全球 Android 手机安全报告【2011.Q1】

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 年第一季度全球 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 年第一季度新增 Android 手机病毒 101 个、恶意软件 1014 款，单月平均新增超过 300 款以上，累积 253 万用户被感染。网秦“云安全”数据中心一季度累计处理病毒、恶意软件 2005 万次，其中 45%感染用户使用 Android2.2 操作系统。**

进入 2011 年，Android 手机出货量持续上升，仅 HTC 预计其 Android 手机在 2011 年第一季度的出货量就将达到 850 万部以上。但在用户享受到 Android 手机带来的便捷应用体验同时，一系列 Android 恶意软件的衍生，也正在对全球手机用户的安全构成严重威胁。**2011 年 2 月 Google 下架数十款恶意应用和近期因安全等问题暂时对 Android3.0 进行“闭源”操作，也体现了 Android 安全威胁的严峻性。**

另据权威的市场调研机构 Frost & Sullivan（沙利文）近期发布了《2011 年中国手机安全产品市场白皮书》，报告显示：**截至 2010 年底，Android 应用程序数量已超过 20 万个，累计下载次数达到 25 亿次。**但恶意软件比例也持续增长，**目前在中国市场上，约有 8%的 Android 应用程序存在各种恶意扣费的程序设置.**

网秦报告显示，感染地域方面，全球范围内**中国大陆地区以 64.1%的感染比例成为威胁重灾区**，美国（7.6%）、俄罗斯（6.1%）、印度（3.4%）、印度尼西亚（3.2%）位居其后。国内方面，**广东省以 21.3%的感染比例居首**，江苏（16.4%）、北京（13.8%）、湖北（7.5%）、福建（6.8%）、上海（5.1%）等同样饱受威胁。

Android 操作系统版本分类方面， **Android 2.2 以超过 45%的感染率成为最易被手机病毒、恶意软件攻击的操作系统。**Android 2.1、2.3 以 34%、16%的感染比例位居其后，Android1.6 及以前版本的感染率已降低至 5%以内。这与 Android2.2 市场份额的递增有明显关系。

恶意软件分类方面，**扣费类恶意软件**的增长速度迅猛，以超过 45%的感染比例位居首位。隐私窃取（30%）、后门软件（12%）、资费消耗程序（7%）、流氓软件（5%）位居其后。另有 1%的 Android 恶意软件存在破坏系统运行等特征。

其中，超过 53%的恶意扣费软件会诱骗用户开通 SP 业务，并拦截相关业务确认短信。超过 31%的恶意软件则以频繁联网下载用于恶意推广的软件、大量上传用户隐私而疯狂消耗流量资费，另有 2%的恶意

程序通过外发彩信等方式扣费。

在以窃取隐私为目的恶意软件中，**超过 49%会感染用户手机联网上传用户的隐私内容**，33%的恶意软件在植入用户手机后会通过短信外发隐私内容，另有 13%的恶意软件以远程窃听方式窃取用户通话隐私。另有 5%通过其它方式（如彩信等形式）窃取用户隐私。

恶意软件的传播途径方面，超过 57%的用户通过 Android 应用商店下载感染。17%的用户则因在“刷机”时不慎安装了被植入扣费软件的**“刷机包”**后感染，另有 14%的用户通过 WAP/WWW 网站下载软件时感染，7%的用户通过蓝牙传输方式感染，3%的用户通过存储卡途径感染，2%的用户通过其它途径感染。

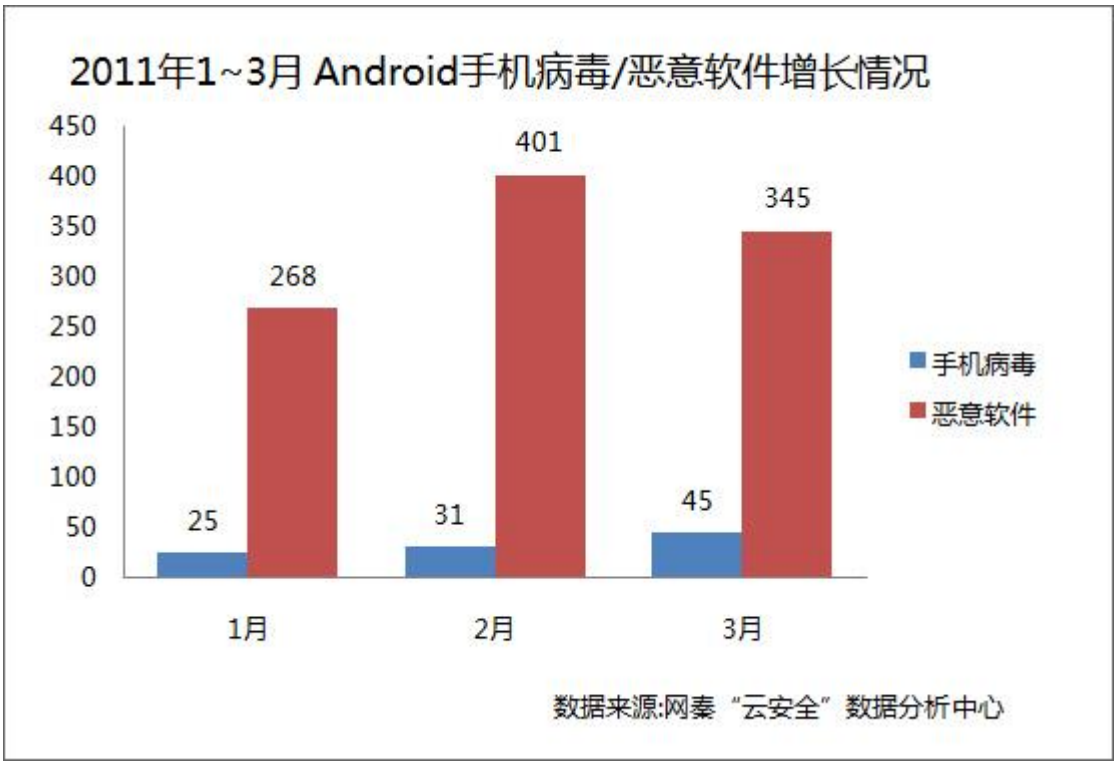
通过数据可以看出，当前 **Android 平台的安全形势正在持续恶化**，由于 Android 手机用户的安全意识还相对较为单薄，缺乏如权限保护、流量管理等方面的知识，导致极易感染各类手机病毒及恶意软件。此外，包括 Android 应用商店、WAP/WWW 下载站对其提供的资源也缺乏安全验证，且 Android 应用存在可被批量植入恶意代码的隐患，导致手机用户正笼罩在恶意软件的阴影之下。

对此，报告指出，迫在眉睫的严重安全形势，已令用户亟待安全厂商尽快拿出专业的解决方案，而在目前，“云安全”技术的实施力度、研发技术的创新，都将决定安全形势的走向。

二、平台安全趋势

1.走势:单月新增恶意软件 300 款以上

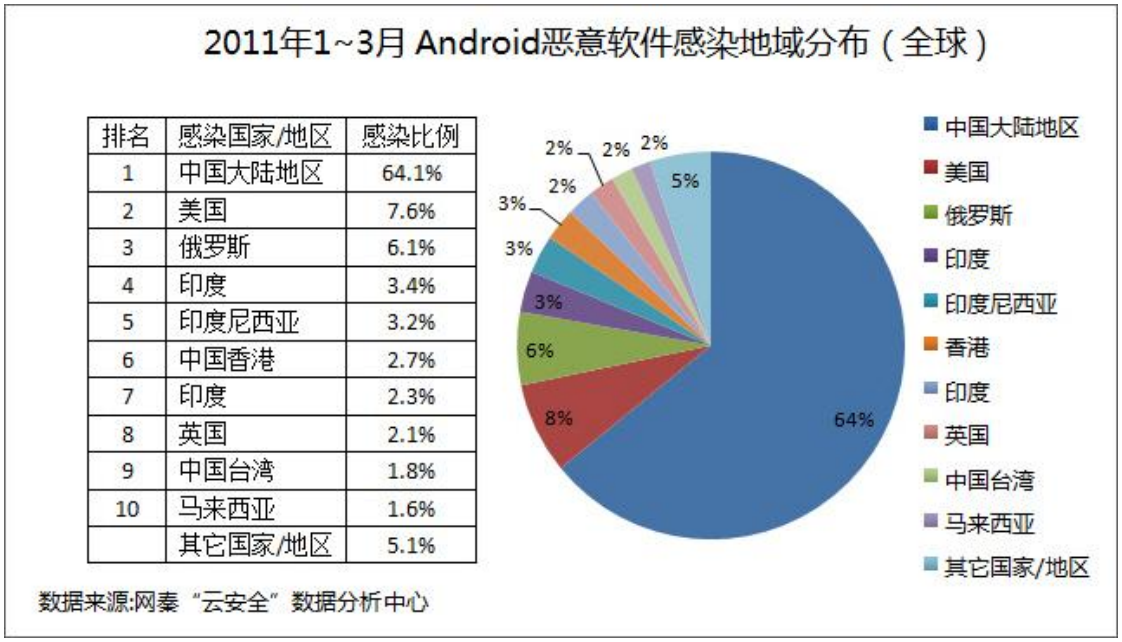
威胁走势方面，据网秦“云安全”数据分析中心的数据统计，2011 年 1 至 3 月累计发现 Android 手机病毒 101 个，恶意软件 1014 款，其中 1 月发现病毒 25 个、恶意软件 268 款，2 月发现病毒 31 个、恶意软件 401 款，3 月发现病毒 45 个、恶意软件 345 款，平均单月新增恶意软件以及变种 300 款以上，数据相对波动不大。



2011 年 1~3 月 Android 手机病毒/恶意软件增长状况

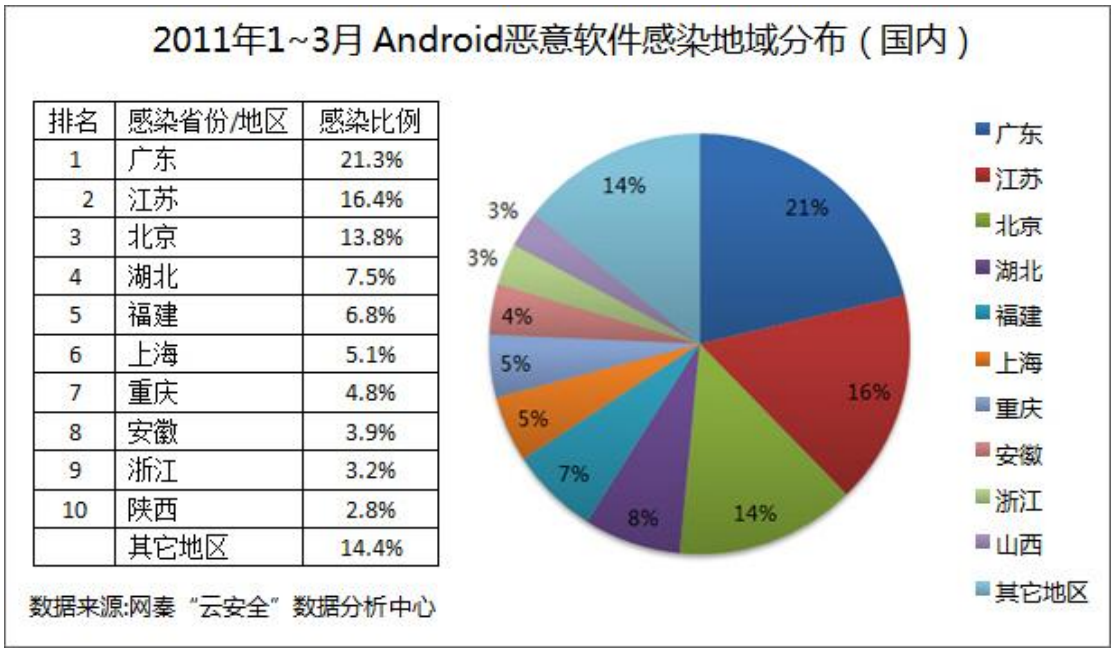
2.地域:中国大陆成重灾区 广东省居首

地域分布情况，2011 年第一季度，中国大陆地区以超过 64.1%的感染量成为重灾区，美国（7.6%）、俄罗斯（6.1%）、印度（3.4%）、印度尼西亚（3.2%）位居其后。国内广东省以 21.3%的感染比例居首，江苏（16.4%）、北京（13.8%）、湖北（7.5%）、福建（6.8%）、上海（5.1%）等地位居其后。



排名	感染国家/地区	感染比例
1	中国大陆地区	64.1%
2	美国	7.6%
3	俄罗斯	6.1%
4	印度	3.4%
5	印度尼西亚	3.2%
6	中国香港	2.7%
7	印度	2.3%
8	英国	2.1%
9	中国台湾	1.8%
10	马来西亚	1.6%
	其它国家/地区	5.1%

2011 年 1~3 月 中国大陆地区以 64.1%的比例排名第一

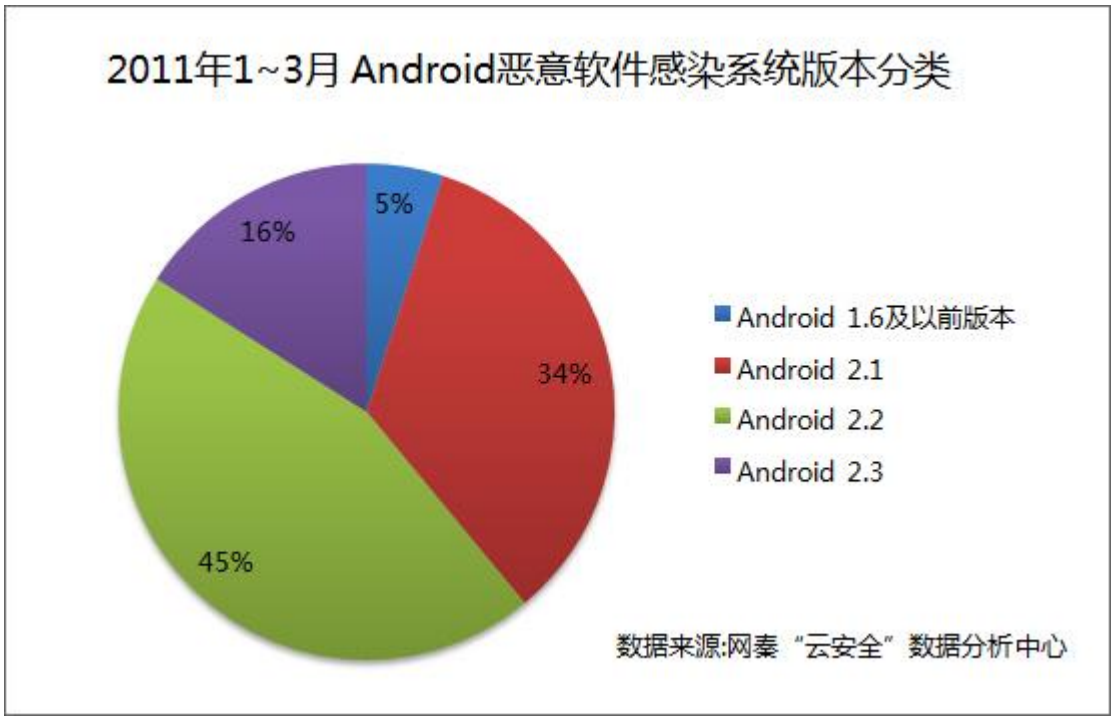


排名	感染省份/地区	感染比例
1	广东	21.3%
2	江苏	16.4%
3	北京	13.8%
4	湖北	7.5%
5	福建	6.8%
6	上海	5.1%
7	重庆	4.8%
8	安徽	3.9%
9	浙江	3.2%
10	陕西	2.8%
	其它地区	14.4%

2011 年 1~3 月 广东省以 21.3%的感染比例位居首位

3.版本:Android2.2 成主要感染对象

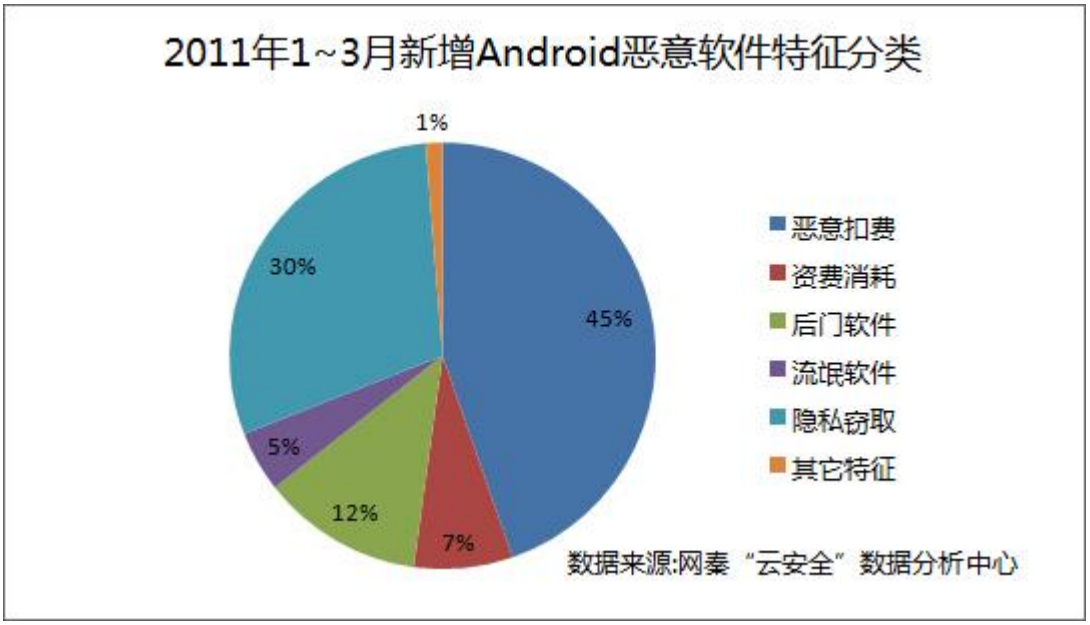
Android 操作系统版本分类方面， **Android 2.2 以超过 45%的感染率成为最易被手机病毒、恶意软件攻击的操作系统。**Android 2.1、2.3 以 34%、16%的感染比例位居其后，Android1.6 及以前版本的感染率已降低至 5%以内。这与 Android2.2 市场份额的递增有明显关系。



2011 年 1~3 月 Android 恶意软件感染系统版本分类

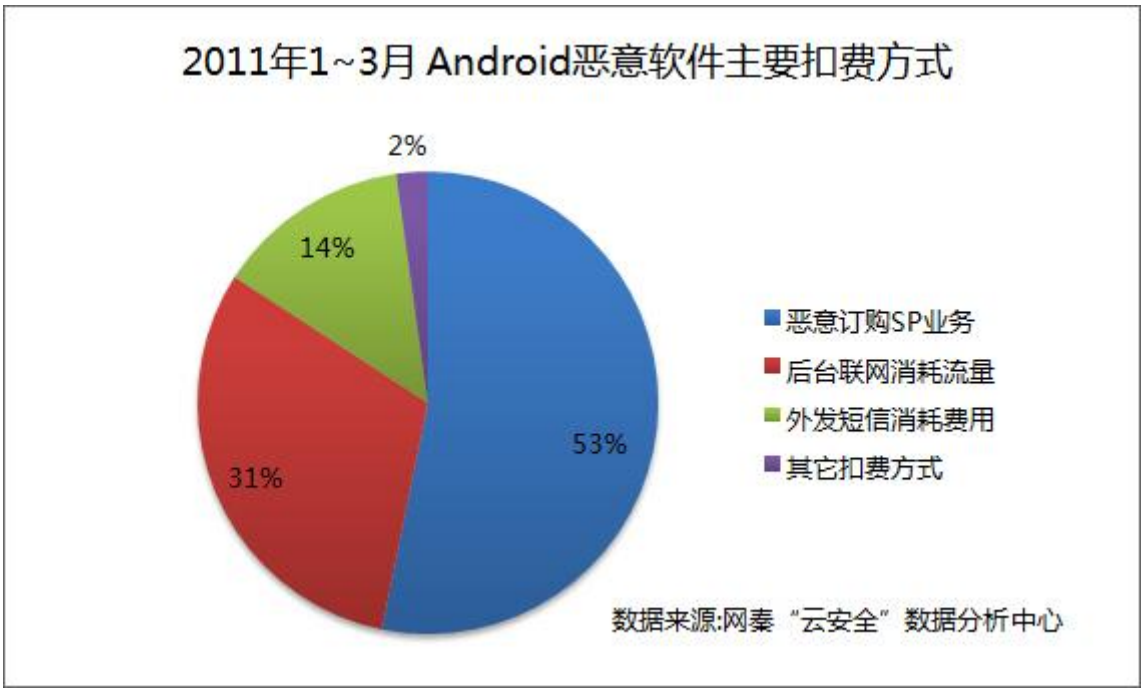
4.类型:45%恶意软件存在扣费行为

恶意软件类型方面，其中**扣费类恶意软件**的增长速度迅猛，以超过 45%的感染比例位居首位。隐私窃取（30%）、后门软件（12%）、资费消耗程序（7%）、流氓软件（5%）位居其后。另有 1%的 Android 恶意软件存在破坏系统运行等特征。



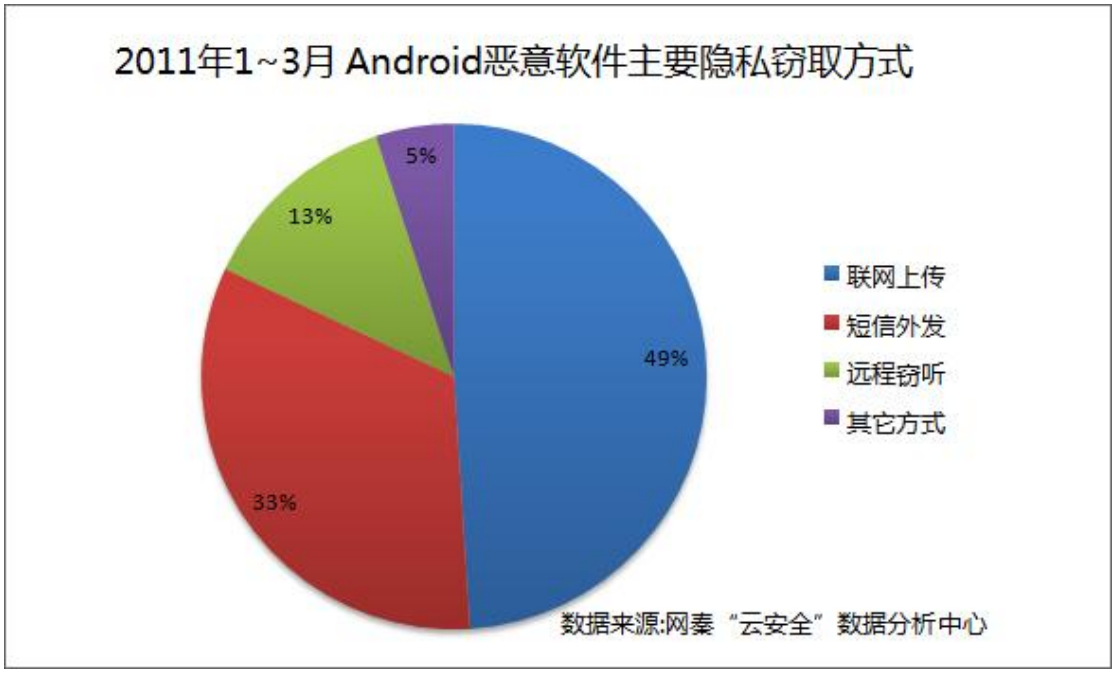
2011 年 1~3 月新增 Android 恶意软件特征分类

其中，超过 53%的恶意扣费软件会诱骗用户开通 SP 业务，并拦截相关业务确认短信。超过 31%的恶意软件则以频繁联网下载用于恶意推广的软件、大量上传用户隐私而疯狂消耗流量资费，另有 2%的恶意程序通过外发彩信等方式扣费。



2011 年第一季度 Android 恶意软件主要扣费方式

同时，在比例高达 30%的**隐私窃取类**恶意软件中，有超过 49%会感染用户手机联网上传用户的隐私内容，33%的恶意软件在植入用户手机后会通过短信外发隐私内容，另有 13%的恶意软件以远程窃听方式窃取用户通话隐私。另有 5%通过其它方式（如彩信等形式）窃取用户隐私。



2011 年第一季度 Android 恶意软件主要隐私窃取方式

5.途径:应用商店/“刷机包”成传播温床

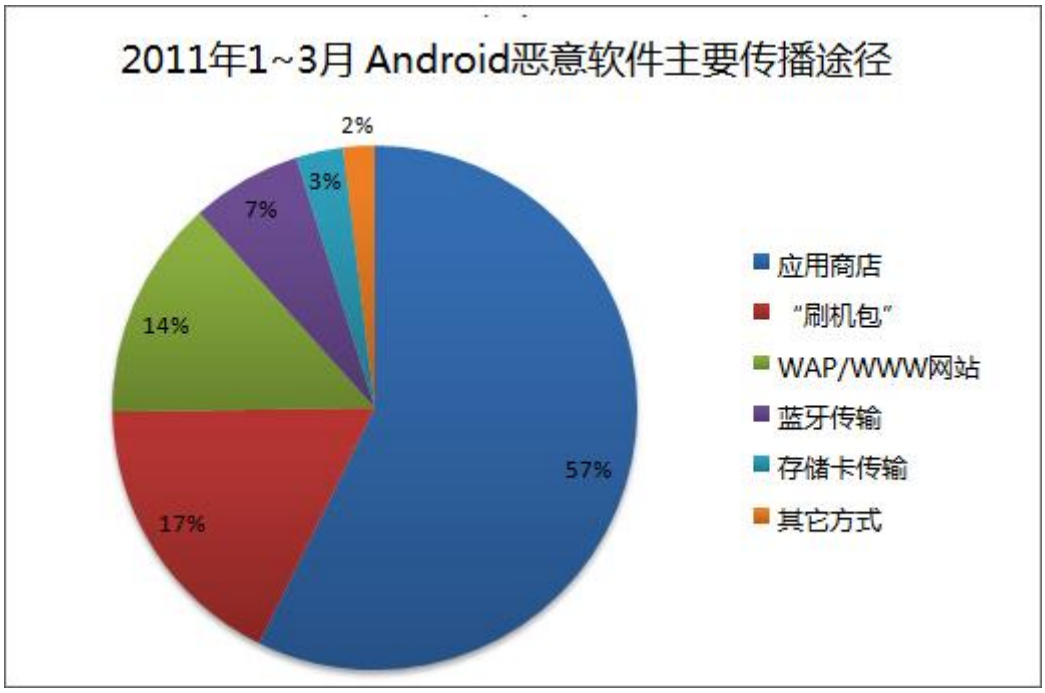
感染途径方面，据网秦“云安全”数据分析中心统计，**Android 应用商店成为手机病毒、恶意软件的**

主要传播途径，超过 57%的用户因此“中招”。17%的用户则因在“刷机”时不慎安装了被植入扣费软件的**“刷机包”**后感染，另有 14%的用户通过 WAP/WWW 网站下载软件时感染，7%的用户通过蓝牙传输方式感染，3%的用户通过存储卡途径感染，2%的用户通过其它途径感染。

小贴士：何为“刷机”？何为“刷机包”？

“刷机”就是更新、升级手机操作系统。可以突破手机本来的限制，个性化自己的手机，可以 DIY 个性化手机，更改、替换机内的各图片、铃声、开关机画面及菜单字符等等。

“刷机包”则指将相应设定进行打包便于用户一次性安装的程序集，作者可将其打包到系统 ROM 镜像中，上传到相关论坛，网友直接下载批量安装后享受到全套应用服务。尽管相当方便，但因部分病毒作者会在“刷机包”中植入恶意扣费代码，故用户在下载安装后极易感染恶意软件。



超过 57%的 Android 恶意软件通过应用商店感染手机用户

三、安全隐患解读

进入 2011 年，Android 手机平台的安全性备受用户关注，据权威的市场调研机构 Frost & Sullivan（沙利文）近期发布了《2011 年中国手机安全产品市场白皮书》，报告显示：截至 2010 年底，Android 应用程序数量已超过 20 万次，累计下载次数达到 25 亿个。但恶意软件比例也持续增长，目前在中国市场上，约有 8%的 Android 应用程序存在各种恶意扣费的程序设置，“恶意扣费”行为一般在用户下载安装相应的应用软件过程中“自动”产生，用户很难觉察。

同时，Android 手机存在的 ROOT 权限隐患、联网流量隐患和 Android 应用商店普遍存在的应用上传时的审核机制隐患以及 Android 应用存在的易被批量植入恶意代码的隐患等，也正在严重威胁 Android 用户的安全。

1. **ROOT 权限被轻易获取**

众所周知，Android 操作系统底层为 Linux 内核，ROOT 是 Linux 超级管理员用户，具有最大的权限。在 Android 的安全设计中，默认情况下用户不具有 ROOT 权限。

但是，近年来， Android 系统出现了多个可让用户获取 ROOT 权限的途径，例如：

1）默认情况下，系统不具有 ROOT 权限，而导致很多操作无法进行（如备份系统），用户为使用更方便，主动利用漏洞或者第三方提供的软件获取 ROOT 权限；

2）用户使用其他人自制的 ROM 刷机，而该 ROM 在制作时已经获取了 ROOT 权限，从而用户在不知情情况下具有了 ROOT 权限；

3）用户安装了某个恶意程序，该程序为了达到某种恶意目的，在用户不知情情况下获取了 ROOT 权限。

一旦获取了 ROOT 权限，不但可以做到应用程序的静默安装，还可以访问其他应用程序以及随意读写用户隐私数据，修改或删除非其他应用程序的文件等等，对用户的 Android 手机造成的安全隐患。

2.联网管理意识淡薄

随着移动互联网的发展，越来越多的应用需要频繁使用网络，如天气资讯与 IM 类软件；同时应用开发者在产品(尤其是免费产品)中植入了广告插件（如 AdMob），而广告插件需要联网更新广告内容。这些导致用户在手机使用过程中流量大增，按照国内以流量为计费单位的方式，很容易让用户产生高额的流量费用。

但在 Android 手机系统中默认并不具备流量管理功能，且多数手机用户尚未养成实时管理上网流量的意识，用户很难察觉到是否超支或是否有恶意软件在恶意联网消耗流量。使得黑客有了在用户毫不知情的状态下，肆意上传隐私和实施扣费的机会。

3.应用发布前缺乏安全审核

作为用户下载 Android 应用的主要渠道，当前应用商店却正在成为恶意软件的传播温床。网秦《2011 年第一季度全球 Android 手机安全报告》显示，超过 57%的用户正在通过应用商店下载。伴随谷歌批量剔除数十款恶意软件等事件的发生，和国内多家 Android 商店爆出发现恶意软件的消息，应用商店安全性已愈发引起关注。

实际上，造成 Android 恶意软件肆意传播的原因在于当前应用商店存在的审核隐患。其中以 Google Market 为例，如果用户要在 Google Market 发布应用，用户首先需要注册，然后支付一定的费用后才能发布应用，如果要发布付费应用，还需要提供一个银行帐号，Google 需要认证。这已经很大程度上规避了用户虚假身份信息。一旦出现法律问题，Google 可以追究其法律责任。

但是 Google 在应用上架时，没有二次认证的审核流程，开发者上传后的 APP 会立刻发布，如果开发者发布了恶意应用，虽然被发现后会被下架，事后也可能会被追究法律责任，但是对在发布后和下架前的

时间段内下载该软件的用户，已经造成了损失。由于开发者能够通过服务器控制客户端恶意行为的发作时间，在应用通过审核上架后再来激活恶意行为，即使通过审核也难以完全确保程序安全性。

4.批量植入恶意代码

与塞班平台不同，当前 Android 平台的恶意软件数量正在呈几何级增长，其中，部分插件在被发现时已累积植入到数十、乃至数百款普通应用软件之中。例如“安卓吸费王”病毒自 2011 年初被发现以后，累积植入到包括手机 QQ、塔防等超过数百款 Android 应用软件之中。

究其原因，由于 Android 应用开发主要使用 Java 语言，Java 语言本身反编译较为容易，恶意程序开发者可以反编译获取应用源码，继而修改原代码并植入恶意插件程序代码，最后再重新编译生成新应用程序包，采用该方式生成的新应用仍然保留了原应用的正常功能，从而具有较高的欺骗性。该方法可以批量进行，使得恶意软件（尤其是变种）的数目剧增。

同时，由于 Android 平台和塞班平台不同，缺乏全面的测试及数字签名验证机制，导致其批量植入恶意代码的成本被进一步降低，从而导致了如“安卓吸费王”等恶意程序的大面积泛滥。

对此，由于 Android 平台存在批量植入恶意代码的隐患，导致在渠道操控中一旦存在安全问题，用户下载应用时极易遭到感染，若未安装专业手机安全软件，将面临极大的安全风险。

四、技术发展趋势

面对错综复杂的 Android 安全形势，也正在对安全厂商的技术研发提出新的课题。其中，为积极应对 Android 面临的安全问题，在众多的应用中第一时间发现恶意程序并且及时响应，“云+端”结合的“云安全”技术模式正在被应用到专业的手机安全软件之中，也将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，对其风险排序，从而第一时间发现高风险软件中的恶意软件，并形成解决方案。云可以将解决方案发放给端提供服务，也可以直接提供服务。

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，并防止恶意软件进入。同时，端也可以作为云的一个重要输入，在用户许可前提下，向其反馈必要的软件信息。

对此，通过“云安全”技术的系统融合，将从包括渠道、终端等多个层面，实现对恶意软件的全面排查。目前，作为拥有全球最大的移动“云安全”数据库的专业移动安全厂商，网秦公司正在为全球超过 7100 万手机用户提供安全保护，并已在 2010 年底对外开放了“云安全”平台的 APK 接口，并已与中国移动、中国电信等多家电信运营商和多家 Android 应用商店达成了合作意向，可实现对其线上资源的全面、实时的安全检测，避免用户下载时遭遇恶意软件威胁。