶意软件比例为 0.04%**、国内第三方应用商店的平均恶意软件比例在 2%至 15%之间。

其中，**Android 应用工具，如升级组件、浏览器、优化工具、日程、管理软件等成为伪装频率最高的应用，占据总恶意软件比例的 33.5%**、壁纸、主题类位居其后，游戏类排名第三。



一季度 Android 恶意软件感染途径分类（数据:网秦“云安全”监测平台）

在最易被恶意软件伪装的十款应用中，**Google 系列应用正在成为恶意软件的主要伪装对象**，在一季度被伪装次数最多的十款应用中，便有 Google Maps、Google Update、Google Dual Core 三款上榜。

十大最易被伪装的高危 Android 应用（数据:网秦“云安全”监测平台）

三、安全形势解析

1.恶意软件增长趋势解析

通过报告数据可以看到，2012 年第一季度，Android 恶意软件的总查杀款数与上季度相差不大，但在感染量上同比 Q4 增长了 90%以上，由于 1、2 月恰逢假期，用户在闲暇时乐于下载手机应用，导致更易不慎下载到伪装为相关应用的恶意软件。

同时，一季度还相继出现了多款具有较强代表性的手机病毒，如 2 月下旬开始在全国范围内肆虐的“食人鱼”、“吸费蝙蝠”两款应用软件，各自感染量均超过 25 万以上，而 2011 年时便已出现的“安卓吸费王”等也仍有新的变种出现，更导致 Android 恶意软件仍呈现增长趋势，并持续扩散。

2. 恶意软件地域分布解读

地域分布数据中，Android 恶意软件的全球化趋势极为明显，而结合各地的国情、价值取向，恶意软件在不同地域也存在有较大的差异，黑客瞄准的是用户的手机话费，更善于利用伪装应用骗取用户开通各类费用高昂的 SP 业务，从而实施恶意扣费。如 2011 年 3 月开始，一款名为“吸费蝙蝠”的恶意吸费软件，曾在短短一周就累计植入到超过 10 万部手机之中。

而在北美、欧洲地区，黑客则着重于对手机隐私的窥探，来自网秦北美研究中心的数据显示，一季度，

有大量美国、加拿大用户在下载应用时不慎感染恶意软件，而在暴露的隐私信息中，通讯录、地理位置位居前列，浏览记录、交易记录也成为恶意软件收集的内容之一，借此了解用户的行为习惯，用以推送各类广告信息。

Android 恶意软件在不同地区的攻击重点（数据:网秦“云安全”监测平台）

在南亚、中东地区，由于存在一定的宗教与社会矛盾，恶意软件又多以信息散播为主要目的，如在 2012 年 3 月，网秦曾在中东地区截获一款以散播某海湾国家宗教领袖肖像，以修改短信内容、篡改手机内图片信息为特征的 Android 恶意软件，通过恶意传播，短期内可将指定的推送信息传播到数万部手机之中。

3.恶意软件感染特征判定

在 2012 年一季度中，隐私窃取、远程控制和恶意扣费仍然是用户面临的主要恶意软件类别，其中，隐私窃取类应用的增长速度惊人，并与其它类恶意软件存在着特征并行的现象，如一款恶意软件既存在扣费代码，又会收集用户的隐私信息，而在主要收集的用户信息中，除通话、短信等敏感内容外，**通常会与 Android 手机绑定的 Gmail、Facebook 账户等，也是其收集的主要对象，**借以分析、了解用户习惯并有针对性的推送广告内容和传递各类虚假欺诈信息。

而在 2011 年下半年开始持续增长的“远程控制木马”在一季度的数量略有下降，这与全球各地均开始加大对恶意软件联网地址的监控、封堵有关，经过相关安全厂商的紧急预警，和各地政府、运营商的积极介入，已有大量恶意软件的控制端 – 远程服务器失效，导致其在植入手机后，也无法再发挥任何效用，而搭载服务的成本逐渐增高，使得这类应用的数量呈降低势头。

相比之下，恶意扣费软件则在一季度呈现上升趋势，其优势在于，具备更强的伪装和传播能力，如 2011 年出现的“食人鱼”、“吸费蝙蝠”等恶意扣费软件，伪装应用数量均超过 100 款，通过密集传播威胁用户的话费安全。

4.安全威胁传播途径分类

传播途径比例中，Android 应用商店依然是恶意软件的主要传播途径，实际上，2011 年下半年至 2012 年一季度，国内外应用商店均已开始引入或自制安全审核机制，但由于 Android 恶意软件的特征分类较多，隐蔽性极强，且存在植入手机后再通过远程指令对后续行为进行变异的情况，使其实际具备有绕过一些非专业安全审核机制的能力，导致其仍可上传到应用商店之中。

如监测数据显示，尽管 Google 已在年初引入了对应用商店的安全审核，但在目前 Android 应用商店的 42 万 5000 款海量应用中（截至 2012 年 4 月，Appbrain 网站数据），**恶意软件的比例仍超过 0.04%**。而目前活跃于全球范围内的中小第三方应用商店，受技术条件制约，安全形式也不容乐观，仅以中国大陆地区为例，目前**国内第三方应用商店的平均恶意软件比例在 2 至 15%之间。**

四、安全防护建议

从 2012 年第一季度的监测数据可以看出，当前 Android 用户仍面临严峻的移动安全威胁，而为避免遭遇安全风险，网秦手机安全专家也为用户提供了安全建议：

1.遏制 Android 手机病毒/恶意软件

一季度 Android 安全报告显示，平台安全形势仍在持续恶化中，而近期在多家 Android 软件商店中，频繁出现伪装成正常手机软件，以外发短信等形式实施恶意扣费、隐私窃取行为的 Android 手机病毒及恶意软件。故建议用户下载应用之后，及时通过专业安全工具进行安全性排查。如“网秦安全”6.0 Android 版（下载: http://www.netqin.com/products/antivirus/android/）软件，基于“本地+云端”双向监测，将可有效识别一系列存在高危风险的手机恶意软件。

目前，网秦安全已经具备一站式立体防御体系，可以有效避免恶意软件在获取 ROOT 权限后联网操控威胁用户隐私安全的现象。同时有效抵御恶意网址对手机用户的侵袭，全面查杀 2012 年第一季度新增的 Android 恶意软件及其变种程序。

网秦安全针对恶意软件构建的一站式立体防御体系（数据:网秦“云安全”监测平台）

2.保护 Android 手机话费/隐私安全

2012 年第一季度以来，隐私窃取、恶意扣费软件数量激增，同时由“远程控制木马”比例仍居高不下哦，为确保用户的话费、隐私安全，专家建议用户选择如“网秦安全”6.0 Android 版来全面保护我们的话费安全。

同时，可通过网秦安全 Android 版中提供“联网管理”功能，全面阻止恶意软件试图索取核心权限后自动联网、自动上传和下载数据的恶意行为，避免因不慎感染恶意软件而遭遇安全威胁，真正阻止“远程控制木马”的肆虐。

3. 确保应用程序的下载安全

安全报告数据显示，应用商店、手机论坛依然是 Android 恶意软件的主要传播渠道，对此，专家建议用户应尽量选择已与安全厂商建立合作管理的软件应用商店，并在下载同时，可通过如网秦“云安全”在线监测平台对其进行安全鉴定，确保下载内容已经过了安全检测。

同时，建议在手机中安装具备实时防护功能的手机安全软件，在安装程序前会扫描其的安全状态，一旦发现其中存在有可能触发扣费或窃取隐私行为的现象，将阻止其安装并立即进行删除。

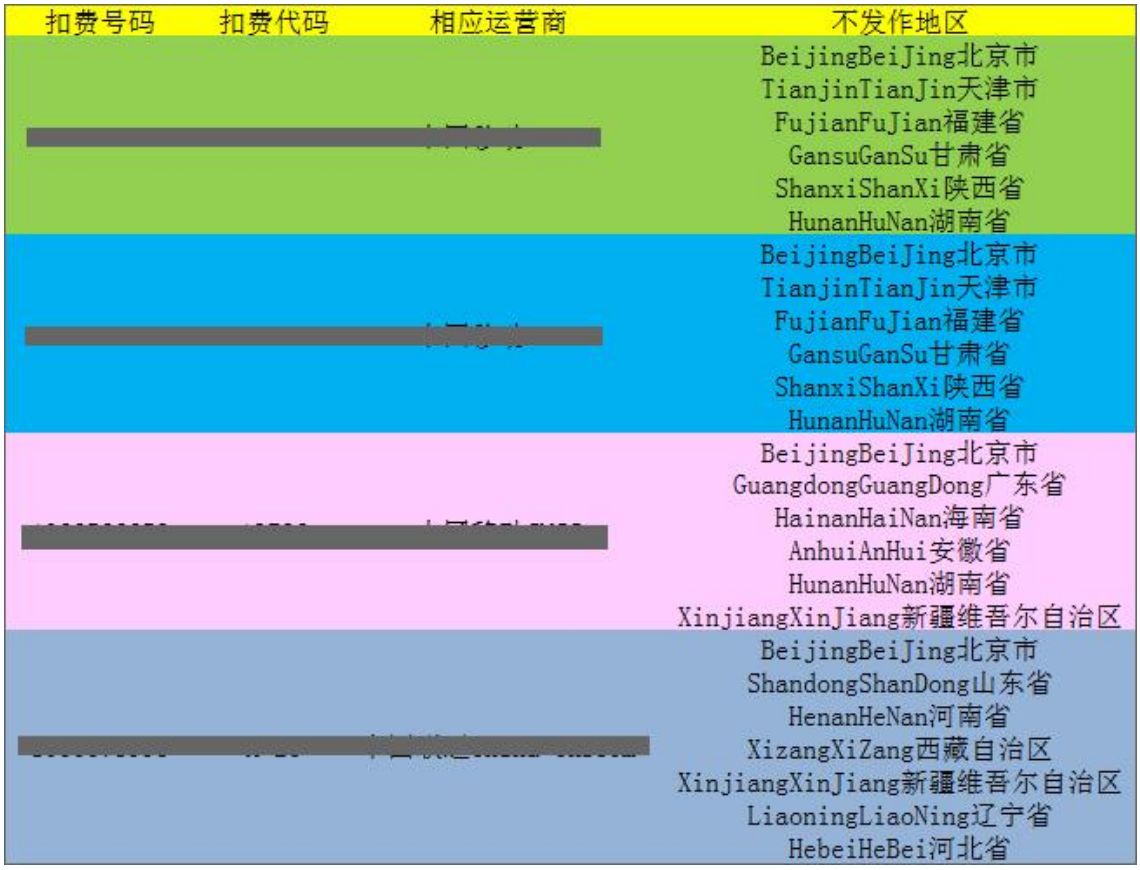
五、安全趋势预测

从数据和走势分析可以看出，2012 年一季度的 Android 安全威胁出现了很多新的改变，而数据依据整体的数据走势和技术形势，也对 2012 年二季度，乃至 2012 全年的安全趋势进行了预测，其中包括，认为手机吸费软件的功能将持续升级，新技术的融入将增大对其的分析难度和 Android 恶意软件向更多平台的迁移。

预测一、恶意软件的功能将持续升级，威胁、危害范围更大（形式、方式、形态的升级）

实际上，从 2012 年一季度的监测数据与分析中就可以看出，Android 恶意软件的功能正在持续升级，以恶意吸费软件为例，通过分析可看出，目前大多数 Android 吸费软件的**扣费形式**已从过去通过本体配置好的特征与行为进行扣费，升级为通过接收远程服务器指令来灵活配置扣费，对此，我们认为这将是一个重要的趋势，未来恶意吸费软件将可能全部通过联网控制，使其具备更强的扩展性。

同时，集合国内、海外不同地域运营商会对本地设置不同的计费政策，未来恶意吸费软件在**扣费方式**上也会有很大的改变，如目前我们已发现有吸费软件可通过灵活配置不同的 SP 计费号段，针对不同地区的收费政策来进行服务配置，从而实施扣费，甚至有选择的规避一部分敏感度较高的区域，甚至不断通过变换扣费区域来躲避查杀和监管。



扣费号码	扣费代码	相应运营商	不发作地区
[redacted]			BeijingBeiJing北京市 TianjinTianJin天津市 FujianFuJian福建省 GansuGanSu甘肃省 ShanxiShanXi陕西省 HunanHuNan湖南省
[redacted]			BeijingBeiJing北京市 TianjinTianJin天津市 FujianFuJian福建省 GansuGanSu甘肃省 ShanxiShanXi陕西省 HunanHuNan湖南省
[redacted]			BeijingBeiJing北京市 GuangdongGuangDong广东省 HainanHaiNan海南省 AnhuiAnHui安徽省 HunanHuNan湖南省 XinjiangXinJiang新疆维吾尔自治区
[redacted]			BeijingBeiJing北京市 ShandongShanDong山东省 HenanHeNan河南省 XizangXiZang西藏自治区 XinjiangXinJiang新疆维吾尔自治区 LiaoningLiaoNing辽宁省 HebeiHeBei河北省

2012 年一季度出现的吸费软件已可有针对性的回避部分地区（“吸费蝙蝠”代码截图）

而在未来，恶意吸费软件在**功能形态**上还将进一步增强其的伪装、隐蔽性，如在吸费软件中同时实现对用户身份信息的读取，借以分析用户习惯、使用属性等，借此更有针对性的通过传播信息诱骗用户的话费支出， 甚至通过计费同步等手段，掌握用户的话费充值、通话频次，实现仅在话费充足或刚刚拨打电话后进行扣费等，并采用小额、多次的扣费方式，使其更加不易被用户察觉。

预测二、恶意软件的隐蔽性更强，空前增大分析难度（混淆代码、隐藏进程及属性）

而在 Android 恶意软件不断变换其特征与行为方式之外，在分析中实际已发现，恶意软件的代码混淆力度正在日益加强，这将空前增大对其的分析难度，如对于早期的部分吸费软件，通过程序类名、变量名能初期判断出其行为，而通过混淆代码后，已无法通过此前预设的此前一些条件去筛选，只能逐个对应每个代码类和函数细节，才能找到其在后台运行的踪迹。

同时，在分析中还发现，目前 Android 恶意软件还越来越多的开始引入 PC 病毒的开发技术，如将代码写入到系统的底层，而非此前的应用框架层中，且已具备隐藏进程，隐藏文件属性的能力。导致技术人员将很难通过信息匹配判断就判定其的直接特征，加之黑客同时提高了对恶意代码的加密层级，更使得分析难度空前增大。

对此，我们预测在 2012 年中，恶意软件在技术方面也将有较大的升级，除目前已发现的相关特点之外，恶意软件还可能会越来越多的对手机操作系统进行持久性的破坏，如劫持手机的开机项目，使恶意软件可随开机就在后台启动，如劫持浏览器、应用程序，使其可辅助于恶意软件的行为触发等，让用户更加难以察觉，让安全技术人员更加难以判断。

预测三、恶意软件将快速向更多数字终端延伸（平板电脑、智能电视、机顶盒）

除功能、形态和技术上的升级，报告预测，2012 年二季度乃至全年中，伴随 Android 4.0 等新平台的推出，Android 操作系统将可支持包括平板电脑、智能电视等更多终端设备，但在为用户提供更多优质服务的同时，随之而来的安全问题也将凸显。

对于基于 Android 操作系统的平板电脑，我们预测将在 2012 年面临极多的安全威胁，如在支持通话功能的 3G 平板电脑中，吸费软件可同样通过各种扣费方式，以订购业务的方式损耗用户的通话费用，并通过恶意推广消耗用户宝贵的 3G 网络流量等，同时由于恶意应用适配性的增强，手机间谍软件也多将可运行在平板电脑之中，直接窥探用户保存在设备中的隐私信息。

而日益普及的智能电视，由于同样采用了更为开放的机制，使其也将面临较多的安全隐患，如通过恶意软件可盗取用户的点播习惯，购买习惯等，使用户沦为信息买卖的对象，利用可同样联网的智能电视构建新的僵尸网络，用以群发垃圾邮件，肆意散播欺诈信息等，同时还可劫持智能电视中的摄像头等设备，通过对其的恶意操控感，直接威胁到用户的室内安全。