

2012 年中国手机安全状况报告

(全年)

360 互联网安全中心

2013 年 1 月

目 录

| | |
|-------------------------------|----|
| 引言及摘要 | 3 |
| 一、2012 年手机木马及恶意软件增长情况 | 5 |
| 二、2012 年手机恶意广告数据增长情况..... | 14 |
| 二、2012 年垃圾短信、骚扰电话数据增长情况 | 16 |
| 四、2012 年手机安全焦点解读 | 17 |
| 五、2013 年手机安全趋势预测 | 26 |
| 六、手机安全建议及解决方案..... | 27 |

引言

2012 年，我国移动互联网用户数量、应用水平、终端普及、市场规模等均呈现迅猛增长态势。中国互联网络信息中心数据显示，截至去年 12 月底，2012 年国内智能终端出货量达 2.24 亿部，已成为全球最大的智能手机生产国。

但在一系列热潮背后，智能手机的安全问题也愈发凸显，在过去一年中，手机木马、恶意广告严重威胁着用户的隐私、话费、流量安全；垃圾短信、骚扰电话直接影响着用户的正常生活和信息安全；僵尸网络、系统漏洞等新安全焦点问题的出现，更使得用户的智能手机在 2012 年时刻处于险恶的安全威胁之中。

为此，360 互联网安全中心发布《360 手机卫士 2012 年中国手机安全状况报告》，力图通过详细、权威的数据展示，全方位、多角度地剖析 2012 年度我国大陆地区手机安全状况，聚焦安全焦点、以关键词、关键数据为依托进行详尽分析。为有关部门、媒体和用户提供有力的数据参照。

摘要

- 2012 年，360 互联网安全中心新增手机木马及恶意软件（以下简称：恶意软件）手机恶意广告插件 347665 款，感染用户 5.5 亿人次。其中新增手机恶意软件样本 174977 款，同比 2011 年增长 1907%，感染用户 71664334 人次，同比 2011 年增长 160%；新增恶意广告插件 172688 款，感染用户 483130415 人次。

- 新增手机恶意软件样本中，71%集中在 Android 平台。Android 平台在新增安全威胁的增速与增量上仍全面居首，成为移动互联网安全攻防主战场。

- 在感染区域方面，广东省以 12.1% 的感染比例位居首位，山东、河南、江苏、浙江以 6.8%、6.7%、5.7%、5.2% 感染比例同列前五。
- 根据对恶意软件的主要恶意行为进行判断，资费消耗成为 Android 手机恶意软件的主要危害之一，占感染人次的 52%，隐私窃取类占 28%，恶意扣费类占 11%，欺诈软件和系统破坏类各占 7% 和 2%。同时，2012 年中大量出现一款恶意软件同时具备多重危害的特点，31% 的恶意软件同时具备三种以上的特征。
- 48.2% 的手机恶意软件来自应用商店、论坛等第三方下载渠道中，另有 31.4% 来自于 ROM 刷机包等途径，13.6% 通过短信内链接，5.7% 通过二维码、短网址传播。1.1% 通过其它方式传播（如蓝牙等）。
- 2012 年第三季度起大规模爆发的“安卓僵尸网络”系列恶意软件，全年累计感染用户 453 万次以上，成为年度感染量最大的系列恶意软件。
- 伪“QQ 网游大厅”以 1705496 次的感染量成为感染量最大的恶意软件。
- 360 手机卫士全年共为 2.2 亿用户拦截垃圾短信 712 亿条，日均拦截近 2 亿条，骚扰电话 352 亿次。日均拦截近 9600 万次。

报告正文

一、2012 年手机恶意软件增长情况

1.手机恶意软件款数激增 同比增长达 1907%

2012 年，360 互联网安全中心新增手机恶意软件样本 174977 款，同比 2011 年增长 1907%，感染人次 71664334 人次，同比 2011 年增长 160%。

其中，Android 平台以新增样本 123681 款，占全部新增样本数量的 71%，感染量达 51746864 人次，占恶意软件感染总次数的 78%，成为手机恶意软件的主要感染平台。2012 年 12 月，其更以单月新增 30809 款达到历史新高。



2012 年 Android 新增恶意软件数量月度变化 (来源:360 互联网安全中心)



2012 年 Android 恶意软件感染量月度变化图 (来源:360 互联网安全中心)

Symbian 平台中, 新增恶意软件数量和感染量则呈现下降趋势, 全年新增样本 51296 款, 占全部新增样本数量的 29%, 感染人次 19917470 次, 占手机恶意软件感染总次数的 22%。

2012 年 Symbian 新增恶意软件数量月度变化图

■ 单位：款



数据来源：360 互联网安全中心（2013 年 1 月）

2012 年 Symbian 新增恶意软件数量月度变化图（来源：360 互联网安全中心）

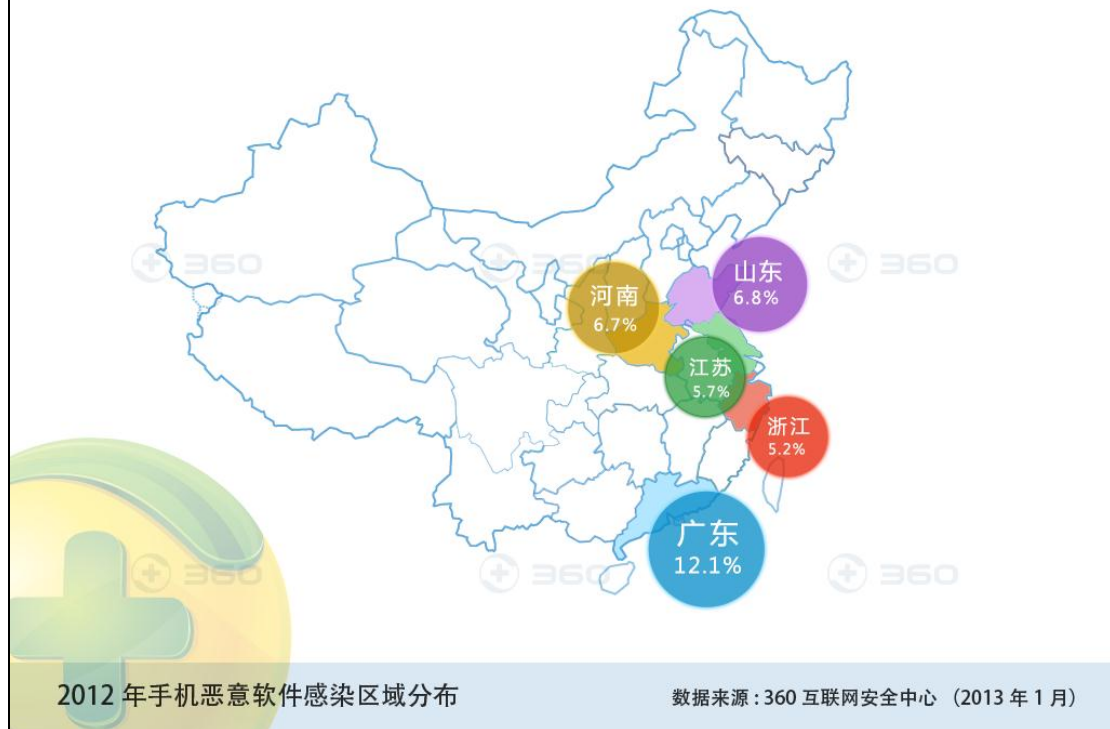
2012 年 Symbian 恶意软件感染量月度变化图


数据来源：360 互联网安全中心（2013 年 1 月）

2012 年 Symbian 恶意软件感染数量月度变化图（来源：360 互联网安全中心）

2. 广东以 12.1% 比例居首，山东、河南紧随其后

在 2012 年手机恶意软件的感染地区分类中，广东省以 12.1% 的感染比例位居首位，山东、河南、江苏、浙江以 6.8%、6.7%、5.7%、5.2% 感染比例同列前五。同时，上述地区活跃的水货刷机渠道也正在成为恶意软件的主要传播源，数据显示，近三成恶意软件被预置在水货手机 ROM 中进行传播。

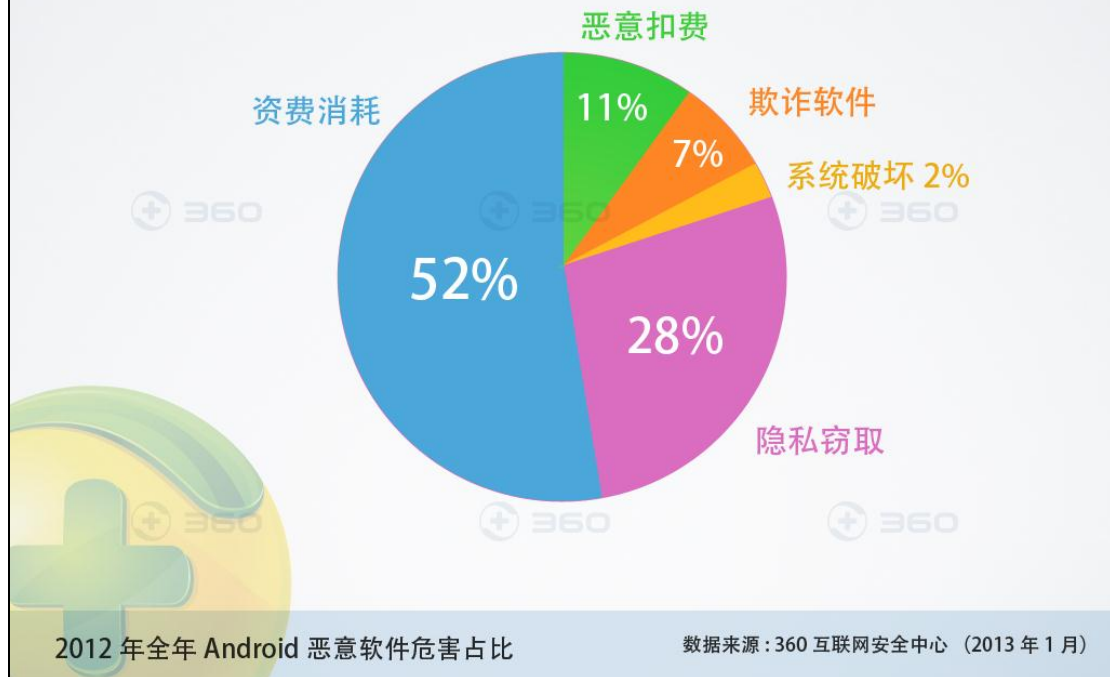


2012 年手机恶意软件国内感染比例（来源：360 互联网安全中心）

3. 资费消耗成主要危害，更多恶意软件集多种危害于一身

危害方面，以 Android 平台为例，资费消耗仍然是手机恶意软件的主要危害，以 52% 的比例位居首位，其在感染手机中，可通过联网指令下载、推送各种应用，严重消耗用户的手机电量、流量。

隐私窃取、恶意扣费也依然是用户另外面临的主要安全威胁。其中，28% 的恶意软件可通过感染手机后，后台收集用户的短信、通话、位置等信息，联网或通过短信外发，直接导致用户的关键隐私泄漏；11% 的恶意软件在引导用户安装后，通过外发短信、联网订购等诱骗用户开通各类 SP 付费业务，借此恶意吸费。



2012 年全年 Android 恶意软件危害占比（来源：360 互联网安全中心）

而在 Symbian 平台中，资费消耗类恶意软件也以 41% 的比例居首，另有 39% 为系统破坏类，如劫持系统管理器、破坏正常的程序组件等，影响手机的正常运行；19% 为恶意扣费类；1% 为隐私窃取类。



2012 年全年 Symbian 恶意软件危害占比（来源:360 互联网安全中心）

此外，在 2012 年中，手机恶意软件出现了一种较为明显的新趋势，即越来越多的木马及恶意软件集多种作恶手段于一身，通过黑客远程控制执行不同的恶意行为，近 3 成的手机恶意软件同时含有资费消耗、恶意扣费、隐私窃取等三种以上的恶意行为。

4.传播途径：近半数集中应用商店/论坛 部分利用二维码、短网址传播

在手机恶意软件的传播途径中，经过分析，第三方应用商店/手机软件论坛仍是手机恶意软件的主要传播途径，以 48.2% 的感染比例位居首位，ROM “刷机包” 则以 31.4% 的比例排名第二，短信链接以 13.6% 的感染比例紧随其后，通过二维码、短网址传播恶意软件的比重有所上升，达到 5.7%。其它（如蓝牙等）占 1.1%。



2012 年手机恶意软件传播途径（来源：360 互联网安全安全中心）

5. 感染量排行：单系列木马最高感染超 400 万 单款恶意软件最高感染近 200 万

2012 年，手机恶意软件呈现了明显的系列化特征，如黑客将同一危害类型的恶意代码同时嵌入到数十、数百款 APP 应用中传播，平均感染手机均达百万次以上。

如自 2012 年第三季度起大规模爆发的“安卓僵尸网络”系列，全年累计感染用户 453 万次以上，成为年度感染量最大的系列恶意软件。

| | |
|---------------------------|-----------|
| a.expense.superpack 系列 | 4538063 次 |
| a.expense.Apxxxad 系列 | 3389375 次 |
| a.privacy.Counterclank 系列 | 2659644 次 |
| a.expense.zooaircraft 系列 | 1859876 次 |
| a.expense.FakeYGapp 系列 | 1814481 次 |
| a.privacy.Tgkiller系列 | 1705496 次 |
| a.expense.Qdplugin 系列 | 1496504 次 |
| a.expense.DPNSer 系列 | 1496360 次 |
| a.expense.i22hk 系列 | 1411109 次 |
| a.expense.apkqu系列 | 1136805 次 |

年度感染次数最高的手机恶意软件系列 TOP10

数据来源：360 互联网安全中心（2013 年 1 月）

年度感染次数最高的手机恶意软件系列 TOP10（来源:360 互联网安全中心）

a.expense.Apxxxad、a.privacy.Counterclank 等系列恶意软件的感染量也平均超过 200 万的感染次数，分类年度感染次数最高的手机恶意软件系列 TOP10。

而在单款软件/篡改软件感染量排名中，伪“QQ 网游大厅”以 1705496 次的感染量位居首位，黑客通过在原版应用中嵌入恶意代码后二次打包，以原名诱骗用户下载安装，在感染用户手机后会在后台私自发送短信到指定号码，定制扣费业务，并自动下载应用，严重消耗用户的手机资费。

同时，包括“易购”、“安卓软件架”、“捕鱼达人”等热门 APP 应用也成为黑客篡改的目标，感染量均达 40 万以上，主要危害包括后台私自下载软件、窃取手机短信、位置信息等。

| | 篡改应用名称 | 全年感染量 | 危害类型 | 描述 |
|---|-------------------------|-----------|--------------|--|
| 后台运行、无图标 | QQ 网游大厅 | 1705496 次 | 恶意扣费 资费消耗 | 安装后无图标显示，私自发送短信到指定号码，警惕该软件定制扣费业务造成流量等资费消耗。 |
| 后台运行、无图标 | z.a | 1635337 次 | 资费消耗 | 该软件后台私自下载安装软件，造成用户流量资费消耗。 |
|  | 易购 | 1331733 次 | 资费消耗 | 该软件后台私自下载安装软件，造成用户流量资费消耗。 |
| 后台运行、无图标 | com.android | 790960 次 | 隐私窃取 | 伪装成系统软件，窃取用户手机短信信息、通话记录、位置信息、手机号码等隐私信息回传至服务器，造成用户隐私泄露。 |
|  | 安卓软件架 | 653758 次 | 隐私窃取 | 伪装成系统软件，窃取用户手机短信信息、通话记录、位置信息、手机号码等隐私信息回传至服务器，造成用户隐私泄露。 |
| 后台运行、无图标 | Android Network_Support | 555245 次 | 隐私窃取 | 会窃取用户短信并对短信进行拦截删除操作，造成用户无法正常接收短信，同时该软件私自下载安装软件，造成流量等资费消耗。 |
|  | 捕鱼达人 HD | 455268 次 | 恶意扣费 | 该软件属于恶意软件，私自发送短信定制扣费业务，同时屏蔽指定号码的回馈短信。 |
|  | Maxthon Browser | 403212 次 | 资费消耗 | 该软件非官方版本代码被恶意篡改，运行后从服务器自动下载恶意代码，可下载未知应用程序安装包，给用户造成资费消耗。 |
| 后台运行、无图标 | Device Statistics | 398624 次 | 隐私窃取 资费消耗 | 内嵌于 ROM 中恶性木马的相关配置文件，盗取用户信息，警惕该软件是否会私自联网下载其他恶意程序。 |
|  | Rope Cut | 380318 次 | 隐私窃取 | 获取用户手机 IMEI、IMSI、SIM 卡序列号、设备序号等手机硬件信息，同时该恶意软件具备修改书签地址，修改浏览器主页，访问指定网址等流氓行为。 |

2012 年恶意软件感染量排名 TOP10

数据来源：360 互联网安全中心（2013 年 1 月）

年度感染次数最高的单款手机恶意软件 TOP10（来源：360 互联网安全中心）

二、2012 年手机恶意广告数据增长情况

除直接危害用户财产、隐私安全的手机恶意软件外，在智能手机特别是 Android 手机平台中存在的恶意广告插件数量也持续激增，据 360 互联网安全中心统计，360 互联网安全中心 2012 年新增恶意广告插件 172688 款，感染用户 483130415 人次。

其中，包括水果忍者、愤怒的小鸟、单机斗地主、鳄鱼小顽皮爱洗澡、泡泡龙等热门游戏的部分版本都被二次打包嵌入恶意广告插件，其中，“水果忍者”以 12191530 人次的感染量居首；手电筒、超酷手电、字体管家等热门工具软件也被打包党修改，嵌入恶意广告插

件。“手电筒”以12017379次的感染量居首。

| 被捆绑应用名称 | | 感染量 |
|--|--|----------|
|  水果忍者 | | 12191530 |
|  Angry Birds | | 9674051 |
|  单机斗地主 | | 7423591 |
|  鳄鱼小顽皮爱洗澡 | | 6521389 |
|  Subway Surf | | 5837919 |
|  疯狂泡泡龙 | | 5456625 |
|  植物大战僵尸 | | 4755020 |
|  TurboFly 3D | | 4677380 |
|  涂鸦跳跳 | | 3401556 |
|  水果连连看 | | 3276725 |

被捆绑恶意广告的手机应用（游戏类）感染量 TOP10 数据来源：360 互联网安全中心（2013 年 1 月）

被捆绑恶意广告的手机应用（游戏类）感染量 TOP10

| 被捆绑应用名称 | 感染量 |
|---|----------|
|  手电筒 | 12017379 |
|  超酷手电 | 6611375 |
|  字体管家 | 5067468 |
|  一键锁屏 | 2972485 |
|  懒人听书 | 2882604 |
|  奇思壁纸 | 2504600 |
|  省电宝 | 2443565 |
|  系统程序卸载器 | 2282713 |
|  丑脸评分 | 2201225 |
|  水墨荷塘动态壁纸 | 1488945 |

被捆绑恶意广告的手机应用（工具类）感染量 TOP10

数据来源：360 互联网安全中心（2013 年 1 月）

被捆绑恶意广告的手机应用（工具类）感染量 TOP10

而在恶意广告的危害分类中，匿名推送和强制下载成为其主要特征，另有部分暗含扣费代码，诱导用户开通付费业务等。

三、2012 年手机垃圾短信、骚扰电话数据增长情况

2012 年中，在用户频遭手机恶意软件、手机恶意广告威胁的同时，垃圾短信、骚扰电话也仍然成为困扰用户的主要安全问题。据 360 互联网安全中心统计，360 手机卫士全年共为 2.2 亿用户拦截垃圾短信 712 亿条，日均拦截近 2 亿条，骚扰电话 352 亿次。日均拦截近 1 亿次。

从用户举报的垃圾短信内容分析，打折推销类占比高达 43% 居首位，欺诈类居其次，占比为 31%，违法类占 23%；从用户举报的垃圾短信发送号码归属地来看，广东、福建、湖南成为全国前三大垃圾短信举报量最大的地区。

而从用户举报的垃圾短信发送方式来看，59% 的垃圾短信通过普通手机号采用点对点方式发送，另有 41% 的垃圾短信仍在利用短信特服号发送。在用户举报的通过点对点方式发送的垃圾短信中，41% 来自中国移动，32% 来自中国电信及电信小灵通号段，27% 来自中国联通号段。

在所有被举报的垃圾短信中，号码 158222846**、131898130**、132437205** 以单日被举报 801、595 次和 485 次，成为年度发送垃圾短信最疯狂的“毒王”号码。

在用户标记的骚扰电话分类中，“响一声电话”以 44% 的比例居首。另有 28% 的骚扰电话为推销内容类，17% 为疑似欺诈类；根据用户标记号码的次数统计，特服号 075595511 以单周 65108 次的用户标记量，成为年度“最敬业”特服号。

关于 2012 年手机垃圾短信、骚扰电话的详细数据分析、特点解读和趋势预测，请参见 360 互联网安全中心另已发布的《2012 年中国垃圾短信、骚扰电话治理报告》（<http://msoftdl.360.cn/mobilesafe/shouji360/report.pdf>）

四、2012 年手机安全焦点解读

在刚刚过去的 2012 年中，手机安全问题正日益凸显，多款新型手机恶意软件的出现，

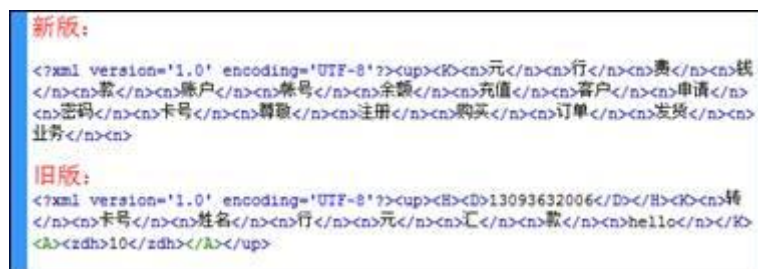
手机僵尸网络的横行、恶意广告插件的激增以及在 Android、iOS 系统中相继出现安全漏洞，都成为了这一年中备受关注的焦点。

焦点 1：僵尸网络横行，感染百万用户

2012 年中，“僵尸网络”成为年度关注度最高的安全焦点之一，在这一年里，360 互联网安全中心相继发现利用手机恶意软件在手机中插入欺诈信息的“短信僵尸”系列恶意软件，以及通过广告弹窗诱骗用户下载未知软件来散播欺诈信息、后台盗取手机号、联系人、照片等隐私的“安卓僵尸网络”系列木马等。

据 360 互联网安全中心统计：截至 2012 年 12 月 31 日，短信僵尸的样本数已超过百款，安卓僵尸网络伪装和篡改的应用均已超过千款，传播范围和影响惊人。

以 360 手机卫士 2012 年 8 月率先截获的“短信僵尸”系列恶意软件为例，其在感染用户手机后可将自己伪装成“Android 服务”后诱骗用户下载安装，而一旦安装，不但能读取用户手机通讯录，还能搜集窃取用户短信中所有带有“卡号、密码……”等数十个关键字的隐私信息，隐蔽上传给木马操控者。



```
新版:
<?xml version='1.0' encoding='UTF-8'?><up><K><n>元</n><n>行</n><n>费</n><n>找
</n><n>款</n><n>账户</n><n>账号</n><n>余额</n><n>充值</n><n>客户</n><n>申请</n>
<n>密码</n><n>卡号</n><n>转账</n><n>注册</n><n>购买</n><n>订单</n><n>发货</n><n>
业务</n><n>
旧版:
<?xml version='1.0' encoding='UTF-8'?><up><H><D>13093632006</D></H><K><n>转
</n><n>卡号</n><n>姓名</n><n>行</n><n>元</n><n>汇</n><n>款</n><n>hello</n></K>
</A><zdh>10</zdh></A></up>
```

“短信僵尸”可在后台窃取包含相应关键字词的短信内容

同时“短信僵尸”在感染手机后，还可自动与服务器连接并接受远程控制，遥控用户手机向其通讯录中的亲友群发短信或拨打电话，利用熟人关系进行防不胜防的网络钓鱼电信

诈骗。

```
if ((str1.equals("M")) && (localNode.getNodeType() == 1))
{
    this.mfasong = 1;
    if (localNode.getNodeType() == 1)
    {
        Element localElement3 = (Element)localNode;
        parse(paramContext, localElement3, paramString);
    }
    j = 1 + 1;
    SMSReceiver.zhongzhi = 1;
    String str3 = this.con;
    String str4 = this.rep; 将诈骗短信发送给指定号码
    smsend(str3, str4);
    String str5 = String.valueOf(this.con);
    String str6 = str5 + ";信息发送成功";
    String str7 = this.dianhua;
    smsend(str6, str7);
}
if (str1.equals("con"))
{
    String str8 = localNode.getFirstChild().getNodeValue();
    this.con = str8;
}
if (str1.equals("rep"))
{
    String str9 = localNode.getFirstChild().getNodeValue();
    this.rep = str9;
}
```

通过短信僵尸在后台自动将欺诈短信发送给指定号码



短信僵尸分别伪装成动态壁纸、电源管理的应用传播

而为更为有效的盗取手机隐私，“短信僵尸”还具备强制开机自启动、强制联网，激活设备管理器，使用户通过常规方式无法删除。

另一“安卓僵尸网络”系列恶意软件，则同样通过篡改热门应用，嵌入恶意代码后重新打包的方式传播，一旦感染手机能够联网接收黑客远程下发的指令执行不同的恶意行为。监测数据显示，2012年中，这一系列恶意软件累计感染用户453万次，成为年度感染量最高的手机恶意软件之一。

如据360互联网安全中心对“僵尸网络”系列恶意软件的云端控制行为进行深入分析后发现，在目前已可查杀到的“僵尸网络”木马中，49.6%可由云端控制消耗用户上网资费。35.2%会窃取用户手机中的隐私信息，13.3%会进行恶意扣费，1.9%向手机推送欺诈信息。



僵尸网络木马的传播和危害（来源:360 互联网安全中心）

焦点 2：系统漏洞频发，涉及数百款机型

2012 年中，更多手机恶意软件还开始利用手机平台中存在的系统漏洞来进行攻击，如 2012 年 10 月，三星 Galaxy 系列手机被曝存在拨号指令漏洞，可被利用使用户误格手机；三星、魅族、小米等手机的芯片组被曝存在内核驱动漏洞，直接涉及如 Galasy S3、Note2 等数百款主流机型。

一系列安全漏洞的出现，也使得手机终端厂商开始愈发重视设备安全问题，如在一系列漏洞出现之后，终端厂商和芯片厂商都在第一时间做出了快速响应，升级系统版本、提供修复补丁等解决方案等，360 手机卫士也相继推出修复补丁，避免用户因手机存在漏洞而存在遭黑客攻击的风险。



针对多款智能手机曝出的系统漏洞，360 均在第一时间提供了紧急解决方案

焦点 3：隐私安全危机，濒临爆发临界点

2012 年中，在智能手机用户持续增长的同时，隐私安全问题也愈发引人关注，大量因

手机丢失导致隐私泄漏的案例，和多款手机 APP 应用被曝存在后台收集用户通讯录、手机短信、监听通话内容甚至录音的行为，使得隐私安全问题已经濒临大规模爆发的临界点，任其发展后果将十分严重。

例如，2012 年中，360 手机卫士相继查杀如专门盗取短信、IMEI(手机串号)、Google 账号等隐私信息的 DroidDreamLight 系列手机恶意软件，可窃听通话、盗取短信内容的 X 卧底系列间谍软件最新变种等，其可通过巧妙伪装植入用户手机，获取录音、联网等权限后盗取用户隐私，行踪隐蔽，让用户很难察觉。

```
public static final String COUNTRY = "Country";
public static final String CellID = "CellID";
public static final int GET_INFO_CMD = 2;
public static final String IMEI = "IMEI";
public static final String IMSI = "IMSI";
public static final String LAC = "LAC";
public static final String LANGUAGE = "Language";
public static final String Model = "Model";
public static final int PARAMS_CMD = 1;
public static final String ProtocolVersion = "2.0";
public static final int SEND_OK = 0;
public static final int SEND_RECEIVE_ERROR = 2;
public static final int SEND_RECEIVE_SUCCESS = 1; 获取用户 IMEI 等相关信息
public static final String SMSCenter = "SMSCenter";
public static final int UPLOAD_DATA_CMD = 3;
public static final int HttpConnectionConnectTimeout = 60000;
public static final int HttpConnectionReadTimeout = 60000;
private boolean cancel = 0;
private Context context;
private HttpHandler httpHandler;
private Transaction transaction;
private Handler uiHandler;

    this.uploadFileFinish = 0;
    this.uploadFileSuccess = 0;
}

private void setUploadStatus(boolean paramBoolean)
{
    this.uploadFileFinish = 1;
    this.uploadFileSuccess = paramBoolean;
}

private boolean uploadData(ContactHandler paramContactHandler)
{
    String str1 = InetAddress.getByName(this.context).getHostAddress();
    int i = Log.d("DGL", str1);
    StringBuilder localStringBuilder1 = new StringBuilder();
    File localFile1 = this.context.getFileStreamPath("data");
    String str2 = localFile1.getName() + ".txt";
    this.filePath = str2;
    StringBuilder localStringBuilder2 = new StringBuilder();
    File localFile2 = this.context.getFileStreamPath("data");
    String str3 = localFile2.getName() + ".txt";
    boolean bool1 = paramContactHandler.createDataFile("data");
    if (bool1)
    {
        String str4 = this.filePath;
        if (zipAndEncryptFile(str4, str3))
        {
            String str5 = this.filePath;
            deleteFile(str5);
            bool1 = !bool1;
        }
    }
}
```

隐私大盗木马专门窃取 Google 账号、短信、IMEI 等相关信息

为此，2012 年初，360 互联网安全中心针对用户面临的手机隐私安全问题，率先提出“四不三必须”倡议，所谓“四不”是指：不该看的不看、不该存的不存、不该传的不传、不该用的不用、“三必须”是指移动应用开发者及厂商应该特别注意“一切行为必须明示，尊重用户的知情权和选择权；必须经过用户许可，软件不能未经授权上传个人隐私信息；必须对手机的用户隐私信息负责”，以此提高对用户隐私安全的保护。

同时，针对 2012 年中连续出现大量用户因手机丢失导致隐私泄漏的案例，更多用户已

为手机安装如 360 手机卫士等专业防盗软件，丢失后及时通过定位找回手机，远程销毁隐私数据。

焦点 4：骚扰问题突出，形成黑色产业链

在因手机恶意软件、系统漏洞导致的安全隐患频发同时，手机用户还面临着严重的骚扰问题，垃圾短信、骚扰电话持续泛滥，轰炸密度也更为集中，在发送方式上也在发生变化。

例如，2012 年中，为躲避运营商的监管，不法分子大量采购非实名手机卡，通过“点对点”方式来发送垃圾短信，并不断变化发送号码。

同时，不法分子还出现通过一些手机改号软件，或利用某些网络 IP 电话中存在的可“匿名呼叫”的漏洞、以及“短信僵尸”等手机木马等，伪装成公安、法院、甚至机主亲友的真实号码实施欺诈的现象，由于具有极高的迷惑性，比普通的垃圾短信、欺诈电话更具危害。

在 2012 年中，垃圾短信、骚扰电话的黑色产业链条还已形成了一条密集的黑色产业链，其主要由四部分构成：电话号码等个人信息的买卖；用于短信群发的“卡资源”渠道销售；经营垃圾短信群发、语音电话推销服务的公司；广告主为垃圾产业持续提供大量资金支持。

由于整个产业链中存在完整的需求、利益交易，使得尽管近年来工信部等政府主管部门、运营商等已分别从立法监管和治理层面打出重拳，但在目前仍未能得到根治。打击黑色产业链是治理垃圾短信、骚扰电话的最紧迫任务和解决这一社会难题的根本方略。

为此，360 互联网安全中心已在 2012 年 1 月初发布国内首份垃圾短信、骚扰电话治理报告，报告呼吁政府、运营商、手机安全厂商、用户及媒体等全社会应共同努力，加强对骚扰信息的治理工作，形成四大机制，包括：由安全厂商与用户共同完成垃圾短信与骚扰电话的用户反馈机制；由公安、运营商、安全厂商、用户建立骚扰证据链的回溯机制；由公安、

运营商等共同完成针对恶意骚扰行业的惩戒机制；以及由政府、行业协会和媒体共同建立的监管监督机制。通过群策群力，共建绿色的移动通信环境。

焦点 5：恶意广告泛滥，严重损害用户

2012 年中，各种移动应用和手机广告出现爆发式的增长，但在这一背景下，一些应用开发者和不良广告商却利用恶意广告插件，肆意推送各种广告。极大地伤害了用户体验和利益，也严重影响到移动互联网的健康发展。

例如，2012 年中，360 互联网安全中心累计截获 172688 款手机恶意广告插件，其多以推送消息、悬浮窗口的形式出现在手机通知栏或 APP 应用窗口中，引诱用户点击自动下载软件，甚至进行恶意扣费和盗取用户隐私等。

同时，恶意广告在展示方式上也不断发生变换，除通过 Android 手机的消息栏不断推送消息外，甚至伪装成其它应用的悬浮通知来诱骗用户点击，一旦点击将自动下载软件，消耗用户流量同时赚取推广费用，严重干扰用户正常使用并侵犯了用户的选择权益。

焦点 6：iOS 安全危机 非越狱也存在

2012 年中，此前被认为因相对封闭，而安全系数较高的 iOS 平台中也开始出现一系列安全问题，如在同年 8 月，法国黑客发现的 iOS 短信漏洞，可将诈骗短信伪装成合法的身份，诱骗用户接收、点击其中的短信链接等，由于这一漏洞在非越狱手机中也同样存在，更使用户极易落入短信欺诈陷阱之中。

同时，随着大量用户开始购买和同时使用多台 iOS 设备，如 iPhone，iPad，Mac 等，在信息同步过程中也开始出现一系列安全问题，如一旦黑客成功破译 Apple ID 账号，可导致用户的 iMessage 信息，安装的应用列表，以及 iCloud 数据被轻易同步到另外的 iOS

设备上，直接盗取隐私信息等。

焦点 7：扩展传播形式 利用二维码、短网址传播

在 2012 年之前出现的手机恶意软件，更多通过第三方应用商店和手机论坛，以及内置在水货手机的 ROM 中传播，而从 2012 年开始，黑客又开始盯上逐渐流行的二维码、微博短网址技术，利用其隐蔽性来进行传播。

相比应用商店、论坛等传播途径，由于二维码、短链接在转换生成过程中已隐蔽掉了其的真实路径，在未做安全检测的状态下，扫描下载时极易误下到被黑客所伪装的恶意软件。

如“广告偷窥者”系列 (a.privacy.Counterclank)，通过嵌入到美女壁纸、明星靓照包装、热门主题等，利用二维码和微博等形式传播，通过诱人标题引诱点击下载，借此提高隐蔽性。为此，360 手机卫士也于 2012 年 10 月率先推出安全二维码扫描功能，阻止黑客利用二维码方式传播恶意软件。



五、2013 年手机安全趋势预测

趋势 1：安全威胁将向更多平台延伸

在 2012 年中发现的手机安全威胁，还更多集中在 Android、Symbian 两大智能手机平台中，新增款数、感染次数惊人。但在 2013 年中，360 互联网安全中心预计，为扩展危害范围，安全威胁还将向包括平板电脑、智能电视、iOS 设备上延伸。

例如，目前市场中已有大量采用 Android 系统的平板电脑、智能电视产品，作为同样可安装第三方应用，具备恶意软件运行能力的载体，安全问题也不容忽视，如在其中存储的信息安全问题，在使用 3G 上网时流量、费用的安全问题等。

正如在报告“年度焦点”中的对 iOS 平台安全问题的解读，伴随越来越多 iOS 安全隐患的出现，这一平台的安全形势也不容乐观，甚至在 2013 年中，可能会相继出现多款专门针对此平台的手机恶意软件。

趋势 2：恶意软件的隐蔽性将空前加强

近年来，伴随手机恶意软件款数、感染用户的激增，用户的安全意识也在逐步增强，如会定期查看已安装的应用列表，仔细查阅软件的授权提示等。而为躲避用户对其的察觉，以能持续在手机中“潜伏”，大量手机恶意软件已开始不断增强对自身的隐蔽性，360 互联网安全中心预测，在 2013 年中，其隐蔽性还会持续加强。

例如，未来手机恶意软件将通过虚假授权提示，在安装前、和运行过程中试图隐瞒

其实际将获取的权限列表，强行获取通讯录、通话等权限。

同时，间谍软件还会采用了更为灵活（在用户易忽视的状态，如只在手机充电时，锁屏时运行）等，专门选择用户不易察觉的时间，使用户极易忽视其在后台的存在，长期运行，通过服务器指令执行恶意扣费、隐私窃取等行为。

趋势 3：手机支付、网购将成黑客的攻击重点

报告预测，伴随近年来通过手机网购、支付人数的增加，未来黑客的攻击目标将瞄准支付消费安全，例如，一旦手机支付用户感染已具备通过监听键盘记录和拦截篡改网络数据包来窃取用户支付账户密码等能力的恶意软件，其便可以通过模拟按键来模拟用户操作以达到恶意消费或转账的目的。

而为进一步威胁用户的支付安全，黑客还将未来通过技术手段设置虚假支付环境，如引导用户访问“钓鱼”网站，模拟高度逼真的买卖过程，骗取用户完成一系列操作，通过截获用户的上行数据破解账户信息，全程记录下用户输入的所有信息来直接获取经济利益。

来自 eDigitalResearch 的一份最新的调查结果显示，尽管大多数人已了解并愿意使用手机支付等功能，但其中有半数以上用户对其安全性表示担心，为此，在手机支付日益兴起的同时，安全问题将尤为关键。

六、手机安全建议及解决方案

纵观 2012 年的手机安全形势，从持续激增的数据，和不断出现的新特点，都预示着用户将面临更多，更为严重的安全威胁。为此 360 互联网安全中心强烈建议广大手机用户，

提高手机安全意识，通过如下四大建议确保用户手机安全。

1. 尽量选择正规渠道购买手机

报告显示，水货手机是目前木马和恶意软件的主要传播源头，其多会在出货前被“刷机”植入吸费、流氓推广木马等，而由已嵌入系统底层，很难通过常规方式卸载清除。为此，360 手机安全专家建议用户在购买新手机时应尽量选择大型正规卖场购买手机，购买手机后，建议安装如“360 手机卫士”等专业安全产品对其进行扫描，避免手机暗藏恶意软件。

2. 选择正规站点、渠道下载应用

报告指出，通过下载应用而感染恶意软件的比例惊人，为保护用户的正常下载安全，360 安全专家建议用户尽量选择专业、可信的应用市场、官网，以及如 360 手机助手、360 软件宝箱等经过安全检测的渠道下载应用。

3. 下载安装应用前，细心留意应用权限

当前，通过篡改、伪装正常应用威胁手机安全的恶意软件，实际会在安装权限中有细微体现，如要求获取的权限与正常应用的获取列表有明显不同，如莫名要求得到敏感高危权限等，为此，建议用户在下载安装应用前，细心留意应用权限，避免被获取后威胁手机安全。

4. 安装手机安全产品，为手机安全保驾护航

为进一步全面保护手机安全，360 手机安全专家建议用户选择安装 360 手机卫士 (<http://shouji.360.cn>) 等具有云安全智能拦截功能的手机安全软件，进行主动防御与一键查杀，远离吸费、流氓推广、盗号和隐私窃取软件，全面保护手机安全。