NQ mobile

NQ 移动公司
《2012 移动安全报告》
发布时间：2013 年 3 月

我们的方法

NQ 移动公司的《 2012 安全报告》基于 NQ 移动公司安全实验室团队的洞察，该团队在全球拥有超过 250 名移动安全专家、科学家和开发人员，他们随时主动监控手机世界，以找出新出现的恶意软件威胁和手机黑客攻击方法。报告中所依据的数据由 NQ 移动公司的多种专用工具和资源收集而来，这些工具和资源包括：

- RiskRanker™：一款应用分析系统，可利用人工智能来自动扫描和标记表现出可疑行为的应用。到目前为止，RiskRanker 已在全球406个不同智能手机应用市场对超过 5.3百万个应用进行了扫描。
- NQ 网络链接(URL)爬网技术：一款扫描引擎，可梳理网络以找寻可疑 URL。2012 年，NQ 移动公司对超过 22 亿个 URL 进行了扫描，并发现了超过5.4百万个欺诈性 URL，这些 URL 试图通过下载木马软件来暗中监控手机设备活动，远程控制设备，或者访问私人信息。
- 全球智能网络：遍布于 150 多个国家的超过 2.8 亿智能手机用户为新型恶意软件的蔓延提供了实时洞察，从而使得 NQ 移动公司能够在第一时间发现手机恶意软件并避免其蔓延。

安全报告摘要：

回顾过去，2011 年是手机恶意软件的一个重要转折点。Android 正式取代 Symbian 成为恶意软件的第一大操作系统目标，并且恶意软件感染开始越过中国和东欧，蔓延到了西欧和美国。这些趋势在整个 2012 年持续演进，但是范围更大，而且恶意软件设计和社群工程均有技术方面的显著进步。

2012 全球恶意软件聚焦：

- 2012 年，NQ 移动公司发现了超过 65,227 个新型恶意软件，软件数量较去年同比增长 263%
- 在 2012 年发现的大部分恶意软件被设计用于攻击 Android 设备与 Symbian 设备。其中，Android 设备数量占所有被攻击设备的 94.8%，而与之相比，Symbian 设备占 4%。
- 据 NQ 估计，2012 年，有超过 3,200 万的 Android 设备被感染，而在 2011 年这一数字为 1,080 万，成长超过 200%。
- 受感染的设备来主要来自中国 (25%)、印度 (19.4%) ，俄罗斯 (17.9%)，美国 (10%)，和沙特 (9.6%) 。

- 在 2012 年发现的手机恶意软件中，有 28% 被设计用来收集用户的个人数据并从中牟利
- 7% 的恶意软件只是用来使用户的设备停止工作（即，使他们的手机处于“瘫痪”状态）
- 2012 年，传输恶意软件的三种主要途径包括短信收费欺诈、恶意 URL 和应用打包

短信收费欺诈
这是从受害者那里提取个人敏感数据的最有效和获利最多的方法之一.网络犯罪分子将社交工程应用于短信和电子邮件中，这样用户就会跟他们进行联系，并被要求点击恶意链接，该链接会将 Premium Rate Service (PRS) 图片自动下载至用户的设备上或者引导用户访问一个恶意网站。网络犯罪分子每发一条短信最多可赚取 4 美元。

URL 篡改
例如，用户使用手机浏览器访问恶意网站，而后该网站将开始在后台偷偷下载至移动设备上。之后，该恶意软件将试图拦截一次性密码 (OTP) 短信。

应用重新打包
网络犯罪分子将恶意代码行添加至真正的应用中，将其重新打包并重新加载至第三方市场，供不知情的手机用户下载和安装。一旦安装完毕，该应用将开始在后台工作，收集用户数据，更改移动设备上的用户设置，或者远程控制该设备以发送短信。

2012 恶意软件发现聚焦

2012 年，NQ 安全移动公司安全实验室发现了许多新型移动恶意软件。其中包括有史以来在全球范围造成最严重损失的短信收费欺诈感染，以及在 Google Play 商店中发现的一例新型高级恶意软件，后者经证实可使用经感染的移动设备感染 PC 。

- **Bill Shocker**：史上感染性最强且造成损失最严重的手机恶意软件，在被 NQ 移动公司发现之前，已感染了超过 600,000 的中国用户。使用腾讯 QQ Messenger 和搜狐新闻等主流应用的移动设备被感染。Bill Shocker 先是偷偷在后台自行安装在 Android 设备上，之后试图对移动设备采取远程控制，包括上传联系人数据、互联网连接、拨号和发短信功能等。然后，Bill Shocker 将设备变成“僵尸”，这样它就可在用户不知情的情况下发送 PRS 短信。此外，Bill Shocker 还能够进行自我升级，这点类似于 VDloader （见下图）。
- **VDloader**：该恶意软件作为客户端运行在 Android 设备上，并请求与远程服务器进行交互。其主要感染路径是借助一条短信链接，通过使用社交工程技术来

锁定受害者。用户点此链接后，它将隐藏在真正的应用后面，只在有要求时才进行广播。同类型的恶意软件中，该软件为首个被全球所有安全厂商报告称可自动自行升级的恶意软件。NQ 发现共有 1714 位用户被 VDloader 感染。

- **DyPusher**：此恶意软件能够上传设备的具体信息（即 IMSI、IMEI、手机号码、系统号码等），并能够在用户不知情的情况下动态下载文件与应用，从而导致隐私丢失和潜在的高额账单。自此种病毒发现后共有 210 位 NQ 用户被感染。
- **FireLeaker**：该恶意软件伪装成 Widget 并隐藏起来，但可收集设备的具体信息（即 IMSI、IMEI、手机号码、系统号码等）和联系人数据，并上传至远程服务器。自此种病毒发现后共有 13 位 NQ 用户被感染。

2013 年恶意软件趋势

网络犯罪分子将继续使用那些起作用的恶意软件，因此我们认为，短信付费欺诈、恶意 URL 和应用重新打包将继续成为恶意软件进入市场的首选方法。但是，2013 年也将会出现几个新趋势。

- **跨平台恶意软件：**在 2013 年首次发现一个新种病毒能从 Android 传播到 PC。这个病毒(a.spread.Ssucl.a)是由 Google 应用商店上的一款清除内存的软件中查到，Google Bouncer 并无检测出。这款恶意软件会发送 / 上传 / 删除短信，开启 WIFI，搜集手机资料，自动开启 Android 自定浏览器,上传内存卡中资料和手机中的档案及照片。NQ 安全实验室的专家发现一但用户开始同步手机和 PC，并且透过 USB 链接同步的动作去传送“AutoRun Attack”，就会驱动这个恶意程序。正因为 NQ 移动能及时发现这个恶意软件，只有极少数用户被感染。可是这也说明跨平台感染是可能的，而将来会有更多类似的恶意软件产生。2013 年，NQ 移动预测跨品台的恶意软件将会透过无限网络同步过程进而感染 PC，手机，家庭网络，和云端。
- **僵尸网络：**这些威胁将充分利用操作系统的漏洞和银行应用 (OTP) （参见下述 P2P）。这一趋势与 rootkit 和手机特定 DDoS 恶意软件一起，将继续推动“黑市活动”。
- **个人对个人应用：**消费者现在已很少使用现金或签发支票，而转向使用个人对个人 (P2P) 应用，此种方式允许个人通过地址、手机号码或者收件人卡号将钱寄给另一持卡人。网络犯罪分子正在寻找拦截一次性密码 (OTP) 的方法，该方法又称为带外验证 (OOBA) 技术。
- **短信收费欺诈：**网络犯罪分子会继续将东欧和亚洲（包括中国、印度、沙特阿拉伯、泰国和印度尼西亚在内）作为将此类恶意软件散布至全球的主要地区。
- **流氓（危险）应用：**恶意软件编写者会继续将恶意 Android 应用上传至第三方市场，并试图绕开 Google Play 商店的 Google Bouncer 扫描引擎。

- **短信和电子邮件钓鱼攻击**—使用短信和电子邮件的社会工程攻击将会继续存在，因为这是从受害者那里提取个人敏感数据的最高效方法之一。
- **儿童黑客（又名“Carder Kids”）：** 除了不断发掘和解析新型的恶意软件之外，NQ 移动安全实验室的专家也定期调查黑客和恶意软件作者的沟通和协作渠道。在这些论坛中，NQ 移动发现 13-20 岁的年轻黑客们，也被称为“Carder Kids”使用结合移动恶意软件和社交工程的方法去盗取手机上的信用卡号码，PayPal 登录细节，或其他财务数据。然后这些儿童黑客再将这些财务信息贩售给其他更有经验的网络罪犯（或“钱骡”），进而将个人财务信息变现。