全球 Android 手机安全报告【2011.Q2】

免责声明：

该报告综合网秦“云安全”数据分析中心、网秦全球手机安全中心等部门的统计、研究数据和分析资料，针对 2011 第二季度全球 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于此相关的一切法律责任。

一、安全报告概要

近日，领先的移动安全服务企业 – 北京网秦天下科技有限公司（以下简称网秦）发布了《2011 年第二季度全球 Android 手机安全报告》（以下简称报告），报告数据显示，**据网秦“云安全”数据分析中心统计：2011 年第二季度新增 Android 手机恶意软件及其变种达到 2386 款**（其中恶意软件 1214 款）。

2011 年第二季度 Android 平台安全形势图（网秦“云安全”数据分析中心）

报告数据显示，中国大陆地区以超过 58.1%的感染比例位居首位（国内广东省位居首位），隐私窃取类恶意软件以 43.5%的感染比例位居首位，其中 54.2%的恶意软件会通过联网上传用户手机中的隐私内容。渠道方面，手机论坛的感染比例正在持续上升。平台方面，受到市场份额递增的情况影响，Android 2.2 版操作系统的感染比例依然最高。

同时，以 Documents To Go、深度睡眠、屏幕水雾等伪装对象，植入恶意代码实施恶意扣费、窃取隐私的现象持续上升，相关软件也成为了 **2011 年第二季度的十大 Android 高危软件**的伪装对象。由于恶意软件正在将伪装对象转向到一系列热门的 Android 应用，用户感染恶意软件的机率正在加大。

报告中的一系列数据和信息表明，Android 恶意软件对用户的威胁正在持续上升。对此，本次安全报告也将对其的传播、泛滥原因进行详细解读，并将针对 Android 平台的安全趋势，同步提供针对恶意软件泛滥、隐私安全、下载安全的对应解决方案。

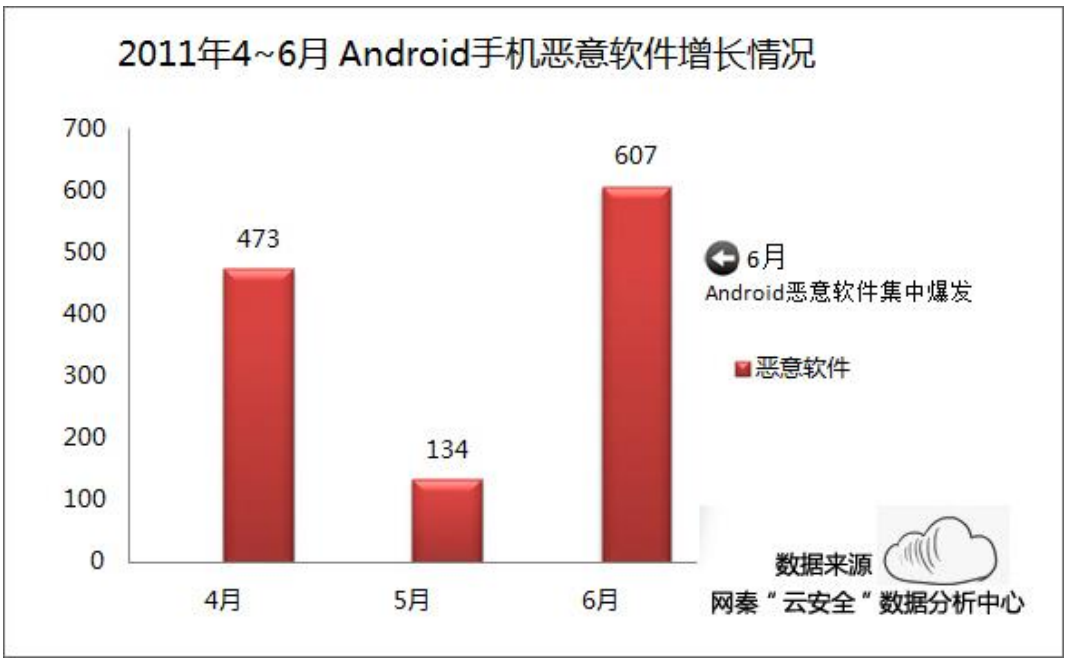
近年来，伴随 Android 安全技术的日益成熟，相关安全厂商也在通过创新技术来提供更为全面的安全解决方案，移动“云安全”技术的全面应用和“实时扣费拦截”、“隐私权限保护”等创新技术的融入，也将整体提升安全软件的性能。此处将在报告“安全技术解析”章节提供重点解读。

二、平台安全趋势

1.安全趋势:安全威胁 6 月呈增长趋势

恶意软件威胁走势方面，据网秦“云安全”数据分析中心统计：**2011 年第二季度查杀到 Android 手机恶意软件及其变种达到了 2386 款**（其中恶意软件 1214 款）， **6 月 Android 恶意软件更呈现增长趋势**，相继出现“短信大盗”、“安卓窃听猫”等以窃取隐私为目的恶意软件，大量恶意软件也出现了数个新变种，并出现了通过“自动拨号”触发扣费和通过 GPS 定位漏洞来窃取用户地理位置的恶意软件新特征。

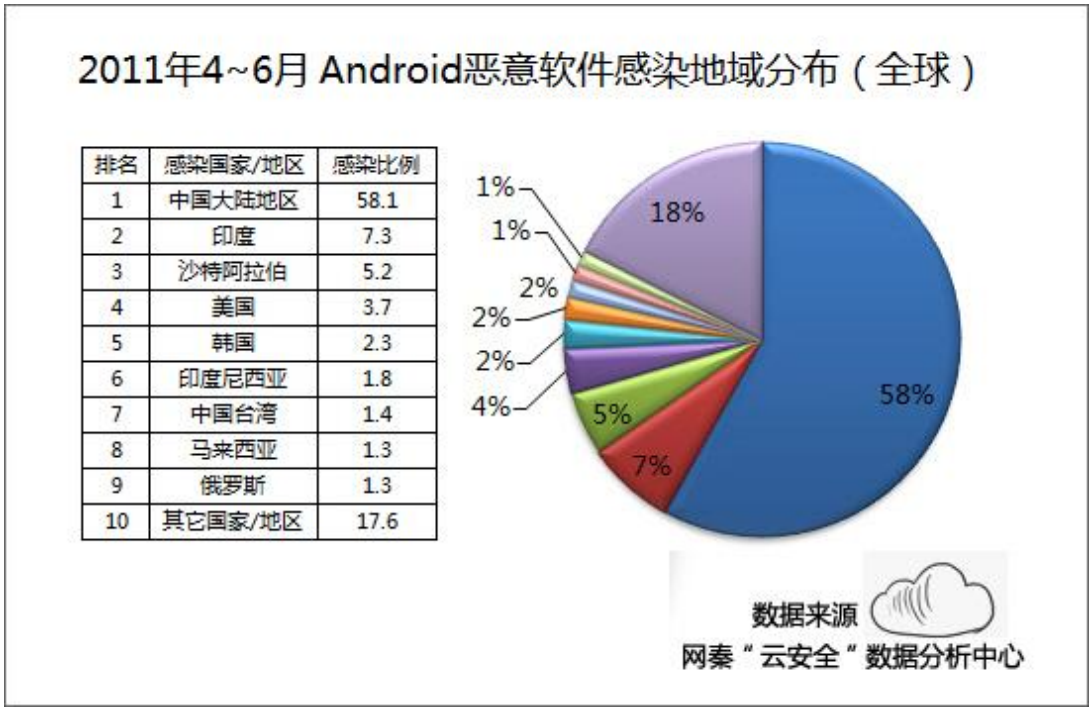
.



2011 年 4~6 月 Android 手机恶意软件增长状况

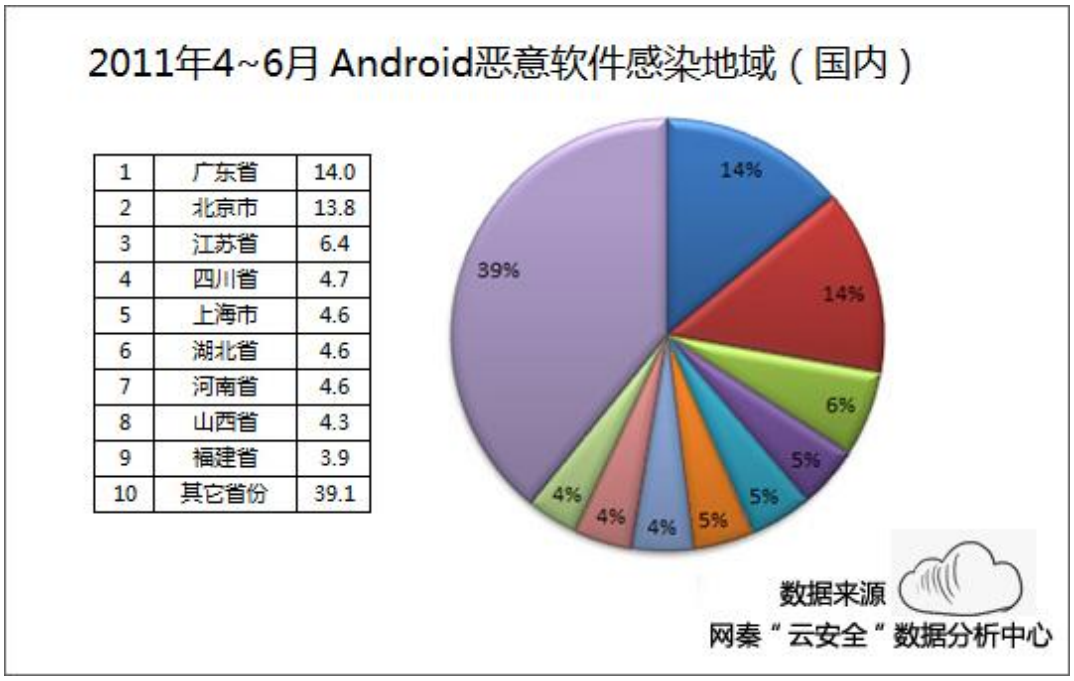
2.恶意软件地域分布:中国大陆成重灾区 广东省居首

感染地域方面，全球范围内**中国大陆地区以 58.1%的感染比例成为威胁重灾区**，印度（7.3%）、、沙特阿拉伯（5.2%）、美国（3.7%）位居其后。



2011 年 4~6 月 中国大陆地区以 58.1%的比例排名全球第一

国内方面，**广东省以 14%的感染比例居首**，北京（13.8%）、江苏（6.4%）、四川（4.7%）等省份同样饱受威胁。

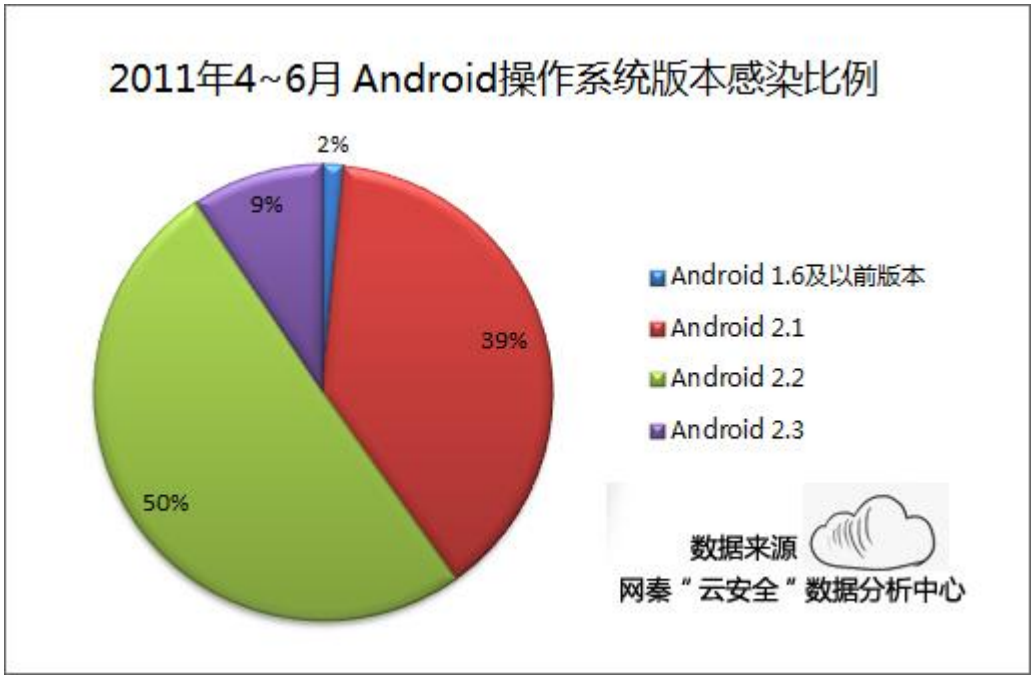


2011 年 4~6 月 广东省以 14%的感染比例位居国内首位

3.平台感染比例:Android2.2 成主要感染对象

在 Android 操作系统版本分类方面， **Android 2.2 的感染比例依然最高，以 50.5%的比例成为最易被**

恶意软件攻击的 Android 操作系统。Android2.1.、2.3 的受感染比例略有下降。这与 Android 操作系统的市场份额递增有明显关系。

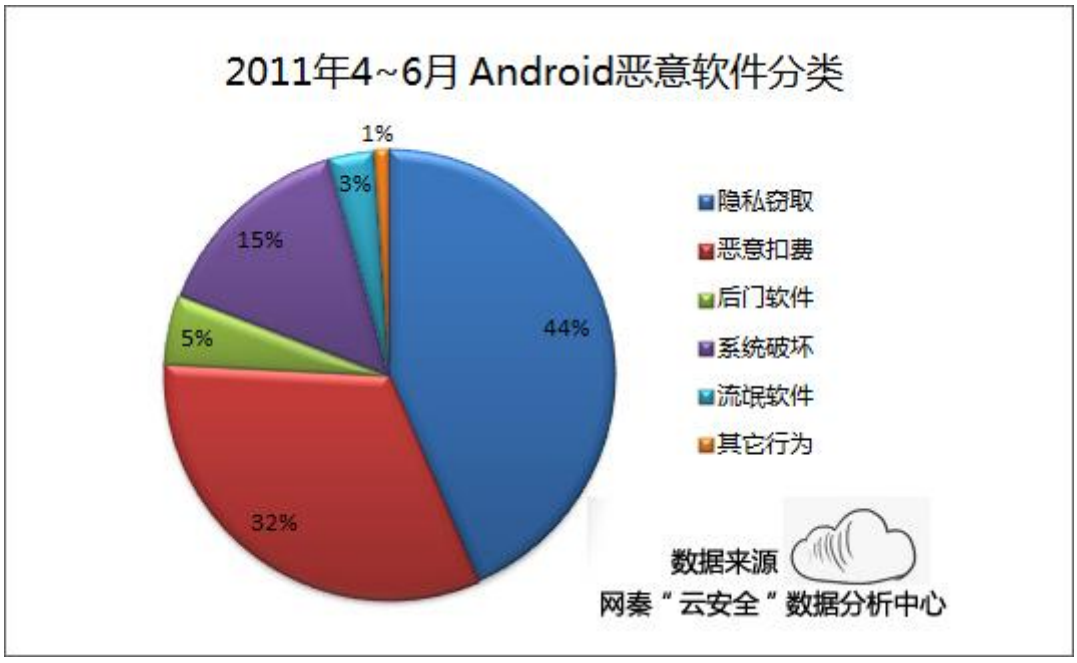


2011 年 4~6 月 Android 操作系统版本感染比例

4.恶意软件特征分类:隐私窃取成恶意软件主要特征

恶意软件分类方面，**隐私窃取类软件以 43.5%的比例位居首位**，扣费类（32.3%）、后门软件（5%）、系统破坏（14.8%）位居其后，另有 3.3%的恶意软件存在流氓行为，1.1%的恶意软件存在其它行为（如恶搞软件等）。

二季度数据显示 44%的 Android 手机病毒存在隐私窃取行为

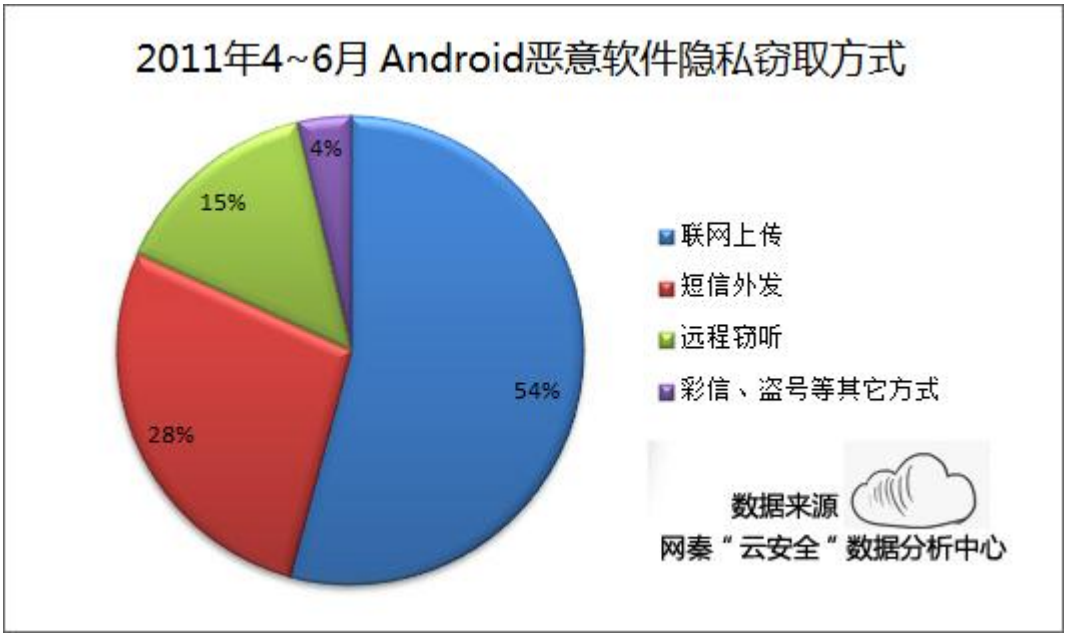


2011 年 4~6 月新增 Android 恶意软件特征分类

备注：恶意软件通常会存在若干种威胁特征，本分类以其第一特征为判定标准，其中扣费类恶意软件包括以诱骗用户开通 SP 服务进行恶意扣费和以联网上传、外发短信、自动拨号等形式消耗用户资费的行为。

隐私窃取类恶意软件的主要窃取类型（通话、短信、照片和密码信息）

其中，隐私窃取类软件当前已包括有，窃取用户通话、短信、照片信息、定位用户地理位置、上传手机型号、系统型号等行为。**54.2%的恶意软件会通过联网上传用户的隐私内容**，27.6%的恶意软件在植入手机后会通过短信外发隐私，14.5%的恶意软件可远程窃听通话，3.7%的恶意存在采用其它方式（如彩信、远程盗号等）。

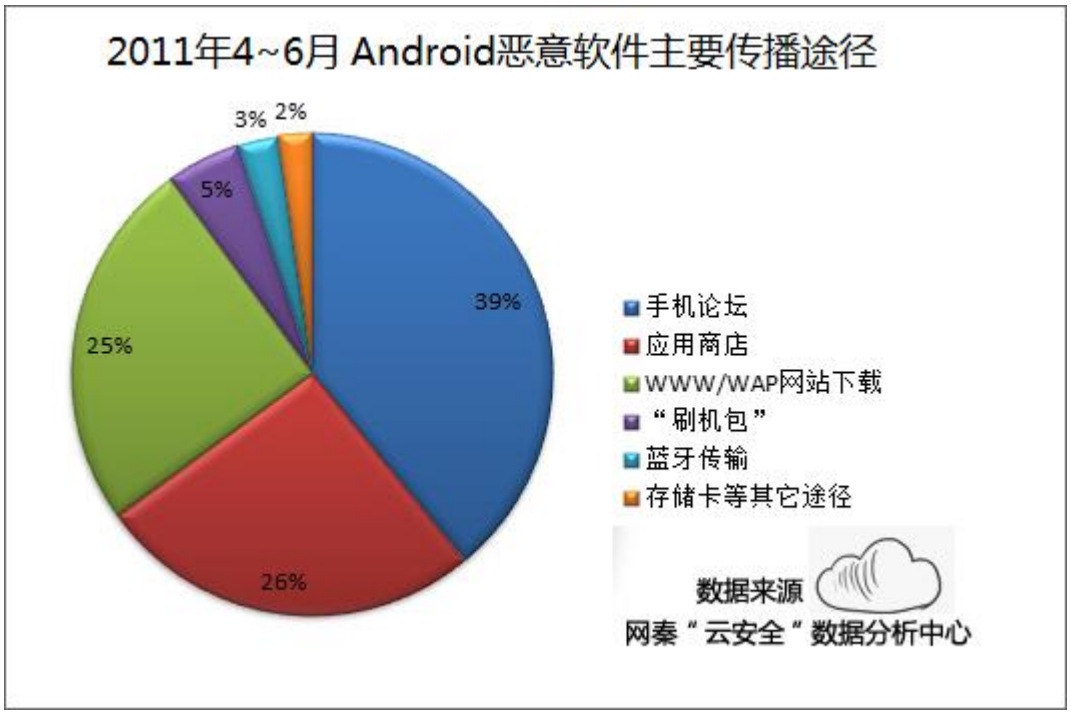


2011 年第二季度 Android 恶意软件主要隐私窃取方式

5.恶意软件传播途径:手机软件论坛成高危区域

感染途径方面，据网秦“云安全”数据分析中心统计，手机软件论坛的危险指数正在持续上升，**以 39%的比例成为 Android 手机病毒以恶意软件的传播重灾区**，Android 应用商店则以 26%的比例位居其后。

2011 年二季度手机软件论坛成为 Android 病毒的传播重灾区



2011 年第二季度 Android 恶意软件主要传播途径

三、安全形势解析

相比第一季度，二季度 Android 恶意软件出现了很多新的特征，包括通过“自动拨号”实施扣费，后台录制手机通话、周围环境音并联网上传等。且均在 6 月的增长速度较快，使得 2011 年 6 月安全形势出现了较为严峻的局面。

1.恶意软件增长趋势

通过报告数据可以看到，二季度 Android 恶意软件继续呈现增长趋势，2011 年 6 月，出现“安卓窃听猫”和“跟踪隐形人”为代表的隐私窃取类恶意软件，大量恶意扣费类软件出现了大量的变种，使得其在 6 月呈现了集中爆发趋势，用户安全面临着严重考验。

2.恶意软件地域分布

由于中国大陆地区的 Android 手机出货量呈现了井喷态势，除依托传统卖场之外，网络营销和电信合作项目的出台，更使得其用户数持续增长，但由于国内手机论坛、应用商店仍缺乏一定的安全验证机制，且仍有用户处于猎奇心理试图接触可能存在安全风险的软件，如购买“X 卧底”等，使得**中国大陆地区的安全形势依然较为严峻**。由于我国广东省、北京市的 Android 手机基数更高，使得其感染机率也相对更大，在地域感染比例中位居前列。

3.系统平台感染比例

在本次包括中可以看出，二季度 Android 平台下，Android2.2 操作系统的感染率依然最高。这主要由由于部分定制机和改装机均基于 Android 2.2 系统，使得其市场份额相对较高导致。而伴随下半年，升级至 Android2.3 及更高版本的手机份额上升，这一比例将逐渐有所变化。

4.恶意软件感染比例

伴随 Android 应用的广泛实施，使其正在逐渐成为用户的掌上隐私信息中心，除短信、照片等手机存储内容外，第三方应用程序的账户密码、应用软件的历史记录、地理位置、游戏信息等隐私也正在成为黑客试图窃取的目标。使得**二季度隐私窃取类恶意软件的比例明显增加。**

而从目前发现的恶意软件中，主要的窃取方式为联网上传用户通讯录、短信和地理位置信息， 相比之下，由于 Android 手机可轻松实现联网，且支持 WIFI 等功能，使得手机在线时间极长，一旦感染恶意软件，且任由其在后台运行，极易利用 Android 手机的后门漏洞来上传隐私内容。二季度报告显示**超过 54%的恶意软件会联网上传隐私**，已超传统的短信外发等形式。

而一旦通过恶意软件获取到用户的隐私内容，如通讯录后，便会通过定向传播方式，向其通讯录中的好友发送推广短信，甚至二次传播手机病毒等等。而部分公司则依托于传播恶意软件，通过获取用户隐私后兜售给部分 SP 公司进行盈利，直接导致了垃圾短信泛滥和部分欺诈信息的广泛传播。

5.安全威胁传播途径

二季度以来，伴随 Google 官方不断加强的 Android 应用商店内资源的安全管理，以及国内多家应用商店与相关安全厂商开展的合作，使得应用商店的安全性已得到整体增强。而应用商店中可由网友任意上传资源的手机论坛则由于内容参差不齐，其基本缺乏安全验证体系，使得**手机论坛极易成为恶意软件的主要传播对象**，其感染比例也出现了较高的增长。

2011 年 5 月，一款伪装为多款热门手机应用的恶意软件在数家缺乏安全验证的手机论坛中进行传播，由于缺乏系统管理，相关主题帖被发现多日后仍然无法联系到管理员进行删除操作。

同时，在本次安全报告公布的 2011 年第二季度的十大 Android 恶意软件中我们也可以看到，恶意软件正在将其的伪装方向转移至 Android 的热门应用之中，一旦用户在缺乏安全机制的渠道下载到被伪装为正常软件进行传播的手机病毒及恶意软件，极易被植入恶意代码，造成个人财产、隐私的损失。

四、十大高危软件

2011 年第二季度，网秦“云安全”数据分析中心共查杀到 Android 恶意软件 1214 款。其中伪装为 Documents To Go、深度睡眠、屏幕水雾、美少女麻将馆、高级任务管理器进行传播的恶意软件感染次数最高，为二季度感染量为被伪装频率最高的十大高危软件。

1.伪装对象:**Documents To Go**
这是一款知名的掌上办公软件，部分传播渠道的安装包被植入了“安卓吸费王”病毒代码，感染用户后将在后台自动联网下载用于恶意推广的软件，大量消耗用户的手机资费。
2.伪装对象:**深度睡眠(5 倍)**
深度睡眠是一款 Android 平台上火热的手机催眠软件，部分黑客将“安卓吸费王”病毒代码植入到部分深度睡眠软件中，一旦用户安装将被触发扣费行为。
3.伪装对象:**屏幕水雾**
屏幕水雾是一款知名的手机个性软件，推出以来便深受好评，部分黑客将手机病毒代码植入到部分屏幕水雾软件中，扣去资费的同时窃取用户的手机型号等信息
4.伪装对象:**BatteryLife**
BatteryLife 是一款 Android 手机的省电软件，可以最大限度的节约电量，因其实用性较强得到了很多用户的青睐。而部分黑客也会将隐私窃取代码植入到这款软件之中。
5.伪装对象:**美少女麻将馆**
作为一款深受用户喜爱的 Android 游戏，美少女麻将馆在二季度也成为了手机病毒的重点模仿对象，部分黑客将“扣费恶魔”手机病毒伪装成这款游戏骗取用户下载。
6.伪装对象: **异能警察**
异能警察游戏在 Android 平台上大热，二季度，部分黑客将隐私窃取代码打包到软件中，诱骗下载骗取用户的短信、通讯录信息
7.伪装对象: **高级任务管理器**
高级任务管理器可以帮助 Android 用户更加全面的管理手机资源，二季度网秦“云安全”数据分析中心却发现了大量伪装成这块软件进行传播，诱骗下载定位用户位置。
8.伪装对象:**欢乐斗地主**
联机游戏“欢乐斗地主”成为了 Android 手机中的热门应用，但在一些中小软件论坛中却有一些病毒作者以提供这款游戏下载为名传播手机病毒。一旦下载将在后台运行恶意程序，以外发短信、强制开通 SP 服务的方式实施恶意扣费。
9.伪装对象: **超脑医生**
超级医生是一款 Android 手机优化软件，网秦“云安全”数据分析中心发现，二季度有部分渠道提供的魔音软件中存在窃取隐私行为。
10. 伪装对象:**超级电池**
超级电池也是一款深受用户好评的电池优化软件，但据网友反应在部分中小手机论坛下载这款软件后，发现手机出现了遭恶意扣费的现象，后据网秦“云安全”数据分析中心发现，部分渠道的这款软件实际被植入了存在扣费行为的“安卓吸费王”手机病毒。

对此，面对迫在眉睫的严重安全形势，使得用户正亟待安全厂商尽快通过技术革新，应对 Android 安全形势的变换，在基于移动“云安全”技术的基础上，解决 Android 用户面临的安全问题。而相关安全厂商也正在通过不同的传播渠道，为用户提供相应的安全防护建议。

五、安全防护建议

从二季度安全报告的数据可以看出，当前 Android 用户正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

二季度 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，即使通过专业安全工具进行安全性排查。如“网秦手机安全”5.0 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。

及时通过“网秦手机安全”等安全软件检测手机中是否存在恶意软件

同时，用户应密切关心自己的手机资费情况，发现手机话费存在异常时，用户应及时通过拨打运营商客服电话等方式做详细了解，或前往营业厅查询当前手机的 SP 业务开通情况。避免因感染恶意软件造成话费/个人隐私损失。

2.保护 Android 手机隐私安全

二季度以来，隐私窃取类恶意软件呈现持续上升趋势，对此，专家建议用户应选择如“网秦手机安全”Android 版等提供有专项隐私保护模块的手机安全软件。

其中，网秦手机安全 5.0Android 版中新增“隐私安全”保护模块，将可及时检测和发现手机中有陌生程序试图索取包括访问通讯录、访问短信息、访问位置信息、访问身份信息等权限的行为。一旦用户发现存在有异常，用户可及时将其进行停用，避免因感染恶意软且被其索取到核心权限导致的隐私泄漏问题。

3. 确保应用程序的下载安全

安全报告数据显示，手机论坛和应用软件商店正在成为手机病毒和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。

通过“网秦在线监测”平台来快速排查软件安装包的安全性

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。

六、安全技术解析

从数据和走势分析可以看出，面对不断涌现的新兴威胁，亟待安全厂商进行通过技术创新来遏制其衍生，并对技术研发人员提出了更高的要求。而以云端协同处理、实时扣费拦截、隐私权限保护为代表的新技术，正在逐一应用到专业的手机安全软件之中。

1.云端协同处理

“云+端”结合的“云安全”技术模式当前正在被快速应用到专业的手机安全软件之中，并已成为当前和未来在移动安全领域的技术发展趋势。其中，“云端”将重点解决恶意软件的发现问题，从各种渠道收集软件信息，并按照某种算法评估软件的风险，而“终端”重点解决恶意软件的查杀与防护问题，通过安装部署在智能终端上的客户端及时应用的解决方案，对恶意软件进行查杀。

而在当前，包括网秦、卡巴斯基等移动安全厂商推出的产品，也已全线支持“云+端”双引擎技术，通过对新兴恶意威胁的快速响应，协同处理手机中存在的安全问题。

2.实时扣费拦截

实时扣费拦截技术和此前手机安全厂商推出的“扣费扫描”技术不同，“扣费扫描”技术仅以对手机收件、发件箱的短信内容进行扫描，排查信息中是否存在扣费号码，由此判定其是否存在扣费风险。且仅能在触发扣费行为之后做排查。

“实时扣费拦截”技术则能对恶意扣费行为进行主动防护，在其试图通过短信、联网外发扣费信息时便将其做主动拦截。并通过“云安全”平台，实时更新最新的扣费号段组，及时抵御新的恶意扣费病毒。

3.隐私权限保护

目前，存在隐私窃取行为的恶意软件均需要获取相应的操作系统权限，并借此实现通过后台记录用户的隐私信息，并将其通过外发短信或联网进行上传等。由于此前用户对权限管理的意识较为薄弱，往往会忽略其可能索取关键权限的行为。对此，二季度以来，安全厂商已在此技术上进行了升级，并通过相继出台隐私保护模块，可在有恶意软件试图索取权限时及时提示用户。