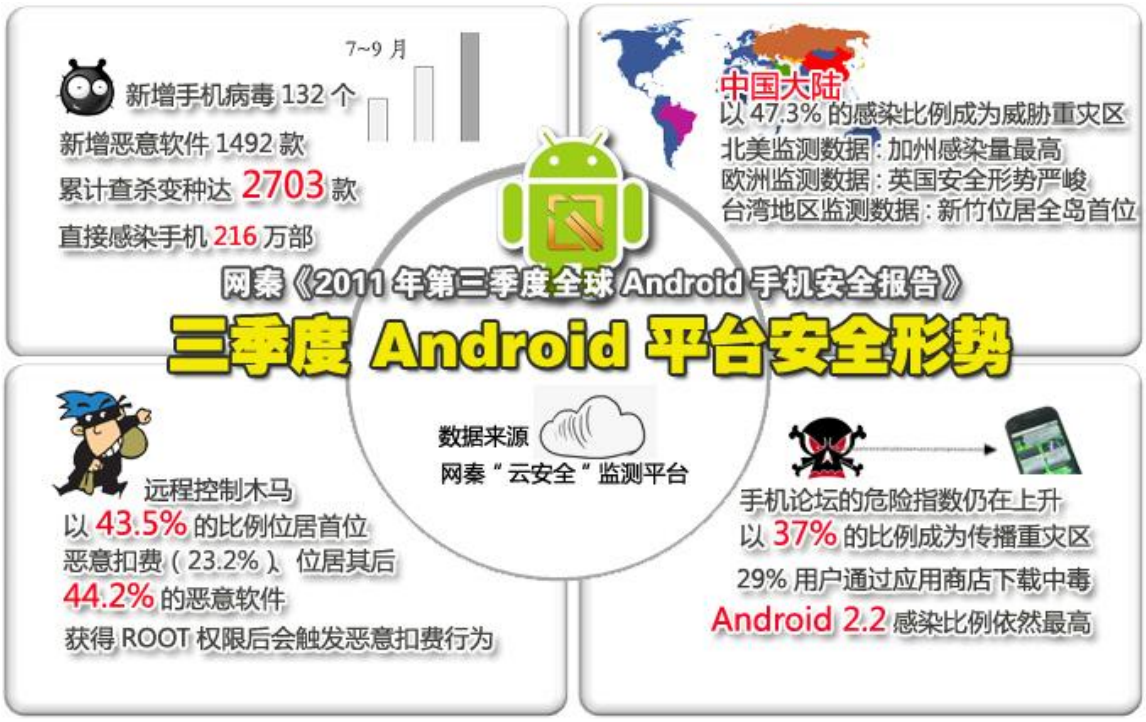
全球 Android 手机安全报告【2011.Q3】

免责声明：

该报告综合网秦“云安全”监测平台、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 3 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

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 年第三季度全球 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 年第三季度查杀到 Android 手机恶意软件及其变种达到 2703 款**（其中新增恶意软件 1492 款），**直接感染手机 216 万部。**



2011 年第三季度 Android 平台安全形势图（网秦“云安全”监测平台）

报告数据显示，**中国大陆地区以超过 47.3%的感染比例位居首位**（国内北京市位居首位），北美方面加利福尼亚州安全形势严峻，欧洲监测数据显示英国 Android 恶意软件呈泛滥趋势，台北监测中心数据显示新竹市以超过 40%的感染比例位居岛内首位。

感染类别方面，**远程控制木马以 43.5%的感染比例位居首位**，其中 44.2%的控制木马会获取 ROOT 权限 – 这一 Android 系统的核心操控权限后通过远程服务器触发扣费行为。途径方面，手机论坛的感染比例仍在持续上升。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。

此外，本次报告还对公布 2011 年第二季度的十大 Android 高危软件，QQ 斗地主、打地鼠、酷 6 视频、老虎机等热门 APP 均在第三季度成为恶意软件的重点伪装对象，成为了 **2011 年第三季度的十大 Android 被易被黑客利用的高危应用**。由于黑客不断将伪装对象转向到时下最热门的 Android 应用，用户感染恶意软件的机率正在持续加大。

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仍在持续上升。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，包括新兴特征、威胁形态的转变等，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。

二、平台安全趋势

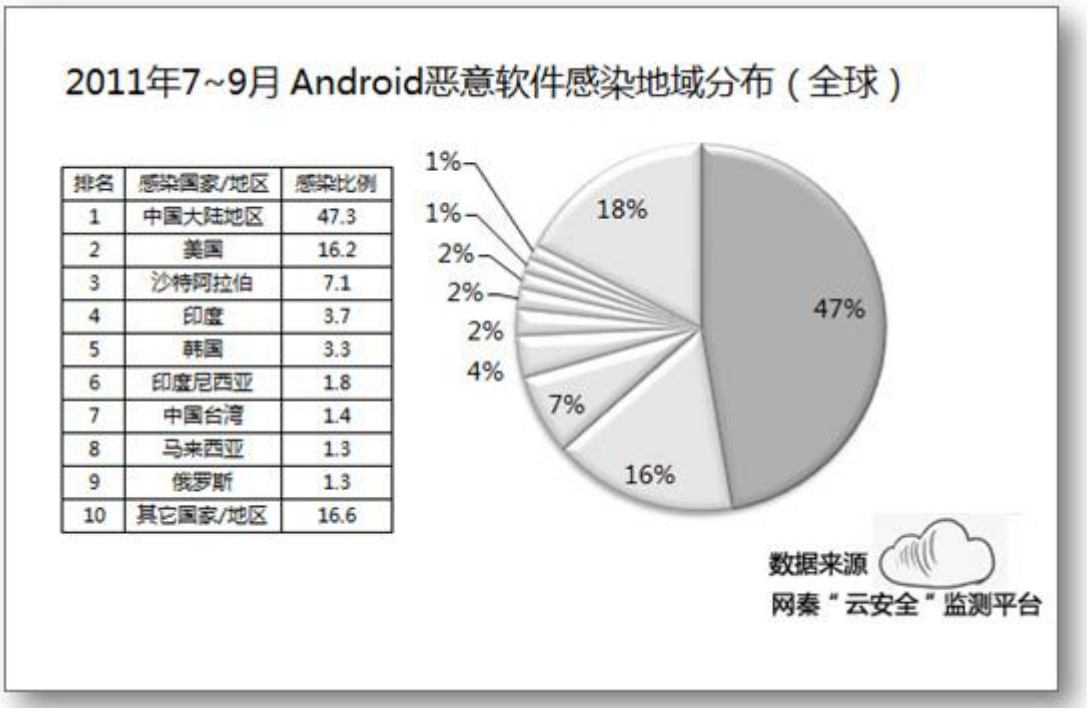
1.安全趋势:新增恶意软件数逐月上升

恶意软件威胁走势方面，报告数据显示，**据网秦“云安全”数据分析中心统计：2011 年第三季度查杀到 Android 手机恶意软件及其变种达到 2703 款**（其中新增恶意软件 1492 款）。相继出现大量利用系统漏洞获取 ROOT 权限后远程控制触发恶意行为的木马程序，实施扣费或直接窃取隐私。

2011 年第三季度 Android 手机恶意软件增长状况（新增数量）

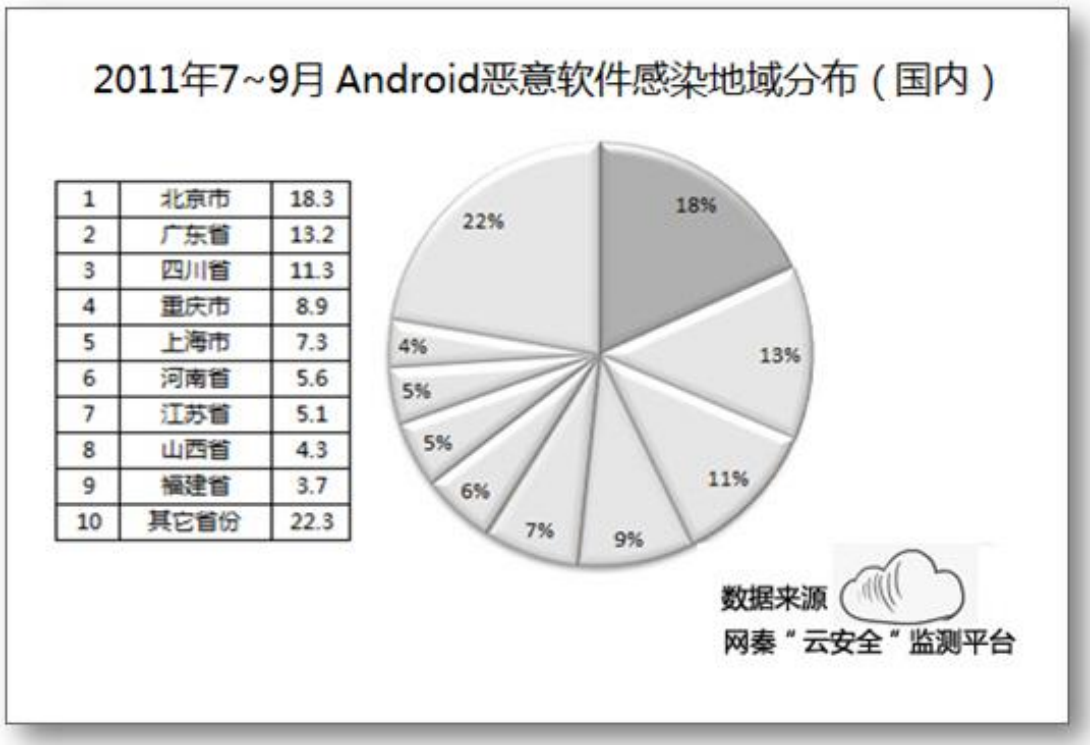
2.恶意软件地域分布:中国大陆成重灾区 北京市居首

感染地域方面，全球范围内**中国大陆地区以 47.3%的感染比例成为威胁重灾区**，美国（16.2%）、、沙特阿拉伯（5.2%）、印度（3.7%）位居其后。



2011 年 7~9 月 中国大陆地区以 47.3%的比例排名全球第一

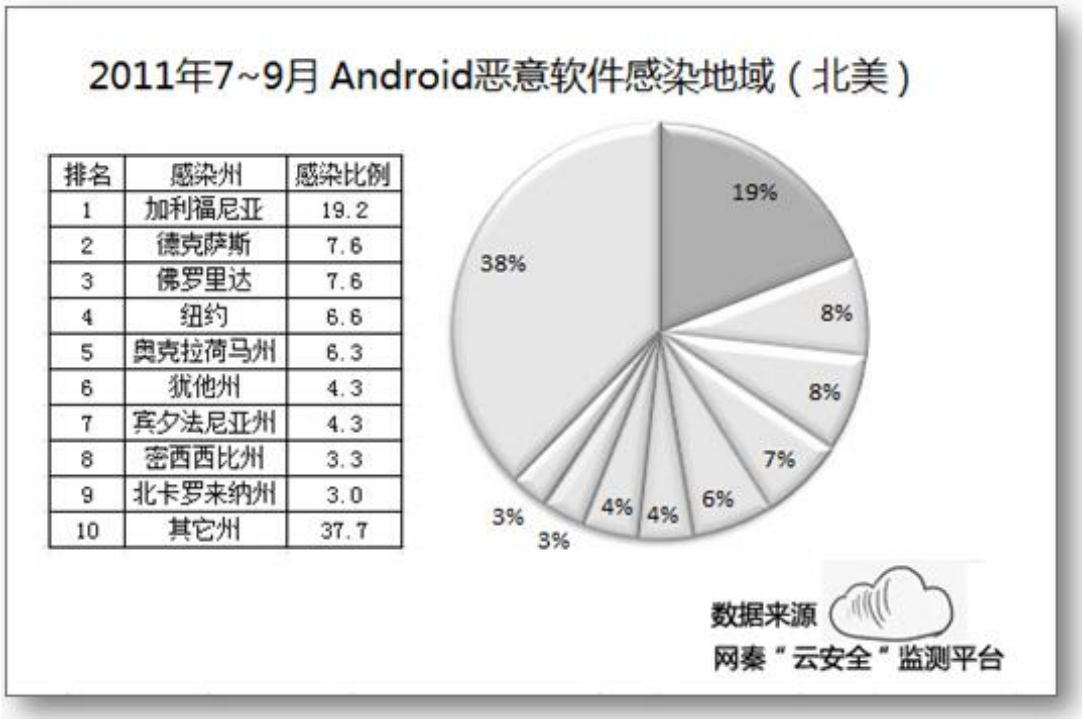
国内方面，**北京市以 18.3%的感染比例居首**，广东省（13.2%）、四川省（11.3%）、重庆市（8.9%）等省份同样饱受威胁。



2011 年 7~9 月 北京市以 18.3%的感染比例位居国内首位

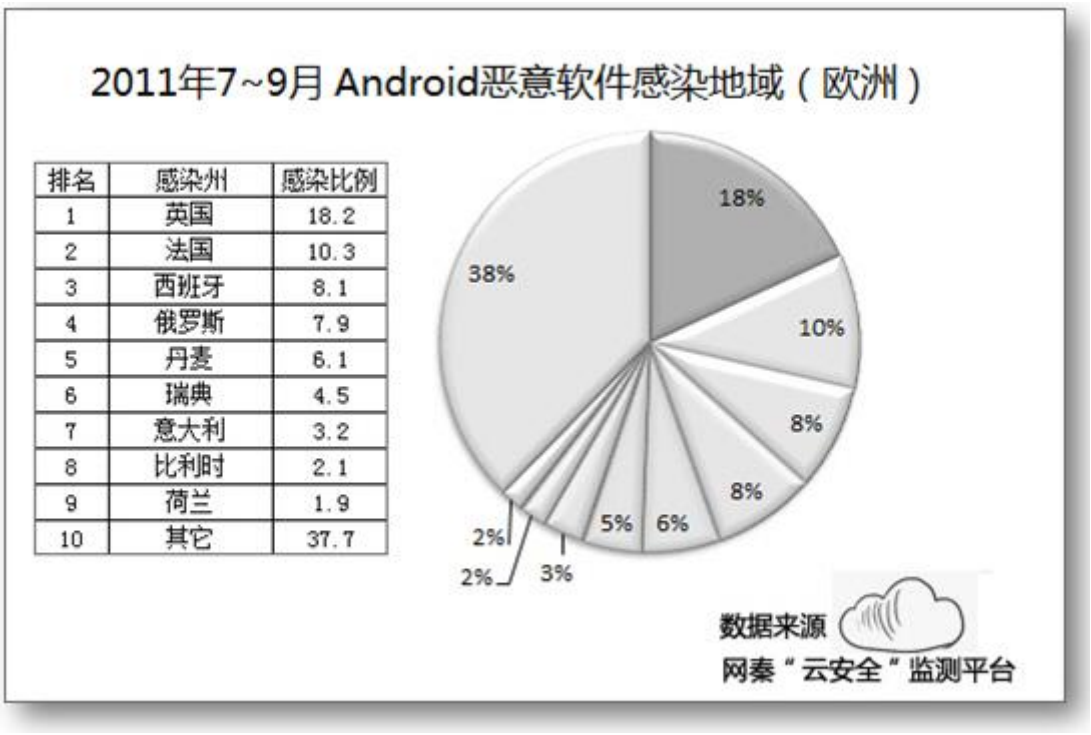
北美地区美国加利福尼亚州（19.2%）、德克萨斯（7.6%）、佛罗里达（7.6%）、纽约州（6.6%）、奥克

拉荷马州（6.3%）、犹他州（4.3%）、宾夕法尼亚州（4.3%）位居前列。



2011 年第三季度 美国加利福尼亚州感染比例位居北美首位

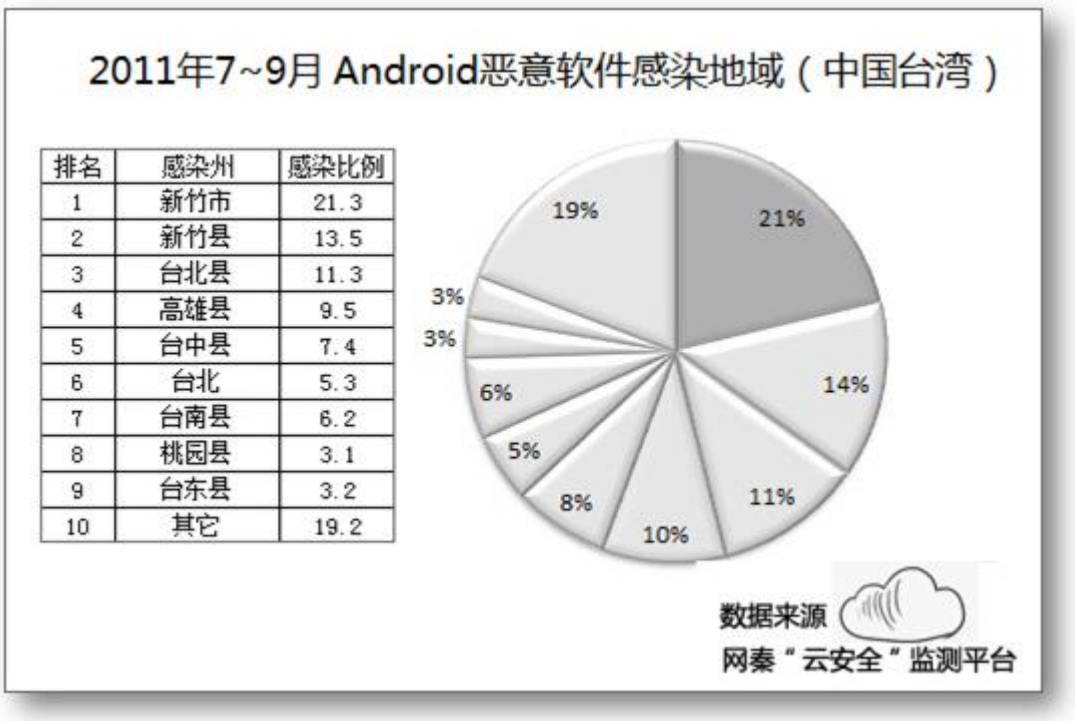
其它地区数据显示，欧洲地区，英国以 18.2%的感染比例位居首位，法国（10.3%）、西班牙（8.1%）等位居其后。



2011 年第三季度 英国以 18.2%的感染比例位居欧洲地区首位

中国台湾省中新竹市以 21.3%的感染比例成为其 Q3 季度的感染重灾区，新竹县（13.5%）、台北县

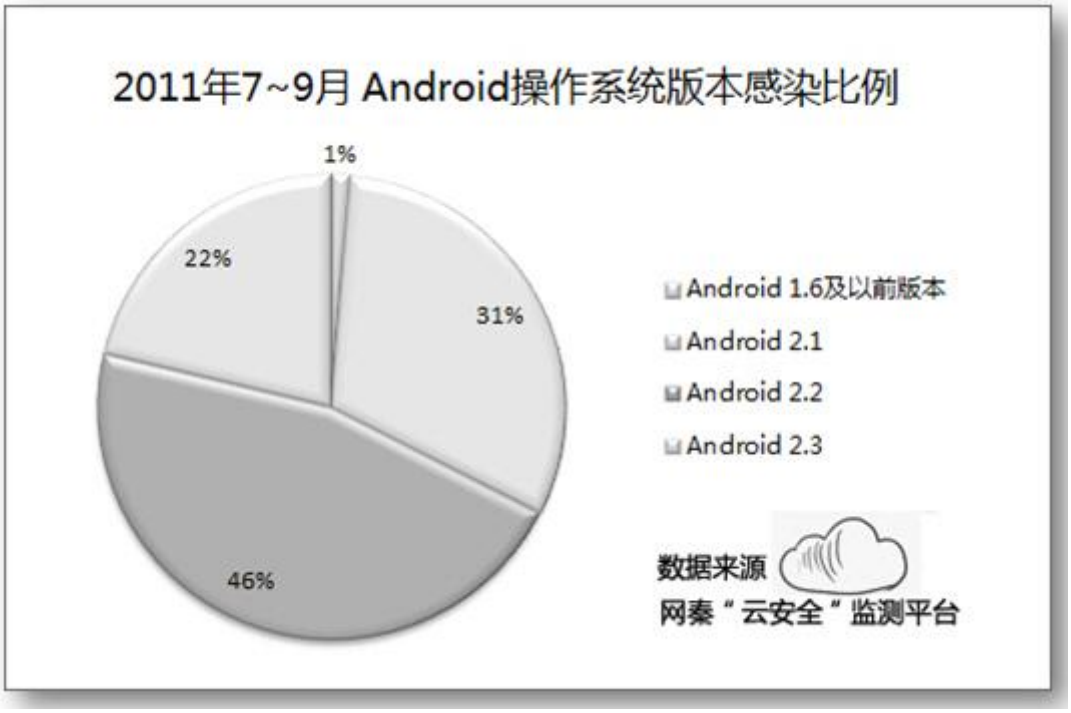
（11.3%）、高雄县（9.5%）、台中县（7.4%）位居其后。



2011 年第三季度 新竹市以 21.3%的感染比例位居中国台湾省首位

3.平台感染比例:Android2.2 成主要感染对象

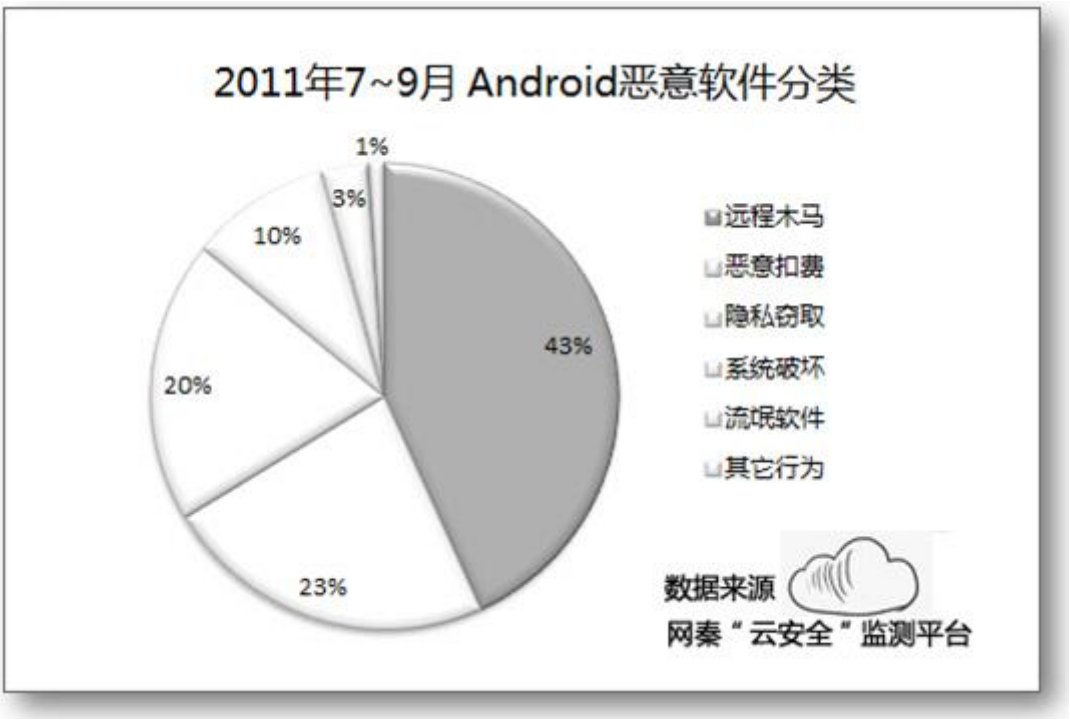
在 Android 操作系统版本分类方面， **Android 2.2 的感染比例依然最高，以 46.3%的比例成为最易被恶意软件攻击的 Android 操作系统。**Android2.1.、2.3 的受感染比例略有下降。这与 Android 操作系统的市场份额递增有明显关系。



2011 年第三季度 Android 操作系统版本感染比例

4.恶意软件特征分类:远程控制木马成恶意软件主要特征

恶意软件分类方面，远程控制木马成为 Q3 季度的主要威胁，**以 43.5%的比例位居首位**，扣费类（23.2%）、隐私窃取（20.1%）、系统破坏（9.8%）等位居其后，这与 Q3 季度出现大量通过获取 ROOT 权限来实施远程控制，派发恶意指令为目的的恶意软件持续泛滥有关（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）。



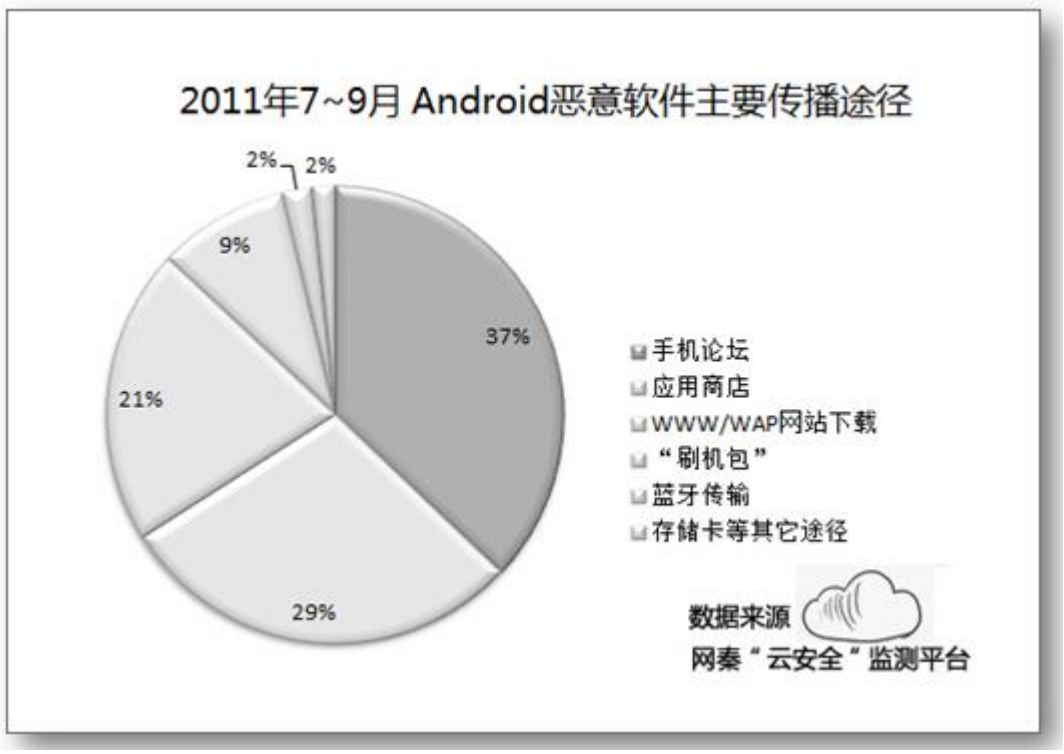
2011 年 7~9 月新增 Android 恶意软件特征分类

备注:何为“远程控制木马”？

“远程控制木马”是一种新兴的手机恶意程序，其典型特征为伪装成手机应用后诱骗用户下载，并在获取 ROOT 权限 – 这一 Android 系统的核心权限后，与远程服务器进行连接来接收其派发的一系列恶意指令。目前已知指令有，远程窃取手机 IMEI、IMSI、短信中心号码，联网触发扣费或后台推送广告程序等。

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”数据监测平台统计，手机软件论坛的危险指数仍在持续上升，**以 37%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 29%的比例位居其后。



2011 年第三季度 Android 恶意软件主要传播途径

三、安全形势解析

相比第一、二季度，三季度 Android 恶意软件出现了很多新的特征，**“远程控制木马”**异军突起导致恶意软件数量仍然呈现增长趋势，而在地域分布方面，北美的安全形势不容乐观。

1.恶意软件增长趋势解析

通过报告数据可以看到，三季度 Android 恶意软件继续呈现增长趋势，并有多个在一季度、二季度出现的恶意软件再度变种，如在 2011 年 2 月截获的“安卓吸费王”恶意软件，在三季度继续呈现爆发趋势，

至今已有超过 500 款应用成为其的伪装和利用对象。

同时，由于远程控制木马的快速兴起，通过“后门”二次传播恶意软件、恶意插件的现象也开始增多，导致出现了短期内大量恶意软件集中发作的现象，部分恶意软件在威胁手机安全的同时还开始向 Pad/数字机顶盒迁移，安全威胁呈现了扩散趋势。

2.恶意软件地域分布解读

地域分布数据中，中国大陆感染比例略有下调，这与“云安全”产品在这一地区的积极部署，和手机用户安全意识的逐渐提升相关。而北美地区的安全形势逐渐呈现恶化趋势，据网秦北美研究中心分析，这主要以通过获取 ROOT 权限后盗取用户隐私的 DroidDream 恶意软件感染量激增有关，数据显示，包括“Super Guitar Solo（超级吉他独奏）”等数十款热门应用均成为其的伪装对象。

3.系统平台感染比例分析

三季度在 Android 平台下，Android2.2 操作系统的感染率依然最高。这主要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。而伴随下半年出厂的 Android 新机陆续搭载 Android2.3 或更高版本，第四季度的 2.3 有望成为新的感染重点。

4.恶意软件感染特征判定

在三季度 Android 安全报告中，“远程控制木马”呈现迅猛增长势头，且比例直线上升，和以往恶意软件固定的、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，如其在强行获取 ROOT 权限 – 这一 Android 操作系统的核心权限之后，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。

而在其它感染比例中，恶意扣费软件比例仍然较高，这主要因“安卓吸费王”变种的激增和先后出现大量以联网扣费为主要方式的吸费软件。相比之下，二季度感染比例最高的隐私窃取类恶意软件比例则略有下降，由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.安全威胁传播途径分类

第三季度，中国大陆地区的 Android 手机出货量继续呈现井喷态势，据美国投资公司 Morgan Keegan 分析师特拉维斯·麦克科特（Travis McCourt）发布的投资者报告分析，第三季度仅在中国市场智能手机出货总量就达到了 800 万至 1000 万部，远超过去年同期的 200 万至 300 万部。其中，采用 Android 操作系统的智能手机占据了当季中国市场智能手机销售总量近一半的份额。

而在 Android 手机出货量激增的当前，手机应用的获取渠道 –Android 应用商店、手机应用论坛由于安全监管机制还较为薄弱，仍然存在有被黑客利用散播恶意软件的现象，如在三季度的网秦“云安全”监

测平台数据显示，**在超过 75%的应用渠道中发现存在或曾存在有恶意软件。**

数据显示手机论坛依然是 Q3 季度 Android 恶意软件的主要传播途径

同时，在本次安全报告公布的 2011 年第三季度的十大 Android 恶意软件中显示，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 年第三季度，网秦“云安全”监测平台共查杀到 Android 恶意软件 1492 款， 在中国大陆地区，“QQ 斗地主”、“打地鼠”、“五子棋”、“指纹锁屏”、“来电翻翻”等十款 Android 应用成为恶意软件的主要伪装对象。

1.伪装对象:**QQ 斗地主**
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**
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**
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**
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:**越测试爱**
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**
三季度数据中，新蜀山剑侠这款热门的 Android 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**
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**
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: **迷你相机**
迷你相机是一款 Android 手机工具软件，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:**来电翻翻**
来电翻翻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 年第三季度 中国大陆地区十大高危软件排行

而在北美地区，Angry Birds Rio Unlocker、AccuTracking、Battery Saver 等成为十大高危软件。欧洲地区，Angry Birds Cheater、GPS Spy Tracker、Paint Master、Sexy Girls 等十款应用排名首位。中国台湾地区，跟雛子一起做運動、極酷鈴聲、SwordRequiem 的感染比例位居首位。

数据证实，面对当前迫在眉睫的严重安全形势，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

从三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

三度 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“网秦手机安全”5.2Android

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，网秦手机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，全面查杀三季度新增的 Android 恶意软件及其变种程序。

2.保护 Android 手机话费/隐私安全

三季度以来，恶意扣费软件数量激增，同时由于近半数的“远程控制木马”存在触发扣费指令的行为，专家建议用户应选择如“网秦手机安全”Android 版来全面保护我们的话费安全。

同时，可通过网秦手机安全 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，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。

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。

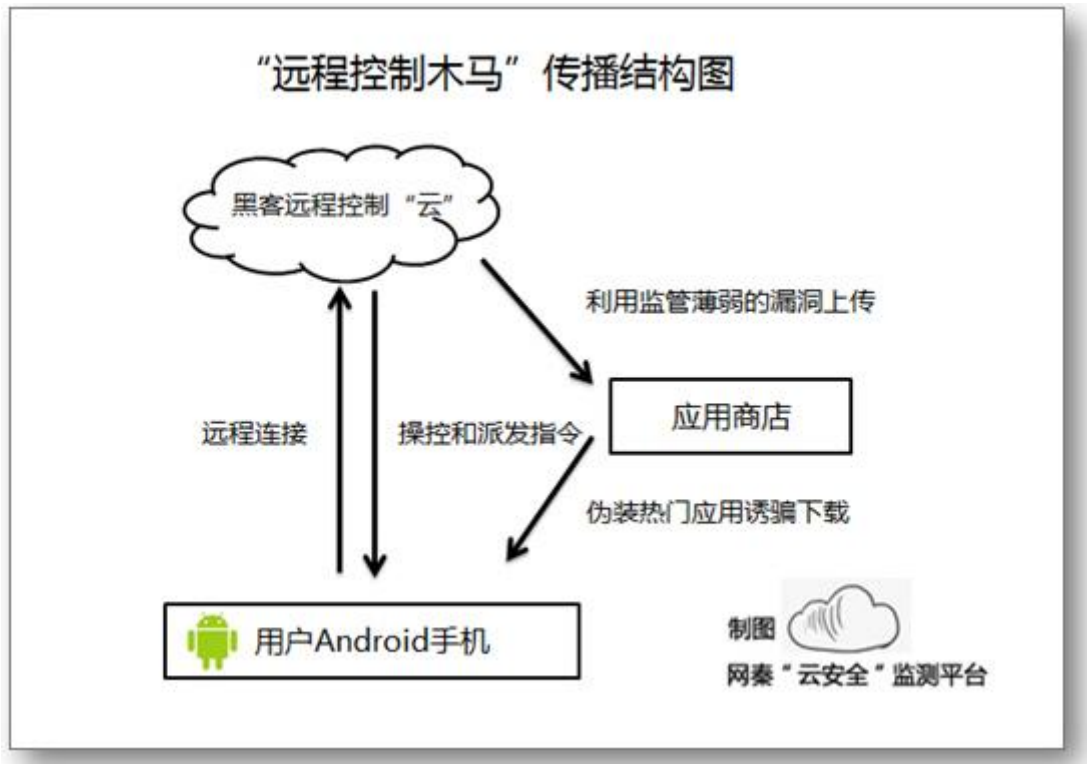
六、安全技术趋势

从数据和走势分析可以看出，三季度安全威胁出现了很多新的改变，一来使得其直接威胁更为隐蔽，二来通过更为广泛的扩散方式增加用户的“中招”机率。

1.新趋势:恶意软件进入“云”时代

就在安全厂商的技术产品以“云安全”作为主要技术手法来遏制安全威胁的同时，“远程控制木马”的出现，使得恶意软件也在三季度出现了向“云”时代迈进的现象。

和安全软件调用“云安全”数据来对安全威胁进行实时鉴定的原理相同，“远程控制木马”首先将控制端打包加入到一些热门应用之中，伪装诱骗用户下载后会通过手机“后门”联网并于远程服务器连接，并接受其发送的对应指令。



“远程控制木马”传播结构图（制图:网秦“云安全”监测平台）

与此前可通过代码解析查阅其实际危害的情况不同，由于“远程控制木马”直接调用网络数据，对手机安全软件的判定工作增加了巨大的难度。同时由于其在打通“中招”用户与网络服务器的连接之后，可通过“后门”推送各类恶意插件，导致用户手机面临大量不确定的安全威胁。

2.新形态:恶意软件向平板等新设备迁移

三季度以来，Android 恶意软件在对手机进行攻击并威胁话费、隐私安全的同时，也开始将目前向使用 Android 操作系统的平板电脑、数字机顶盒迁移。如在 2011 年 8 月，来自网秦北美研究中心的分析显示，已有恶意软件可对基于 Android2.3 系统的平板电脑发起攻击。

分析显示 Android 恶意软件将威胁更多智能终端

分析显示，存在通话功能的平板电脑是目前的高危终端，由于其与智能手机相同同样以 3G 线路接入，无论是因感染恶意软件导致的扣费问题或流量消耗问题都将在未来成为平板电脑的安全隐患，在三、四季度“千元平板”大行其道的当前，安全问题正日益凸显。

3.新弊端:流量管理问题已日益凸显

由于 Android 手机的多数应用均需联网使用，联网过程中消耗的流量成为了用户关注的重点，三成 APP 无法直接关闭，后台偷跑流量 30%恶意软件后台联网的现象，导致用户饱受扣费、隐私泄漏问题困扰的同时，还在思索如何有效管理上网流量的问题。

同时，由于目前相关恶意软件在单纯消耗上网流量的同时，还存在传播恶意软件的情况，更使得其可能对手机用户构成进一步的危害。可以预见在 Q4 季度，这一现象将依然普遍，也亟待手机安全厂商在“网络防火墙”产品的研发中尽快取得突破。