Android 手机游戏安全状况报告

（2013.3）

360 安全中心

引言

手机游戏已成为移动互联网最早一批形成成熟商业模式的产业，特别是在开源性和开放性都相对更高的 Android 系统平台下，游戏款数、用户数、市场收入逐年激增，据《2012 年中国游戏产业调查报告》显示，去年中国移动游戏用户达 0.89 亿人，同比增长 73.7%；移动游戏市场销售收入达 32.4 亿元，同比增长 90.6%。

但随着手机游戏应用量的剧增，国内手机游戏应用乱象丛生，通过伪装篡改热门游戏嵌入木马、在游戏中捆绑恶意广告插件来构建谋利链条，使不少手机游戏用户频频上当，落入吸费、隐私窃取、流氓推广陷阱之中。

如 2013 年央视 315 晚会上曝光的红警世界联盟等游戏收集用户手机号码，手机串号，用户谷歌账号，以及用户手机上的通讯录和地址等，直接威胁用户的隐私安全的案件就引发了用户关注，国内 Android 手机游戏整体安全状况不容乐观……

为此，360 安全中心在 2013 年 3 月发布《中国 Android 手机游戏安全状况报告》，通过截至 2012 年 1 月至 2013 年 2 月积累的分析数据，以专项研究形式全方位、多角度地剖析当前国内手机游戏安全状况，为有关部门、媒体和用户提供有力的数据参照。

摘要

- 2012 年全年及 2013 年 1 月、2 月中，360 安全中心共截获到伪装、篡改 Android 游戏的手机木马及恶意软件（以下简称：游戏木马）、恶意广告插件共 134927 款，感染用户近 2 亿人次。

- 57%的游戏木马存在安装后向用户推送广告、后台下载软件消耗用户上网流量的行为，26%存在后台发送短信恶意扣费的行为，14%会收集、上传用户隐私，2%存在系统破坏及其它恶意行为。

- 在通过对 1000 款热门游戏进行抽样的权限分析后发现，其中 41.2%存在调用过多权限，如在非必要情况下，读取用户通讯录、短信、位置信息的情况。

- 45.2%的游戏木马会通过应用商店、手机论坛诱骗用户下载，另有 23.4%存在于“ROM 刷机包”中， 另有 16.5%通过二维码、短网址传播，13.2%通过短信内链接。1.7%通过其它方式传播（如蓝牙等）。

- “植物大战僵尸”成为被伪装、篡改次数最多的 Android 手机游戏，有 222 个经过二次打包的非官方版本，存在木马及恶意广告插件。

- 在 1414 个不同版本的“水果忍者”中有 566 款均为存在恶意行为，其也以单月 1615815 次的总感染量成为感染量最大的 Android 手机游戏。

目录

免责声明：

本报告为 360 安全中心发布的研究数据和分析资料。报告针对 2012 年中国 Android 手机游戏安全状况进行统计总结，并发布安全趋势研究结论。

本报可提供给任何个人、政府相关部门及行业机构、企事业单位查考，但对于本报告所阐述之内容、数据及分析结果，360 安全中心不承担与此相关的一切法律责任。

报告正文

一、国内手机游戏安全状况

1.木马疯狂伪装、篡改 Android 手机游戏，感染用户已近 2 亿人次

2012 年全年及 2013 年 1 月、2 月中，360 安全中心共截获到伪装、篡改 Android 游戏的手机木马及恶意软件（以下简称：游戏木马）、恶意广告插件共 134927 款，感染用户近 2 亿人次。其中截获到手机木马样本 60718 款，恶意广告插件 74209 款。

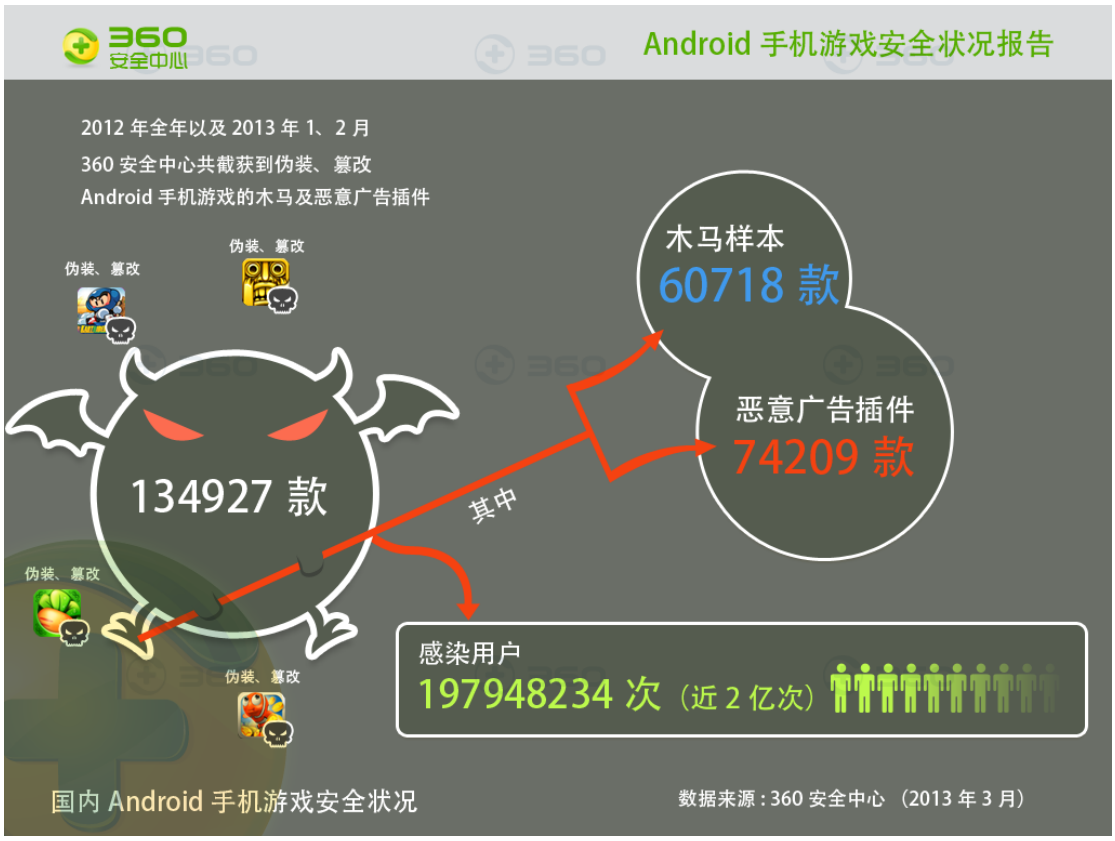

图 1　2012 年全年及 2013 年 1、2 月 Android 手机游戏安全状况

2. 资费消耗成游戏木马主要危害，推送广告、后台下载软件

57%的游戏木马存在安装后向用户推送广告、后台下载软件消耗用户上网流量的行为，26%存在后台发送短信恶意扣费的行为，14%会收集、上传用户隐私，2%存在系统破坏及其它恶意行为。

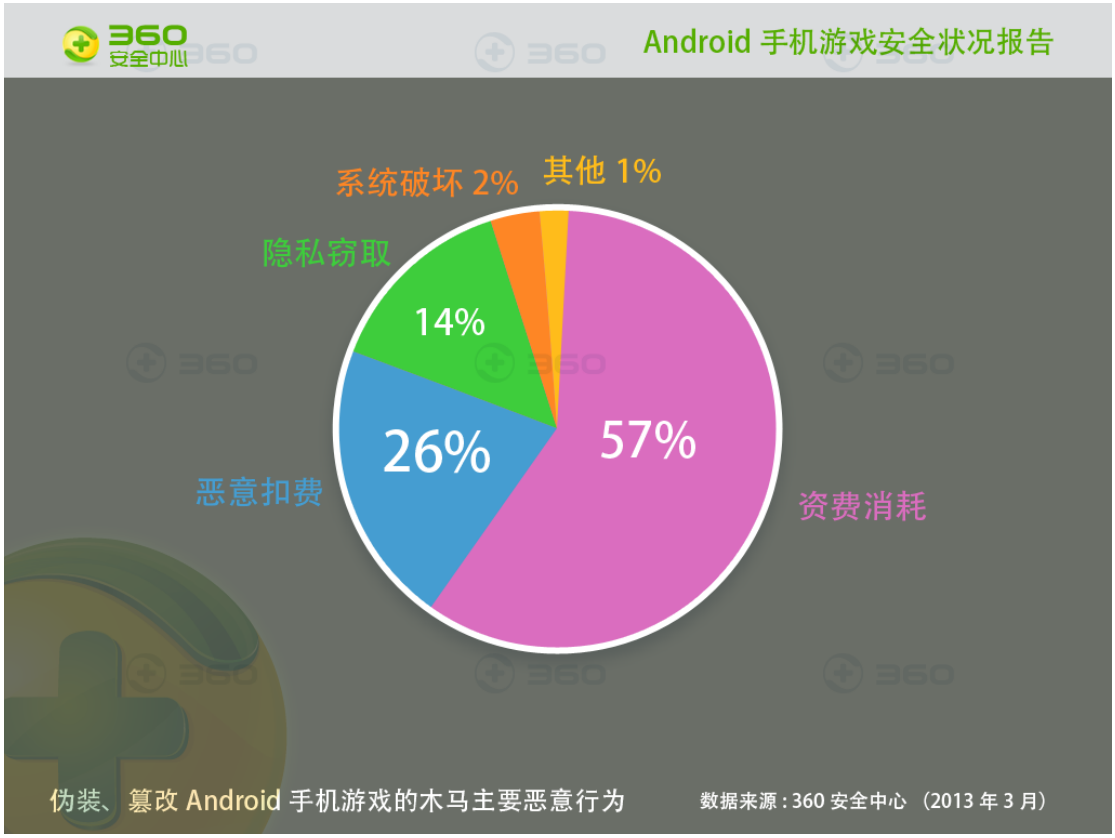

图 2　伪装、篡改 Android 手机游戏的木马主要恶意行为（来源:360 安全中心）

3.手机游戏滥用权限现象严重，近四成读取非必要权限

除确认存在恶意行为的手机木马、恶意广告插件外，360 安全中心还分析发现，大量 Android 手机游戏存在在非功能必要情况下调用过多权限的情况，如通过对 1000 款热门手机游戏进行抽样的权限分析后发现，其中 41.2%存在调用过多权限，如在非必要情况下，读取用户通讯录、短信、位置信息的情况。

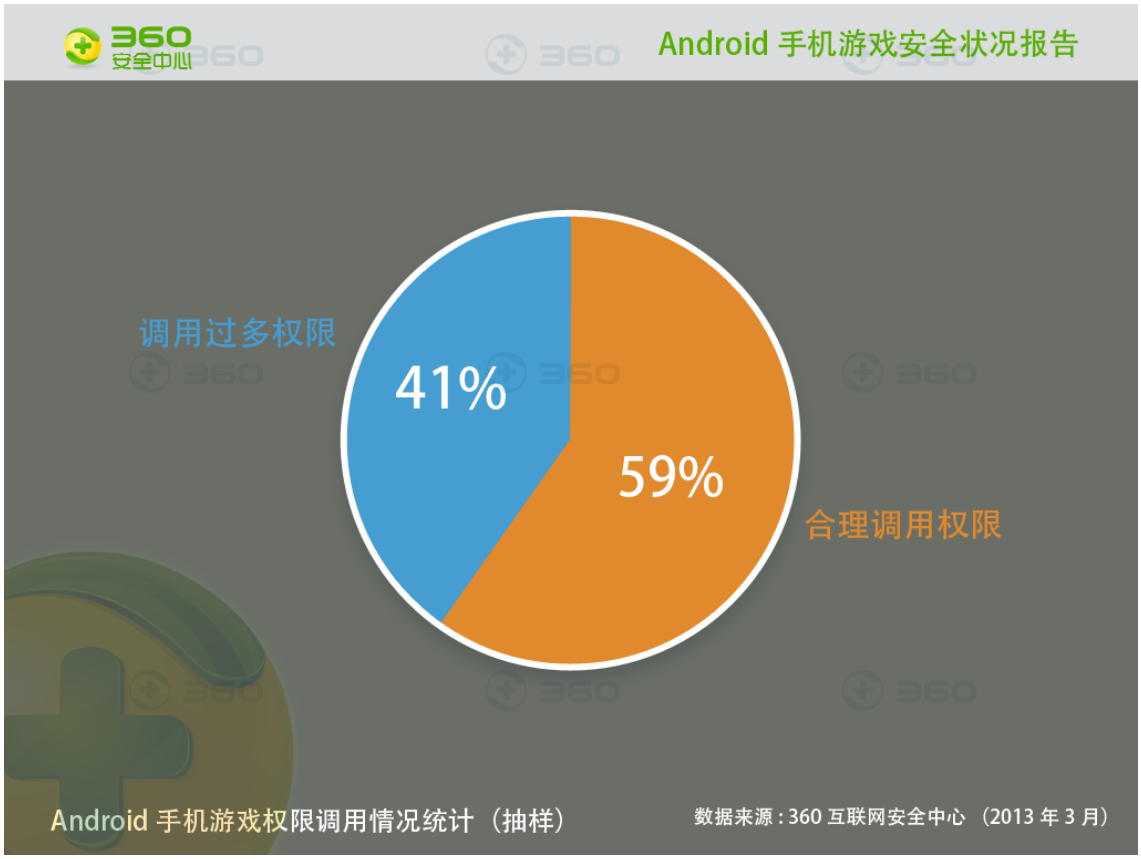

图 3　Android 手机游戏权限调用情况统计/抽样（来源:360 安全中心）

4.手机应用商店、论坛及二维码成游戏木马的主要传播途径

在 360 安全中心截获的 134927 款伪装、篡改 Android 手机游戏的木马、恶意广告插件中，45.2%的游戏木马会通过应用商店、手机论坛诱骗用户下载。

另有 23.4%存在于“ROM 刷机包”中， 另有 16.5%通过二维码、短网址传播，13.2%通过短信内链接，1.7%通过其它方式传播（如蓝牙等）。

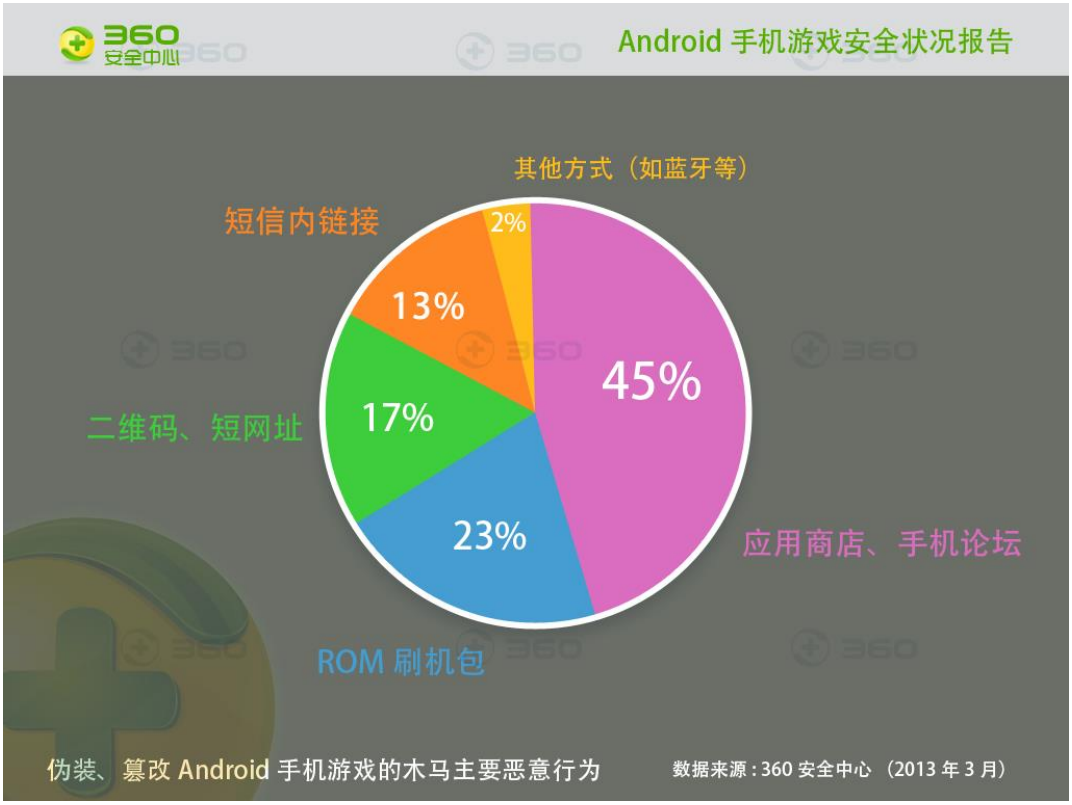

图 4 伪装、篡改 Android 手机游戏的木马主要恶意行为（来源:360 安全中心）

5.篡改目标盯准热门手机游戏，最多篡改版本超两百款

在传播过程中，木马为提高其诱骗用户下载、安装的几率，通常选择热门游戏作为伪装和篡改对象，如在被伪装、篡改次数最多的游戏木马 TOP20 中，便包括“植物大战僵尸”、“疯狂泡泡龙“、”“英雄守卫“、“水果忍者”、“最后的防线”等。

其中，“植物大战僵尸”成为被伪装、篡改次数最多的 Android 手机游戏，有 222 个不同版本的相关游戏为被伪装、篡改版本，存在手机木马或恶意广告插件，一旦下载安装将使用户的手机话费、隐私面临安全威胁。

被伪装次数最多的游戏木马 TOP20（来源:360 安全中心）

6.篡改热门游戏感染量惊人 篡改“水果忍者”感染量超 160 万

手机木马及恶意广告插件伪装、篡改同一款游戏，并分别衍生出数十、数百个版本诱骗用户下载安装的情况，极大增加了其感染用户的几率和量级，以 2013 年 2 月的感染量数据为例，在当月伪装、篡改感染量最大的游戏木马 TOP20 中，“水果忍者”以 1615815 次的总感染量成为感染量最大的 Android 手机游戏。

“植物大战僵尸”、“神庙逃亡 2”、“捕鱼达人”、“超级玛丽 “、” 疯狂泡泡龙” 等也以单款超过十万的感染量位列其中，篡改热门游戏的感染量惊人。

伪装、篡改感染量最大的游戏木马 TOP20/2013 年 2 月单月统计（来源:360 安全中心）

二、国内手机游戏安全状况剖析

1. 手机应用下载渠道中，山寨、盗版游戏数量众多

在目前的 Android 手机游戏下载渠道中山寨、盗版手机游戏数量众多，且内容鱼龙混杂，由于消费者追捧热门应用的心理，加上普通人难以区分正版盗版，以及应用市场安全监管能力的不足，令恶意广告和病毒木马上传，利用传播到用户手机中。

如以热门游戏“水果忍者”作为搜索对象，可分别从各应用商店、论坛中搜索下载到超过 1414 个不同版本， 除部分标注为官方版外，还有大量以H D版、Fans 版、终极免费版等名义推荐下载，让用户难以分辨和选择。

但经实测发现，其中 566 款均为存在恶意行为，恶意软件比例高达 40%，一旦下载安装相关游戏，用户手机将为黑客远程控制，自动下载软件及弹出恶意广告，以及控制手机外发恶意扣费短信、上传手机隐私等，由于应用商店、论坛中山寨、盗版游戏数量众多且暗含安全风险，渠道安全已不容忽视。

2.游戏滥用权限情况突出，存在大量潜在安全隐患

在直接伪装、篡改手机游戏，嵌入恶意代码进行危害外，大量手机应用引起存在“越权”调取关键权限的行为，同样存在大量潜在安全隐患。

如以热门游戏“打地鼠”为例，作为一款单机的普通手机游戏，却实际会在安装、运行后监控电话、读取手机号码、IMEI 号码且获得发送短信的权限，在与之功能无必要关联情况下掌握过多权限，尽管未利用其进行恶意破坏，但已具备和存在利用控制权限进行恶意扣费、窃取隐私的能力。

另一款名为“忍术训练”的单机手机游戏，在安装后还会读取位置信息，且获得可随时开启/关闭 wifi、开启/关闭 GPRS 网络的权限，一旦其为黑客利用，可操控其自动下载软件，甚至连接到存在安全风险的 Wifi 网络中等，存在大量潜在隐患。

3. 游戏付费过程缺乏规范化，屏蔽付费业务短信

伴随 Android 游戏商业模式的日益成熟，越来越多的手机游戏开始引用增值功能，如付费道具、虚拟货币等，但受经济利益驱动，目前有部分手机游戏的付费流程存在不规范，甚至屏蔽运营商的业务确认短信来强行扣费的情况。

如以热门 Android 手机游戏“武林奇侠”为例，这款带有付费道具的手机游戏便在支付流程上缺乏规范甚至存在隐患 ,如其会在支付游戏道具过程中屏蔽指定运营商号码的回馈短信，点击付费按钮后即可完成扣费，这种借助安卓系统的开放性，更改底层数据来拦截扣

费短信，剥夺用户知情权，对产业环境破坏较大。

三、手机游戏安全防护措施

通过本次 Android 手机游戏安全状况报告中的数据、现状剖析可以看出，手机木马、恶意广告插件的肆虐，正在严重威胁到手机游戏用户的隐私、话费安全，为此 360 安全中心强烈建议广大手机用户，提高手机安全意识，通过如下五大建议确保手机安全。

1 .从正规的渠道购买手机。水货手机是目前手机木马、恶意广告插件的主要传播渠道，由于刷入或内置入 ROM 的程序通常很难用常规手段卸载或清除 ,建议用户尽量通过正规渠道购买手机，获得放心保障。

2 .从正规安全的渠道下载应用。建议用户可通过 360 手机助手等安全、专业的下载平台下载应用，这些应用下载平台均经过 360 手机卫士的安全检测，且收录游戏数量更多、质量更高，确保下载安全。

3 .不要见码就刷。通过本次 Android 手机游戏安全状况报告可以看出，二维码已成为手机木马的另一主要传播渠道，手机用户最好安装如 360 手机卫士等具备二维码恶意网址拦截的手机安全软件进行防护，降低二维码染毒的风险。

4 .安装专业安全软件，为全面确保手机用户的游戏安全，手机用户可下载安装如 360 手机卫士等手机安全软件定期给手机进行体检和病毒查杀，另外，手机用户还可以使用该软件的隐私权限监控、软件联网管理等功能，及时监控恶意软件的过度权限要求和后台私自联网等恶意行为，阻止木马恶意行为，保护手机安全。

5 .不要随意点击短信链接。据 360 安全中心分析，目前有 13.2%的手机游戏木马通过短信链接传播，为此建议用户切勿随意点击收到的短信链接，及时安装 360 手机卫士并开启恶意网址检测，避免落入欺诈陷阱。

通过建议用户及时关注@360 手机卫士 官方微博，360 安全中心将随时对最新的手机安全威胁进行预警，曝光新近出现的伪装、篡改游戏及其它工具类应用的手机木马，提供安全建议，为您的移动生活保驾护航。