移动安全专家
NetQin 网秦

# 2011年中国大陆地区手机安全报告

# 网秦《2011 年中国大陆地区手机安全报告》

## 目录



本报告讨论范畴为移动互联网恶意代码和移动互联网恶意代码样本，移动互联网恶意代码（俗称:手机病毒）是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、代码模块或代码片段。移动互联网恶意代码样本是指存放移动互联网恶意代码的文件实体形态，通常以软件形式存在，又称为移动互联网恶意软件（以下简称：恶意软件），其MD5值各不相同，故通过感染款数计量。

## 一、安全报告摘要

《2011 年中国大陆地区手机安全报告》（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。报告指出，2011 年网秦“云安全”监测平台**全年新增手机病毒 2943 个，查杀到手机恶意软件 24794 款，同比增长 266%，中国大陆地区 2011 全年累计感染智能手机 1152 万部，同比增长 44%。**

平台方面，**Symbian 平台依然是手机恶意软件的重点感染对象，平台比例仍在 60%以上， Android 平台则以 38%的感染比例位居其后**，但保持高速增长势头，并**自 2011 年 10 月开始单月查杀次数已超过 Symbian**。2011 年 1 月查杀达到 1851 款恶意软件，创历史新高。

在全球范围内，**中国大陆地区以 31.6%位居首位。国内广东省以超过 22.1%的感染比例位居全国之首。**北京（19.3%）、上海（16.5%）、河南（13.3%）、江苏（9.6%）、天津（6.3%）、福建（5.2%）等省份位居其后。 其中天津、福建两地的增长速度较快。

恶意软件特征方面，在 2011 年截获的 24794 款手机恶意软件中，**“远程控制木马”以 27.3%的感染比例位居首位，**恶意扣费、隐私窃取、资费消耗类、系统破坏类则以 25.5%、16.3%、11.2%、8.4%的比例位居其后。

传播途径方面，数据显示，**手机论坛依然是 2011 年恶意软件的主要传播途径，所占比例超过 24%，**手机应用商店、WWW/WAP 网站和 ROM“刷机包”则以 20.3%、17.3%、13.2%的感染比例位居其后。而在**非 Google 官方的手机应用商店中，恶意软件比例已从 2011 年 6 月的不足 0.8%上升至 2.2%**，部分国内中小应用商店的恶意软件比例更达到 10~15%。

同时，本次报告在发布 2011 年中国大陆地区手机安全数据和对各项数值的增长比例进行解析之外，还同期公布了 2011 年的十大手机病毒，其中 Android 平台的**“安卓吸费王”以累计植入超过 700 款手机应用，和累计感染 200 万人次的数据成为 2011 年影响、危害最大的手机恶意软件**，安卓窃听猫、跟踪隐形人等 2011 年的热门恶意软件位列其中。

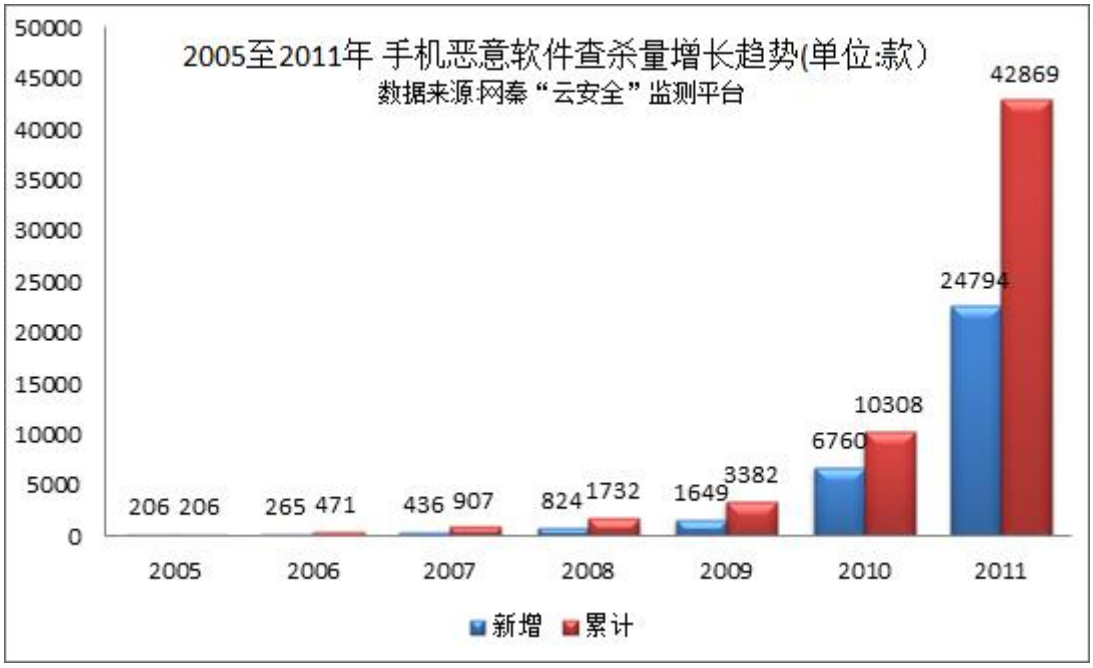
而在被手机病毒植入次数最多的手机应用软件排行中，QQ 斗地主、手机加速器、深度睡眠、五子棋、超级电池等热门 APP 均榜上有名，受其感染量基数、频次影响，**QQ 斗地主更成为 2011 全球被伪装次数最多的手机应用。**

此外，报告还对 2011 年的安全特点进行了深入分析，如对**造成恶意软件大肆泛滥的原因 – 批量伪装技术的应用、ROOT 权限被滥用的现象以及渠道安全管理的淡薄**进行了解读。并对 2012 年的手机安全行业发展趋势进行了预测，包括未来的技术发展、产品创新和渠道合作模式等。

## 二、平台安全数据

### 1.安全趋势:全年查杀恶意软件 24794 款 同比增长 266%

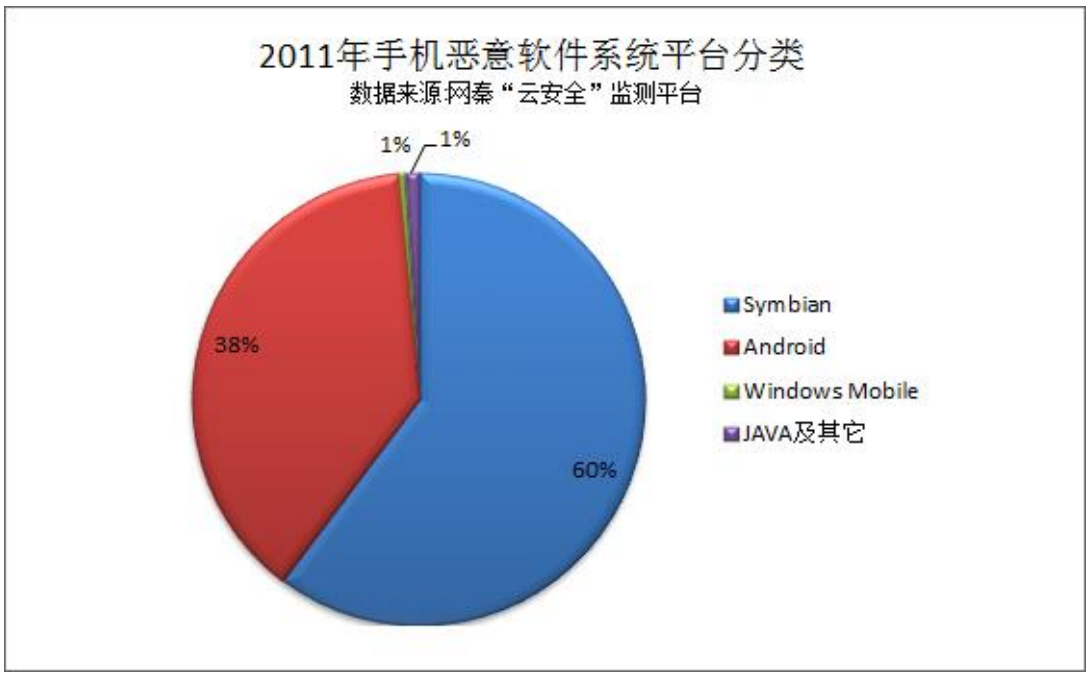
数据显示：截至 2011 年 12 月，网秦“云安全”监测平台新增手机病毒 2943 个，同比增长 14.4%，全年查杀到手机**恶意软件 24794 款，同比增长 266%**，2005 年至今累计查杀 42869 款，**中国大陆地区 2011 全年累计感染智能手机 1152 万部**，全球范围内，累计感染智能手机 3711 万部（以感染次数统计，未去重）。




2005 至 2011 手机恶意软件增长趋势（数据:网秦“云安全”监测平台）

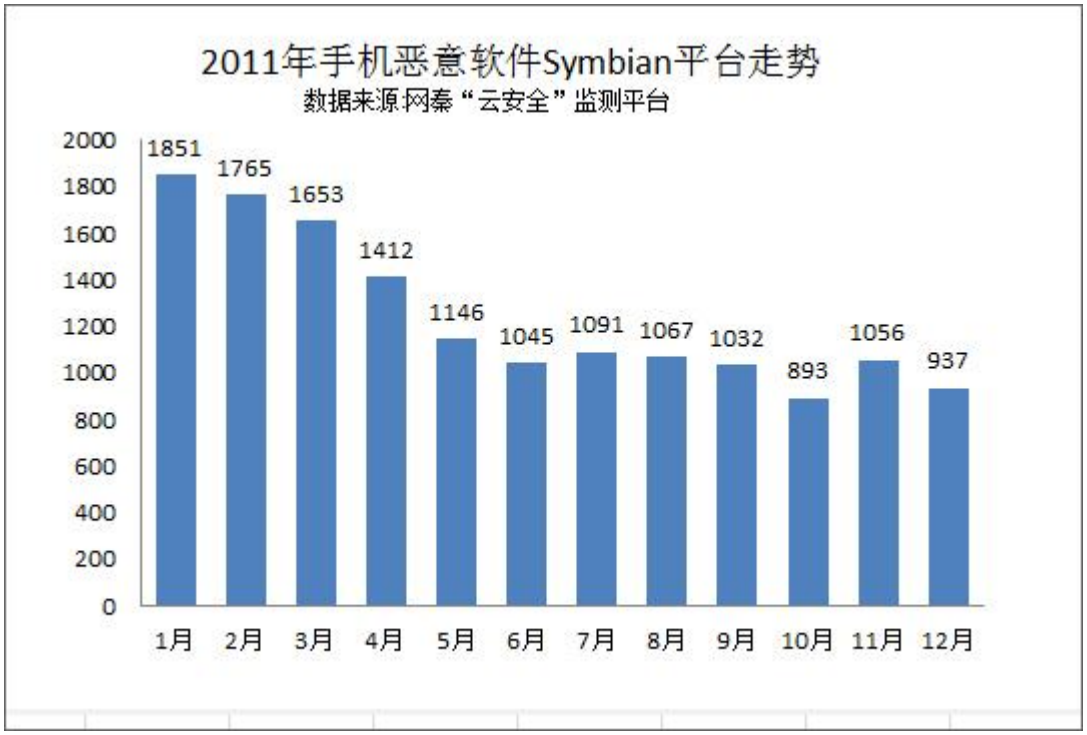
### 2.平台走势:Android 恶意软件全年涨幅超过 1880%

平台方面，截至 2010 年 11 月，**Symbian 平台依然是手机恶意软件的重点感染对象，平台比例仍在 60%以上，** Android 平台则以 38%的感染比例位居其后，但相比 2010 年 Android 不足 10%的感染比例，其在这一年中的增长速度极快。




2011 手机恶意软件系统平台分类（数据:网秦“云安全”监测平台）

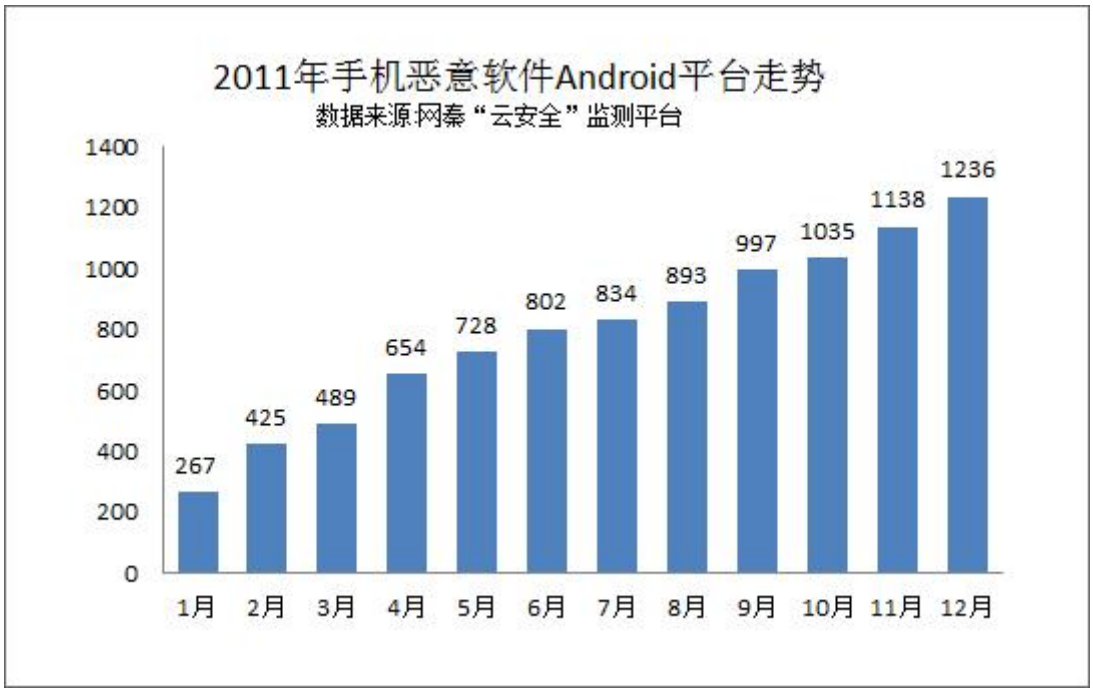
而通过单独的平台走势分析可以看出，尽管截至 2011 年底，Symbian 手机平台依然是恶意软件的感染重灾区，**2011 年 1 月单月查杀到 1851 款恶意软件，达到历史新高**，但从其单月走势来看已整体呈现下降趋势，如 10 月之后的单月查杀数量已逐渐少于千款。



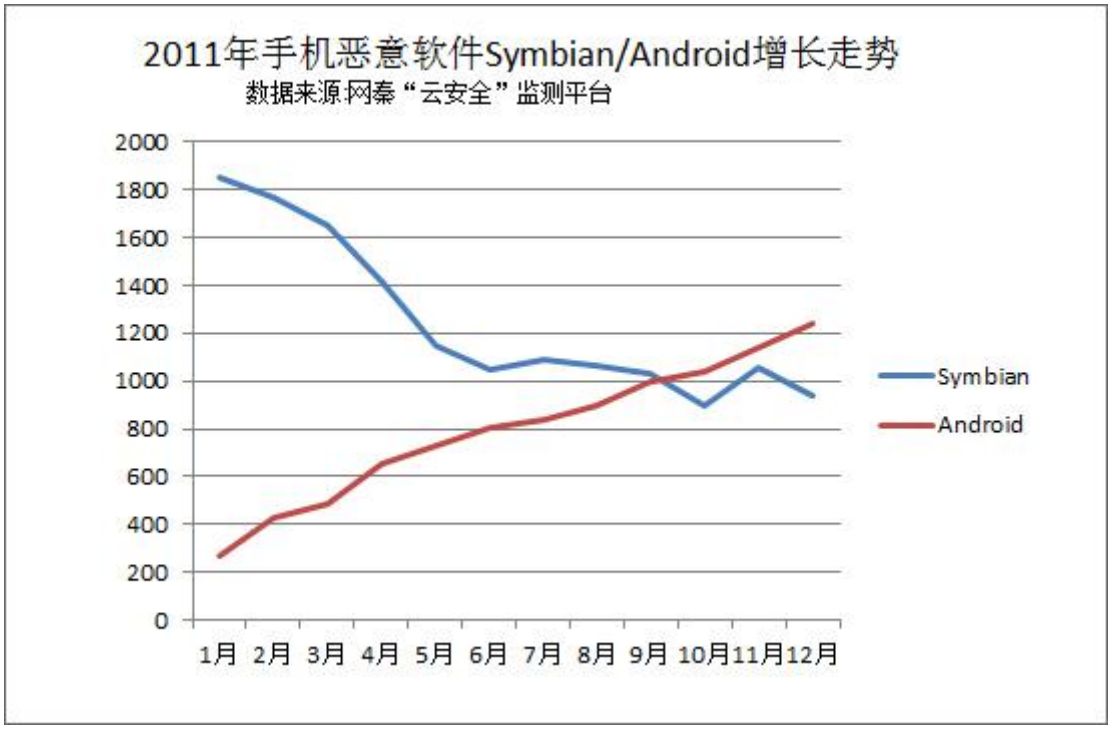

2011 年 Symbian 平台手机恶意软件增长趋势（数据:网秦“云安全”监测平台）

相比之下，**Android 平台则正在以同比超过 1880%的涨幅快速增长**，并在 2011 年 12 月以单月查杀 1236 款的数据达到历史新高，**且自 10 月以来开始超过 Symbian**。数据两极化现象的出现，恰好与智能手机在

2011 年的平台换代节奏相吻合，也充分表明了当前手机黑客正在将开发重点向 Android 等新兴平台转移。




2011 年 Android 平台手机恶意软件增长趋势（数据:网秦“云安全”监测平台）

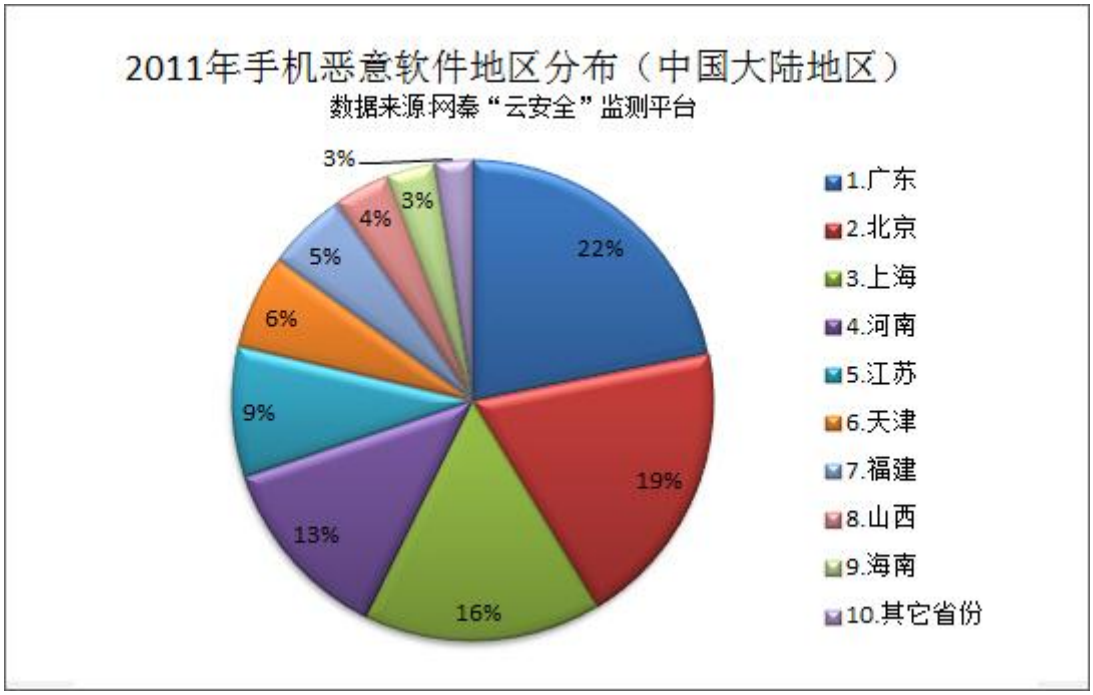



Android 恶意软件款数在 10 月超过 Symbian（数据:网秦“云安全”监测平台）

**3.地域分布:广东以 22.1%的感染比例位居首位**

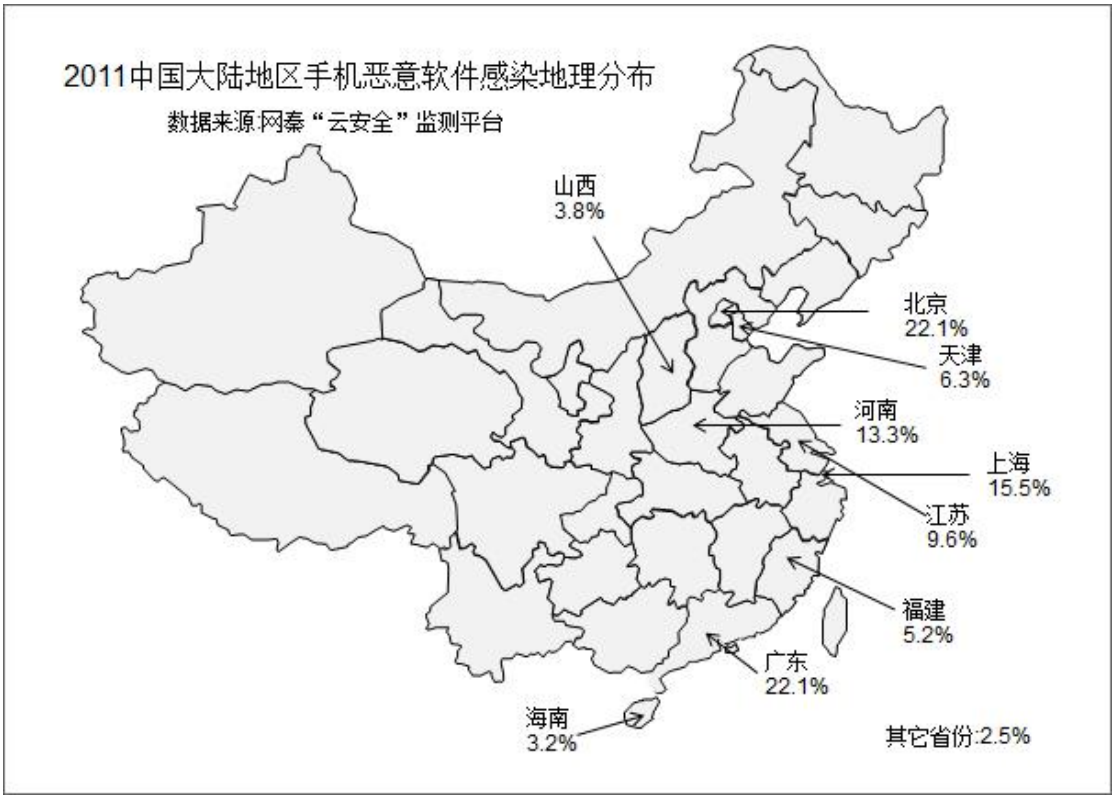
地域分布方面，据网秦“云安全”监测平台数据显示，在全球范围内，**中国大陆地区以 31.6%位居首位。国内广东省以超过 22.1%的感染比例位居全国之首，**成为手机恶意软件感染重灾区，其在 2010 年也同样以 21.6%的感染比例位居全国之首。

而北京（19.3%）、上海（15.5%）、河南（13.3%）、江苏（9.6%）、天津（6.3%）、福建（5.2%）等省份位居其后。 其中天津、福建两地的增长速度较快。




2011 年手机恶意软件感染量地区分布图（数据:网秦“云安全”监测平台）

而根据地理分布可看出，**沿海地区为目前恶意软件的集中扩散区域**，这与智能手机在相关地区的普及率相关，但伴随 2012 年，运营商的一系列低价策略，和“千元智能机”的陆续上市，中西部地区用户的手机安全也将面临挑战。



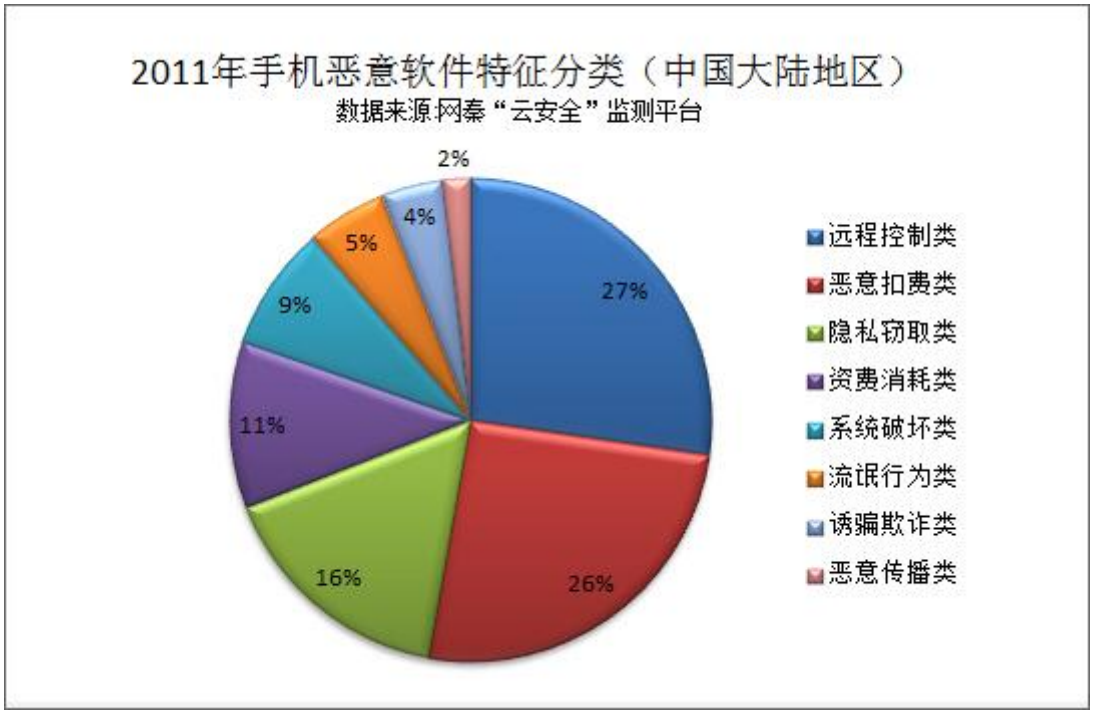

2011 年手机恶意软件感染量地理分布图（数据:网秦“云安全”监测平台）

**4.感染类型:近三成恶意软件为“远程控制木马”**

相比 2010 年，2011 年的手机恶意软件感染类型已覆盖到多个层面，威胁方式也出现了较大的变化，在恶意扣费和隐私窃取类恶意软件依然肆虐的情况下，“远程控制木马”等新特征分类的出现，和传播范围的愈发广泛，对用户的手机安全构成了极大的威胁。

据网秦“云安全”监测平台统计：在 2011 年截获的 24794 款手机恶意软件中，**“远程控制木马”以 27.3%的感染比例位居首位。同比 2010 年初涨幅高达 89%，全年累计感染手机 291 万部，成为 2011 年度智能手机的第一安全威胁。**

而恶意扣费、隐私窃取、资费消耗类、系统破坏类则以 25.5%、16.3%、11.2%、8.4%的比例位居其后，其后则为流氓软件（5.3%）、诱骗欺诈（4.1%）、恶意传播类（1.9%）恶意软件。（注：部分恶意软件同时会存在多个破坏行为，故以实际的破坏行为作为统计基准，未去重）。

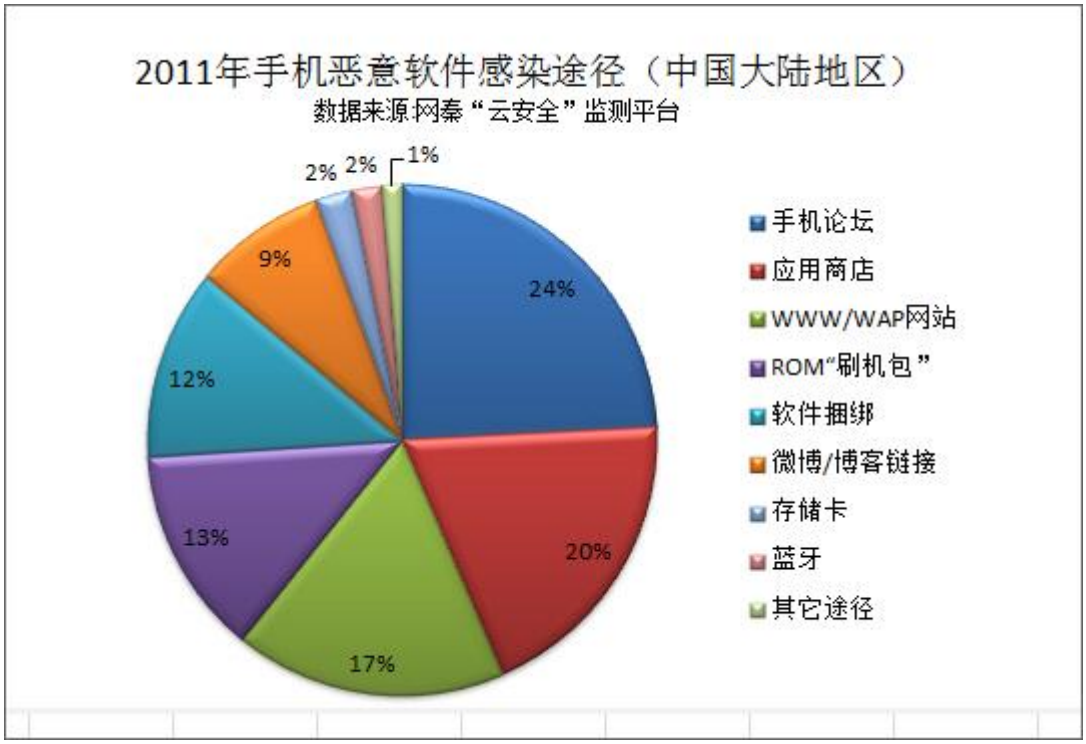



2011 年中国大陆地区手机恶意软件特征分类（数据:网秦“云安全”监测平台）

**5.感染途径:手机论坛成为恶意软件重灾区**

相比 2010 年，手机恶意软件的传播方式发生了很大的改变，伴随 Android 手机用户的极速增长，与其相配的官方、第三方软件商店层出不穷，并出现了大量分享 APP 应用和交流、讨论的手机论坛，而在 Android 平台下，ROM 刷机包也愈发火热。但就在用户借此可享受到更为便捷的应用服务同时，在其中“潜伏”的安全威胁也不断出现。

数据显示，2011 在中国大陆地区，手机论坛成为了恶意软件的最大传播途径，数据显示，**有 24.2%的手机恶意软件主要通过手机论坛传播**。而手机应用商店则以 20.3%的比例位居其后，WWW/WAP 网站和 ROM“刷机包”也以 17.3%和 13.2%的比例紧随其后。




2011 年中国大陆地区手机恶意软件主要感染途径（数据:网秦“云安全”监测平台）

而在应用商店中，目前谷歌官方应用商店（Google Android market）、运营商自营应用商店（如移动 MM 商城、天翼空间等）、手机终端厂商自营应用商店（如 OVI 商店、HTC 应用商店等）和第三方中小应用商店（如安卓网、91 助手等）的安全等级也各不相同。**如据统计数据显示，Android 官方商店的恶意软件比例为 0.04%，而中小应用商店的整体恶意软件比例达到 2.2%以上**，部分国内中小应用商店在特定月份的监测数据中，恶意软件比例更超过 10~15%。

## 三、安全形势解析

### 1.恶意软件增长趋势解析

相比 2010 年，2011 年的手机安全形势持续恶化，这主要源于智能手机的高速发展，根据市场调查公司 Strategy Analytics 的数据，2011 年第三季度，中国以 2400 万台的出货量，打败同期的美国(2300 万台)，成为全球最大智能手机市场。

但在智能手机在中国大陆地区快速普及的同时，移动安全问题也日益凸显。如据报告数据可以看出，**2011 年全年累计截获的手机病毒个数和恶意软件款数均超过去 6 年总和**。以“安卓吸费王”等为代表的恶意扣费软件所具备的伪装应用极多的特征，也是恶意软件款数在 2011 年持续激增的原因。**如“安卓吸费王”截至 2011 年 12 月的伪装对象已超过 700 款。**

### 2.恶意软件平台走势解析

平台走势方面，Android 平台的恶意软件上升比例最为明显，作为 2011 年移动互联网产业的主角 – Android 在这一年发挥了至关重要的作用。如据资策会产业情报研究所(MIC)6 月预测数据显示 Android 平

台 2011 年出货量将达 2.06 亿台，而中国大陆地区的一系列电信政策和“千元智能机”的热销，更将进一步促进其快速发展。

然而，正由于 Android 系统支持更多更为智能化的应用，导致其在提供便利服务的同时实际增加了感染恶意软件的风险，由于国内仍有大量手机论坛、应用商店缺乏安全监管，以及 Android 恶意软件具备同时伪装多款应用进行传播的特征，更使得其更易直接威胁到用户的手机安全。

**3.恶意软件地域分布解读**

相比 2010 年的安全形势，尽管在数量、平台等方面都出现了较大差异，但在感染地域的整体变化并不明显，受智能手机普及率的影响，一线城市的感染比例依然靠前，如以广东省为例，作为国内较大的“水货”手机集散市场，也成为了恶意软件重点入侵的地域。**上海市同比 2010 年的增长比例高达 87%，成为增长速度最快的地区。**

以网秦目前掌握的 ROM 程序样本量和通过分析得出的数据抽样对比显示，目前广东地区充斥的大量“水货手机”中，存在大量在 ROM“刷机包”中植入扣费病毒的现象，**恶意软件比例高达 7%。**

如“远程控制木马”（a.rogue.PushBot.a）经检测便存在于超过 20 余个“水货”手机的 ROM 程序包中，以其每日数以千计的出货量计算，用户安全将面临严重威胁。由于恶意软件作者为躲避查杀和相关渠道对其进行的监管，又不断更换传播渠道，且不同地区的用户又存在有不同的下载习惯，导致其感染比例会根据时段略有变化。

**4.恶意软件感染类型分析**

感染类型方面，“远程控制木马”的肆虐和恶意扣费类软件的坚挺是其主要表现。作为 2011 年新近出现的恶意软件特征，与传统恶意软件固定的、静态的威胁特征不同，“远程控制木马”的威胁则是动态的、可变的。

例如，“远程控制木马”在感染用户的智能手机后，会强行连接到对应的网络服务器中，并等待其派发的指令来实施进一步的威胁，如可操作其联网上传用户隐私、盗取用户地理位置、通过派发恶意指令触发扣费行为等。

与传统意义上的手机病毒和恶意软件不同，这类应用的特点是通过同一套程序实施不同的危害，**其由于通过同一“后门”可派发不同的威胁指令，在用户毫不知情的状态下运行，直接造成多种危害。**

而在其他感染比例中，恶意扣费软件的持续坚挺则来源于以“安卓吸费王”为代表的恶意软件激增，由于其平均单月感染手机 50 万部以上，按照平均单次扣费 5 元的比例计算，黑客单月可直接获利 250 万元以上，受此经济利益驱动，导致扣费软件仍然是黑客开发的重点之一。

但相比之下，尽管隐私窃取软件也曾被媒体多次曝光，在汇总全年数据可看出，其比例实际略有下降，这主要来源于媒体的多次曝光和国家相关机构的坚决治理，目前包括“X 卧底”、“窃听猫”等恶意软件都得到了系统整治，安全形势略有好转。

**5.恶意软件感染途径解读**

感染途径方面，**应用商店和手机论坛则始终位居最前两位**，并在 2011 年上、下半年存在较大差异。上半年时，由于国内仍有大量应用商店缺乏安全验证，导致其成为了黑客利用传播恶意软件的主要通道。而下半年开始，伴随应用下载渠道对安全性的关注，且逐渐在提升安全等级，其安全性已有所提升。

而手机论坛则由于网站较多，内容参差不齐，也多以个人分享为主，更易被黑客利用，以诱人词汇作为论坛贴标题来肆意传播，包括利用部分用户不愿付费购买 APP 的心理，以破解版、修正版来诱骗下载等等，实际借此传播被打入恶意代码的应用。


数据显示手机论坛依然是恶意软件的主要传播途径（图片来自于网络）

而位居三、四名的 WWW/WAP 下载站和 ROM“刷机包”尽管曾在 2011 年上半年一度超越论坛。这两大传播渠道由于受众面较广，且缺乏完善的安全验证、应用审核机制，导致极易沦为黑客传播恶意软件的主要平台。

WWW/WAP 下载站的安全形势严峻，主要是由于大量传统 PC 软件下载站也相继推出了手机软件频道，以及在传统 WAP 网站中开放的手机软件专区，但其中因审核不严导致出现了恶意软件，而 ROM“刷机包”成为恶意软件主要传播途径，主要由于其背后存在着相当大的经济利益驱动，如在当前手机水货市场仍普遍存在恶意软件作者与“水货”手机供货商敲定合作机制，以较高价格诱惑其将恶意软件装入 ROM 之中的现象，大量用户因此感染恶意软件，面临一系列安全威胁。

由于 ROM“刷机包”内的 APP 应用，在未开启 ROOT 权限 – 这一 Android 系统核心权限的情况下无法对其进行卸载，更直接导致其更具备传递安全风险的可能。**如 2011 年全年肆虐于 Android 平台的“安卓吸费王”恶意软件，便有近三成的感染比例来自于 ROM“刷机包”中。**

**四、2011 年度十大手机病毒及分析**

2011 年的十大手机恶意软件为：安卓吸费王、短信窃贼、短信大盗、X 卧底、安卓窃听猫、电话吸费军团、电话杀手、跟踪隐形人、联网杀手、阿基德锁。

**1.安卓吸费王（MSO.PJApps）**

截获时间:2011 年 2 月 平台:Android 主要特征:恶意扣费

安卓吸费王是 2011 年 Android 平台中感染次数最多、传播范围最广和影响范围最大的恶意软件，其自 2011 年 2 月被发现以来，目前累计植入超过 700 款 APP 应用之中，并仍在不断扩展其的伪装范围，同时由于其具备直接扣费威胁用户手机话费安全的特征，也多次被国内媒体重点曝光。

安卓吸费王是 2011 年感染范围和直接影响最大的 Android 恶意软件

作为一款典型的恶意扣费软件，其原理为利用技术手段将扣费插包批量嵌入热门应用来诱骗用户下载，装入手机后通过后台强行启动恶意进程来定制 SP 付费业务。由于其具备拦截中国移动、中国联通业务短信的行为，使得用户极易在不知情的状态下落入黑客设置的吸费陷阱之中。

**2.短信窃贼（SW.Spyware）**

截获时间:2011 年 4 月 平台:Android 主要特征:隐私窃取（短信）

顾名思义，“短信窃贼”是一款威胁指向性极强的 Android 恶意软件，其直接瞄准了用户的短信隐私。通过伪装下载手段骗取用户安装后，则会通过其已预先设置的恶意代码，在智能手机后台读取手机用户的短信内容，并通过联网进行上传。

“短信窃贼”也是网秦 2011 年初截获的第一款具备自动设定任务计划的恶意软件，经过分析发现，其可每隔 1 小时就发送用户手机中的短信内容到指定邮箱，具有很强的隐蔽性、攻击性，将直接威胁用户

的短信内容安全。

**3.短信大盗（SW.SecurePhone）**

截获时间:2011 年 6 月 平台:Android 主要特征:隐私窃取（短信）

“短信大盗”与“短信窃贼”的主要威胁目标相同，均瞄准了用户短信内容。这款恶意软件在被截获时发现，其不断可提供下载，还将部分产品以商品形式直接通过网络兜售，并以购买后可随意盗取用户隐私为诱饵来引导购买。

经过分析发现，“短信大盗”在植入手机后会自动隐藏在手机操作系统后台，并按照一定的时间频率自动记录手机短信和来电信息、照片信息。更令人吃惊的是，恶意软件在开发过程中，特别考虑到手机自身的内存空间有限，为最大限度的记录用户的隐私数据，其还会自动识别 SD 卡路径，并将其保存在扩展存储卡内。

而在成功启动后台监听，并记录到相应的隐私信息之后，“短信大盗”（SW. SecurePhone）则会利用用户手机联网时将隐私信息悄然上传到网络服务器中。此时窃听人通过远程登录到软件提供的隐私查看网站中，便能轻易调取和查阅被上传到此处的短信、来电信息和地理位置等等。

**4.X 卧底（Spy.Flexispy）**

截获时间:2011 年 6 月截获最新变种（2006 年已存在） 主要特征:窃听

“X 卧底”是一款自 2006 年便开始在中国大陆地区扩散的手机间谍软件，并已经被包括央视等媒体进行了多次曝光，甚至更被国家计算机病毒响应中心定性为高危间谍软件。但因其背后存在相当的经济利益驱动，目前“X 卧底”仍有进一步的扩散趋势。

造成其持续扩散的经济渠道源于其具备一条完善的网络销售链条，通过兜售 X 卧底，即可通过出售产品直接获利，又能通过其收集用户隐私、利用或转卖来间接获利。由于“X 卧底”在植入手机后没有任何的前端提示，用户极易在不知情的状态下成为窃听对象。

**5.安卓窃听猫（SW.Msgspy）**

截获时间:2011 年 8 月 平台:Android 主要特征:窃听

“安卓窃听猫”又名“灵猫窃听王”，其是首个可实时监听 Android 手机通话内容的间谍软件，在被截获时其仍在多个网站中以商品形式出售，并公开标识可直接窃听用户通话、后台录音及上传到指定的服务器中。

同时，“安卓窃听猫”还采用了“后台录音+联网上传”的方式窃取隐私，且具备监听手机周围环境音的功能，使得其不但监听范围更广，直接获取录音，还可被黑客快速转做于其它非法用途。

**6.电话吸费军团（BD.LightDD）**

截获时间:2011 年 7 月 平台:Android 主要特征:资费消耗/恶意推广

“电话吸费军团”是网秦截获的一款典型的资费消耗类恶意软件，自被截获后已先后伪装为超过 200 款 APP 进行传播。其会后台泄漏用户的地理位置等隐私，同时还会通过远程服务器获取指令，后台下载恶意程序，并在其中大量消耗用户的资费。

**7.电话杀手（SW.PhoneAssis）**

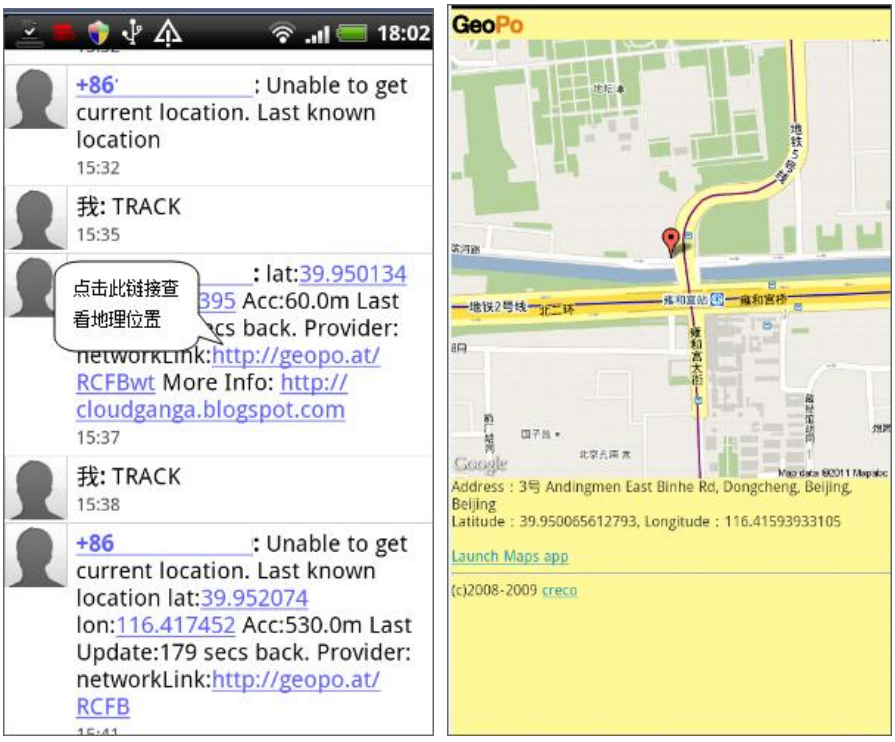
截获时间:2011 年 7 月 平台:Symbian 主要特征:隐私泄漏

该病毒以电话助手为名诱使用户下载。安装后自动运行，并且向陌生号码发送手机收件箱和发件箱中所存的短信内容以及通讯记录列表的彩信内容，严重泄露用户隐私信息，给用户手机安全造成威胁。

**8.跟踪隐形人（BD.TRACK）**

截获时间:2011 年 6 月 平台:Android 主要特征:隐私泄漏（地理位置）

“跟踪隐形人”是网秦 2011 年 6 月在谷歌官方应用商店发现的一款恶意应用，这一间谍软件的窃密方式是由监控人下载此应用后，将其植入到试图进行实时定位的被监控人手机之中。当希望查询其所在的地理位置时，此时间谍软件便会自动开启手机 GPS 定位功能，直接发送短信指令，便可直接收到对方的位置坐标。




“跟踪隐形人”感染用户手机后可通过短信指令获取监控人的地理位置

而在收到位置坐标后，点击短信中内嵌的坐标链接，便能在自动打开的手机地图中快速定位到被监控人的地理位置，如北京海淀区中关村大街某某大厦、上海徐家汇某某街某某楼等等。由于其利用了手机

GPS 基站定位技术，经过测试定位精度极高，用户很难察觉此间谍软件存在，也会直接暴露自己所在的地理位置。

**9.联网杀手（s.rogue.uFun）**

截获时间:2011 年 10 月 平台:Symbian 主要特征:资费消耗

其典型特征是联网后频繁消耗用户的上网流量，并自动联网和下载恶意推广软件，同时具有自我保护机制，启动恶意进程导致样本无法卸载。

**10.阿基德锁（a.privacy.AckidBlocker）**

截获时间:2011 年 12 月 平台:Android 主要特征:远程控制

“阿基德锁”是一款典型的 Android 远程控制木马，与以往仅具备单一特征的手机扣费和隐私窃取类恶意软件不同，其可通过多次接收远程指令触发不同的恶意行为，且拥有极为完整的从植入手机、自动后台联网再到接收远程控制指令来实施恶意攻击的流程，如其首先会通过伪装为多个标题诱惑性极强的 APP 应用来引导下载安装.

在成功装入手机后，“阿基德锁”便会通过手机后台自动联网，并借此不断接收远程服务器派发的恶意指令，代码分析显示，由于其预先设定的“短信广播优先级”已远高于 Android 系统自身的程序优先级，导致其可以轻松获得更多更大的远程操作权限，如直接通过指令让手机自动联网触发扣费行为。

**五、2011 年十大最易被手机病毒植入的应用**

2011 年，网秦“云安全”监测平台共查杀到手机恶意软件 24794 款，且其呈现伪装款数极多、传播范围极广的现象。在被植入次数最多的高危软件排行中，QQ 斗地主、手机加速器、深度睡眠、五子棋、超级电池等热门 APP 均榜上有名，受其感染量基数、频次影响，**QQ 斗地主更成为 2011 全球被伪装次数最多的手机应用。**

而从本次报告公布的 10 大高危应用可以看出，Android 平台的恶意软件由于其伪装对象更为热门，且传播效果更快，所占比例更高，而 Symbian 平台受到数字签名等验证限制，实际比例呈现明显下降势头。

| |
|---|
| 1.伪装对象:**QQ 斗地主** 平台:Android |
| 这是一款知名的手机游戏，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:**手机加速器** 平台:Android |
| 手机加速器是一款 Android 平台上火热的工具软件，其被植入了远程控制代码，植入手机后自动联网接收服务器派发的一系列恶意指令。 |
| 3.伪装对象:**打地鼠** 平台:Android |
| 打地鼠游戏是 Android 平台上的一款热门游戏，后经发现在部分渠道中传播的应用被植入了远程控制代码，植入手机后会自动连接服务器接收恶意指令 |
| 4.伪装对象:**五子棋** 平台:Android |
| 五子棋是一款 Android 休闲游戏，经分析发现部分渠道中传播的这款应用中存在吸费代码 |
| 5.伪装对象:**指纹锁屏** 平台:Android |
| 作为一款 Android 热门应用，经分析发现在部分渠道中提供的下载包内存在在窃取隐私的代码，通过远程控制木马植入后会派发恶意指令来盗取用户隐私。 |
| 6.伪装对象: **新蜀山剑侠** 平台:Symbian |
| 根据“云安全”数据监测新蜀山剑侠这款热门的 Symbian 游戏的部分程序中被植入了吸费代码，一旦下载将落入黑客设置的陷阱之中。 |
| 7.伪装对象: **语音短信** 平台:Symbian |
| 语音短信是一款新兴的移动互联网应用，但其也很快成为了黑客的伪装对象，数据显示部分渠道中存在的这一应用被植入了吸费代码。 |
| 8.伪装对象:**欢乐斗地主** 平台:Android |
| 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: **冷血狙击** 平台:Android |
| 冷血狙击是一款 Android 热门游戏，网秦“云安全”数据分析中心发现，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:**来电反转** 平台:Android |
| 来电反转是一款热门的手机工具软件，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。 |

2011 年中国大陆地区 10 大高危手机应用排行（数据:网秦“云安全”监测平台）

## 六、2011 年手机安全威胁特点解读

2011 年的移动安全形势依然严峻，且黑客正在不断利用不同的攻击技术和手机新的漏洞、隐患来发起攻击，如更多使用 ROOT 权限 – 这一 Android 系统的核心权限来植入“远程控制木马”，以及通过批量伪装来实施危害等。对此，本次报告也对 2011 年在智能手机平台存在的相关安全威胁特点进行了全面解读。

### 特点 1:恶意软件批量植入到数十/数百款手机软件之中

当前，手机恶意软件存在一个显著的特征，就是伪装对象极多，如 2011 年 2 月被网秦率先截获的“安卓吸费王”恶意软件，自首次发现至今，累计植入 APP 多大 700 款以上，“短信大盗”、“短信窃贼”等恶意软件的伪装对象也在 50 至 100 个之间，**批量植入、传播成为了其第一主要特质。**

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 Symbian 平台和 Android 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，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。

### 特点 2:ROOT 权限更易被获取，极易被滥用

“该病毒首先会获取 ROOT 权限后……”在 2011 年各大安全厂商发布的 Android 恶意软预警中，这句话常被提及。而 ROOT 权限，这一 Android 系统的核心权限，在 2011 年成为了很多恶意软件利用的对象。

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。

而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。此外，当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。

而一旦恶意软件成功获取了 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。

**特点 3:APP 应用发布前缺乏安全审核**

Symbian、Android 智能手机能快速获得用户的认可和欢迎，源于其可提供大量的手机 APP 应用，包括通过第三方接口，接纳更多的开发团队加入。根据移动应用调研公司 Distimo 在 2012 年 1 月最新的调研数据显示，目前 Android 应用商店上的 APP 应用已超过 40 万个，但在海量应用为用户提供便捷服务的同时，受到安全审核机制的限制，其中正潜在大量的安全风险。

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。

但除官方商店具备较强的安全机制外，**国内大多手机论坛、应用商店实际并无二次认证的审核流程**，开发者上传后的 APP 会立刻发布，即使被安全厂商通达其中可能包含恶意应用，并对其进行了紧急下架，但实际对已下载应用的用户仍然造成了极大的损失，且无法避免其持续扩散。

特别是伴随 2011 年下半年“远程控制木马”的兴起，如果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。

**七、2012 年手机安全行业发展趋势**

2011 年愈发严峻的手机安全形势，也正在给安全厂商的技术研发提出新的课题，2012 年，为应对安全威胁，安全厂商也将在技术领域不断进行创新，如在技术层面，继续深化“云安全”技术的应用，进一步加快对安全威胁的快速响应，以及在产品层面，通过变换产品设计思路，从传统单一查杀向一站式防御转移，和在渠道层面，通过 SDK、API 接口的开放，与产业上下游渠道共建安全移动互联网平台等。

**1.技术发展:“云安全”技术的持续深化**

2012 年，安全厂商将对“云安全”技术进行进一步深化，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技术引擎，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。

这样，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 1.2 亿手机用户提供安全保护，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。

**2.产品创新:一站式防御体系的构建**

2011 年，手机病毒、恶意软件正在呈现更为多样性的传播和攻击方式，而传统安全厂商采用的基础查杀服务，则实际已无法真正满足用户的需求。对此，2011 年下半年开始，以网秦为代表的安全厂商，正在着眼于“一站式立体防御体系”的构建。

与传统的病毒查杀服务不同，一站式防御可对恶意软件的下载、安装、启动后可能实施的恶意攻击进行全面防范，例如有效拦截手机恶意网址、并在下载前就启动对程序安全性的监测，还可在监测到手机中可能存在如隐私窃取软件、包括窃听软件时通过不同的监测模式对其进行拦截。

同时，除对智能手机进行安全保障之外，伴随平板电脑、机顶盒等数字移动终端的出现，安全产品还将陆续在这些领域进行发力，如在 2011 年，网秦已推出了可为基于 Android 系统的电视机顶盒提供安全保障的产品，在这一领域不断取得突破。2012 年，即将发布的网秦安全新品，还将继续关注更多新的安全隐患、途径等，依托技术创新为用户提供安全保障。

**3.渠道合作:全生态系理念的实施**

在技术和产品层面，分别依托技术深化和理念创新来在 2012 年继续为用户提供服务保障的同时，在移动互联网产业日益成熟，链条基本形成之时，移动安全服务企业在其中发挥的效用也将日益凸显。

而面对 2012 年更为严峻的移动安全形势，安全厂商除对个人终端提供安全保护外，还将在商业产品中持续发力，并通过针对不同渠道终端提供不同的服务，构建全生态系的保障链条。

例如，目前网秦“云安全”监测平台已为运营商、终端厂商和渠道伙伴提供了包括 SDK 和 API 两种形式的安全服务，前者可以通过本地部署到客户指定的服务器中来保障服务器内信息的完整性和安全性，后者则通过打通渠道与网秦“云安全”监测平台的接口，通过远程调用信息来实施保护，相关合作项目已陆续开展，有望在 2012 年取得更大突破。