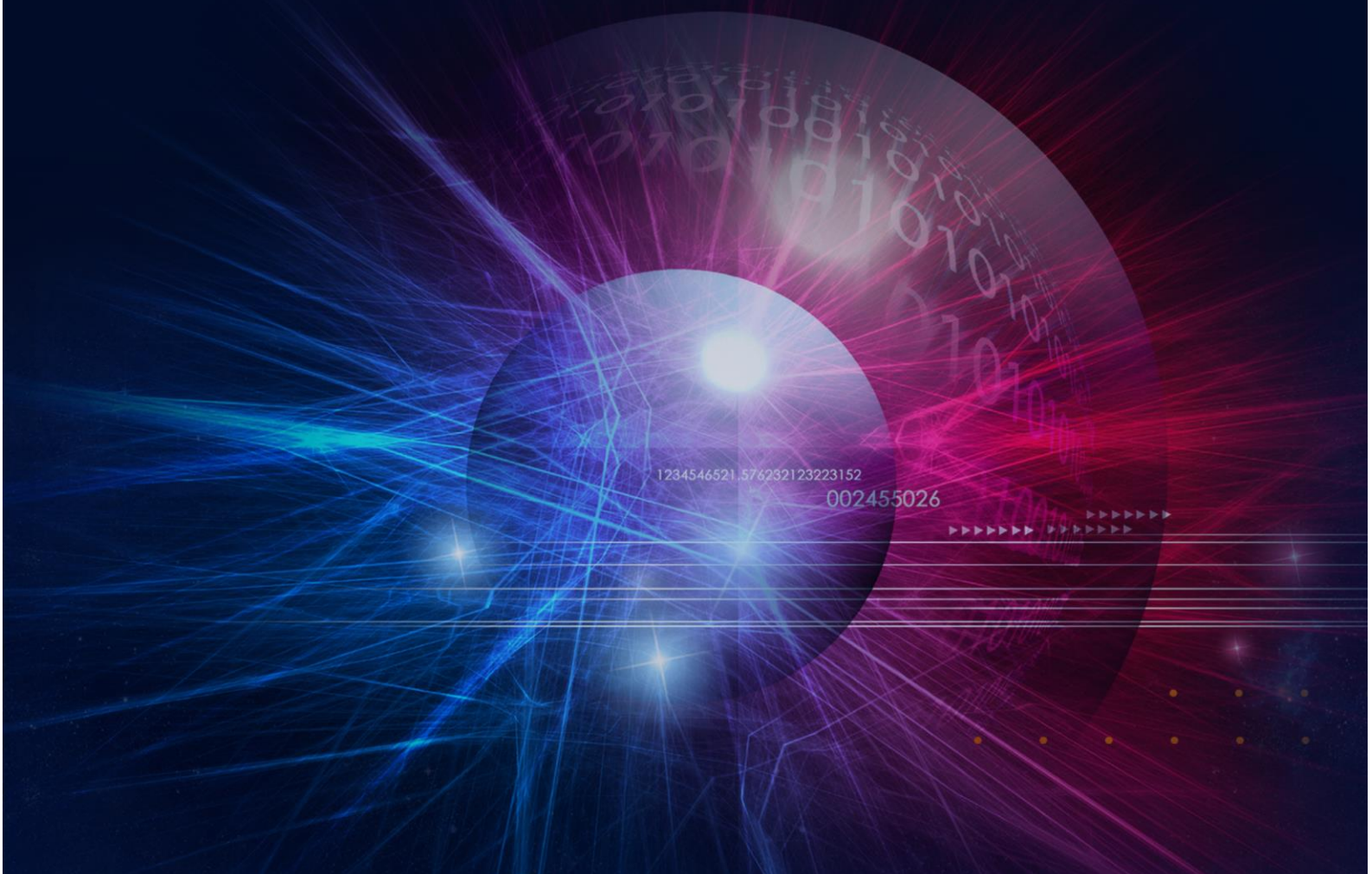
2015移动安全病毒年报



阿里聚安全

阿里安全开放平台

摘 要

- 2015 年，18%的 Android 设备感染过病毒木马，阿里聚安全共查杀 3 亿个病毒，为用户抵御了大量的安全风险。
- 阿里聚安全病毒样本库新增 1005 万病毒样本，月均涨幅达 12%，病毒检测能力持续增强。总病毒样本库中，以恶意扣费类病毒样本为主，占比 67%。
- 52%的用户感染过流氓行为类病毒，这类病毒匿名弹窗、恶意推送广告、私自下载软件，对用户造成极大体验困扰和安全隐患。
- 广东地区的用户感染病毒最多，占全国总感染量的 14%，其他感染量靠前的还有江苏、浙江等。病毒感染的区域总体呈现出以中东部发达省份为主，西部为辅的格局，病毒制造者重点依然瞄准东部沿海手机用户来掘金。
- 18 个行业的 Top10 应用中，95%的应用都存在仿冒应用，平均每个应用有 66 个仿冒。其中社交类 Top10 应用的仿冒量最高，平均含 500 个仿冒。这些仿冒应用大部分都有恶意扣费行为，用户需谨慎使用，并在在官方渠道下载正版软件。
- 71%的仿冒行为伪造正版软件的应用名称，仿冒正版软件包名的占 15%，两者同时仿冒的占 14%。仿冒软件利用与正版应用相似的特征，诱导用户下载安装，之后实施恶意的病毒行为，对用户的危害极大，用户需谨慎使用。
- 2015 年诈骗事件层出不穷，诈骗短信如“积分兑换”,“银行客户端升级”、“车辆违规”、“老公出轨”等。钓鱼木马诱骗用户网银信息，诱导用户安装“短信拦截马”进一步行骗。短信拦截马全年感染 200 万用户，并已形成社工、木马开发、多渠道传播、洗钱分赃等一条完整的非法产业链。
- 加固木马持续爆发，病毒量达 2155 万，这类木马使用 Apkprotect 等第三方加固技术躲避查杀，大大提高了防御成本。
- 色情诱惑类病毒木马重出江湖，数月内感染了近 100 万用户。木马利用诱惑性应用图标和低俗内容诱导用户下载安装，利用加固技术躲避查杀，且长留在用户手机中无法卸载，存在恶意扣费、窃取隐私、静默安装推广应用等恶意行为。
- 2015 年病毒木马攻击手法的专业性较去年有明显提升，尤其是对社会工程学的利用使得在移动平台上的钓鱼诈骗手法到了登峰造极的地步，这些都使得传统的移动端病毒拦截技术遭遇到了前所未有的挑战。此外，iOS 平台 XcodeGhost 事件也只是一个开始，后续定会出现利用相关漏洞进行攻击的病毒。

目 录

第一章 2015 年病毒和仿冒应用发展分析

在移动互联网高速发展的今天，移动设备给人们的生活带来的诸多便利与变革，但也时刻面临着不同程度的安全风险，其中病毒木马是最为普遍且有效的攻击方式之一。不同于以往 PC 时代攻击场景相对独立的情况，移动设备作为人们与外界进行绝大部分信息交流的重要工具，同时也提供了更多被黑客利用的机会。另一方面，随着移动支付的普及，以及移动设备承载了几乎所有的隐私信息，使得移动设备成为黑客实施以经济利益为目的理想的攻击对象。

根据阿里移动安全的分析统计，2015 年移动恶意代码数量和用户感染量虽然呈现出一定程度的下降趋势，但全年仍有 18%的设备感染过病毒，且病毒木马攻击手法的专业性较去年有了明显的提升，例如利用系统漏洞的攻击和安全加固技术的防御，尤其是对于社会工程学的利用使得在移动平台上钓鱼诈骗手法几乎到了登峰造极的地步，这些都使得传统的移动端病毒拦截技术遭遇到了前所未有的挑战。

除 Android 平台以外，2015 年苹果的 XcodeGhost 事件也打破了 iOS 平台不会被病毒染指的神话。鉴于 iOS 系统漏洞曝光越来越频繁的现状，我们相信 XcodeGhost 事件只是一个开端，后续必会出现利用相关漏洞进行攻击的病毒。

1.1 18%的 Android 设备感染过病毒

2015 年度，Android 平台约 5.6 台设备中就有 1 台染毒，设备感染率达 18%，阿里聚安全病毒扫描引擎共查杀病毒总量 3 亿，病毒木马的查杀帮助用户抵御了大量的潜在风险。

2015 年，病毒查杀量和感染设备量呈下降趋势，下半年病毒查杀量比上半年下降 23%，下半年感染设备量比上半年下降 38%，病毒数量虽有所减少，但总量依然十分庞大，2015 年月均病毒查杀量达 2248 万次，网民和安全服务提供商仍不可掉以轻心。

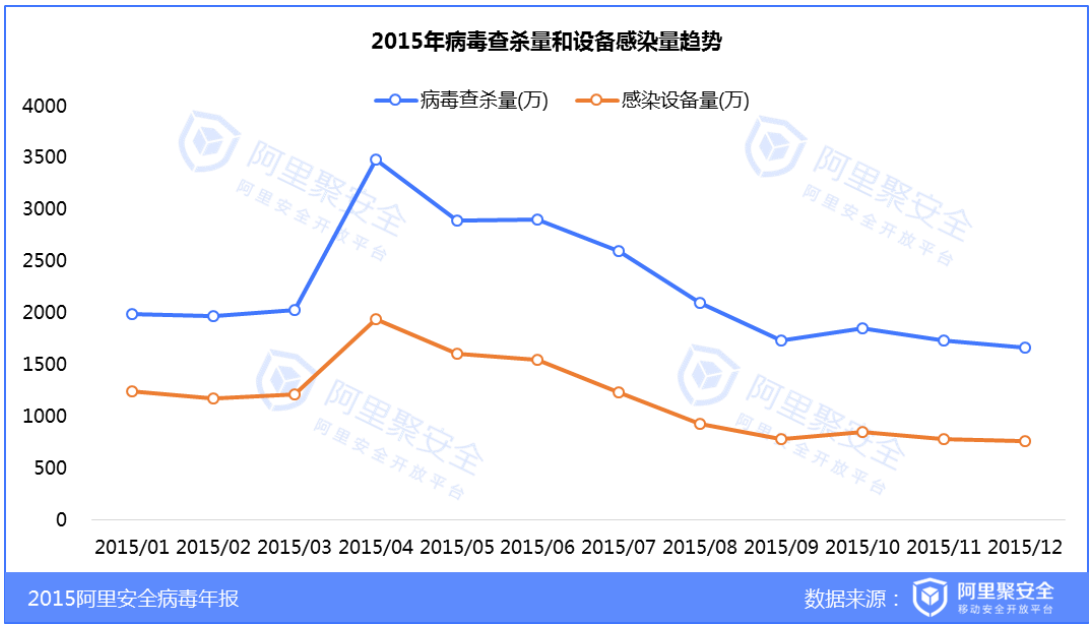


图 1 2015 年病毒的设备感染量和查杀量

虽然病毒查杀量和感染用户量趋于下降，但阿里聚安全病毒样本库的规模仍持续增长，2015 年度新增病毒样本量 1005 万，病毒样本量月均增长率为 12%，总体平稳增长。

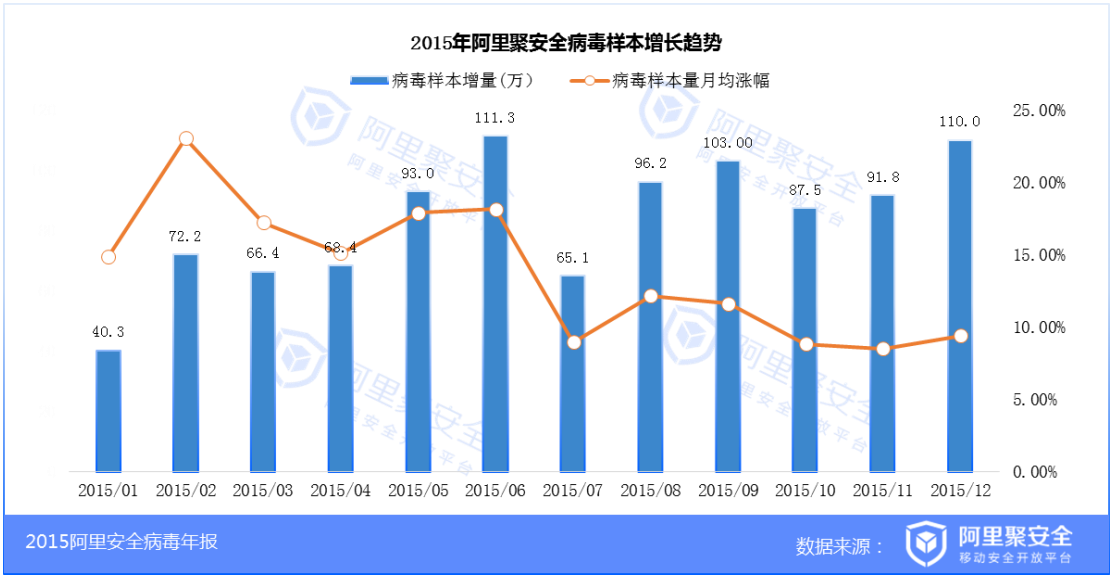


图 2 阿里聚安全病毒样本库增长趋势

2015 年，在阿里聚安全病毒样本库中，恶意扣费类病毒样本量占比最高，达 67%。该类病毒应用未经用户允许私自发送短信和扣费指令，对用户手机的资费造成一定风险，需谨慎使用。

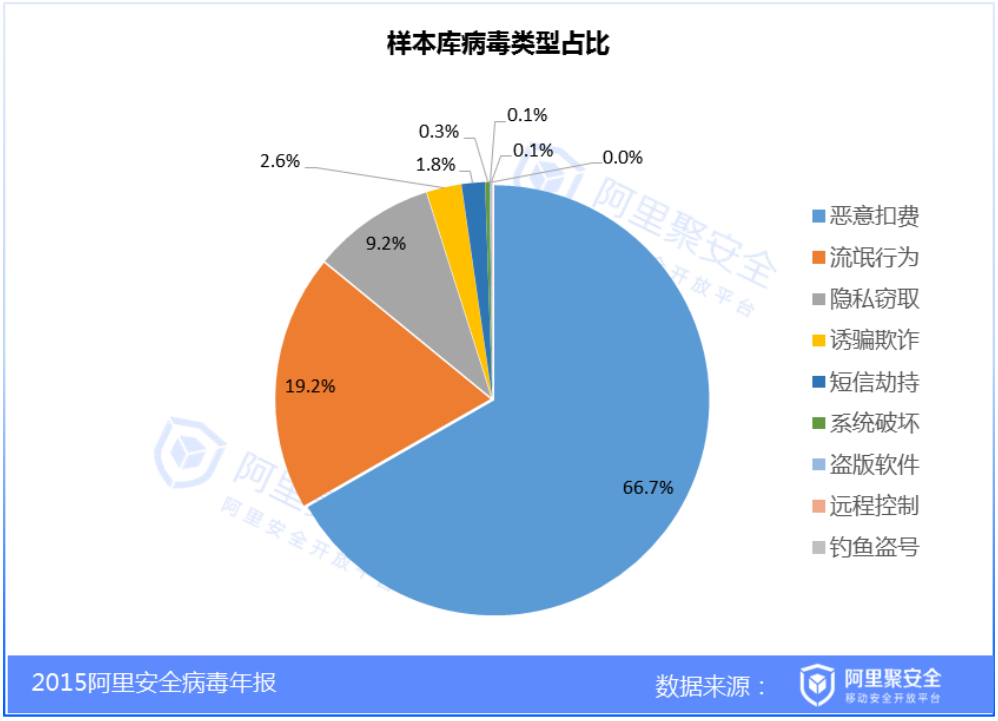


图 3 2015 年阿里聚安全病毒样本库各类样本占比

流氓行为类病毒感染用户量最多，占比达 52%，这类病毒匿名弹窗、恶意推送广告、私自下载软件等，对用户体验和手机安全造成危害。

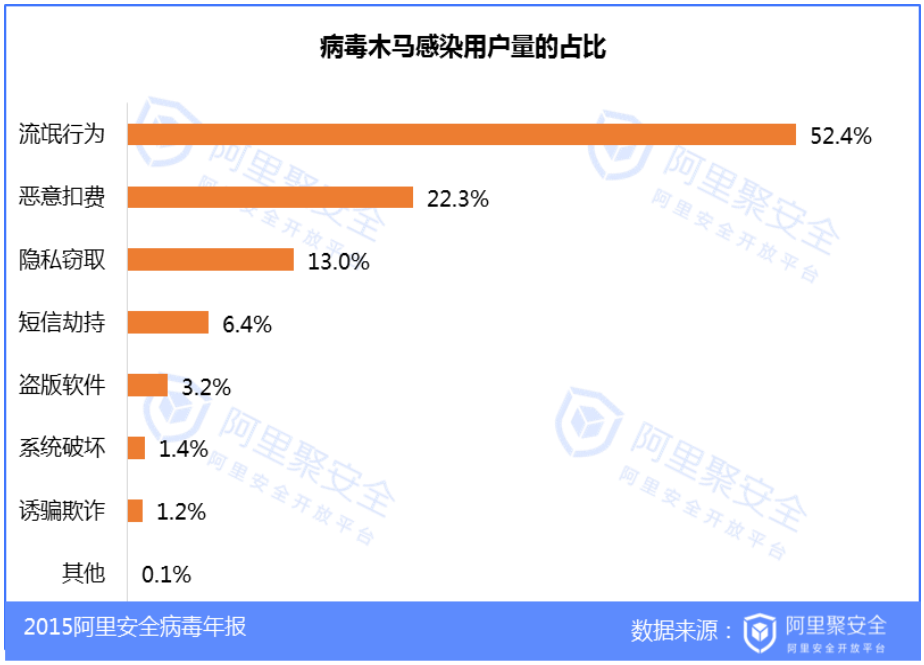


图 4 2015 年各类病毒感染用户量的占比

1.2 广东用户感染病毒最多

2015 年，广东是受病毒感染用户量最多的省份，其全年的设备感染量约占全国总感染量的 14%。由于广东省经济发达，华为中兴等本土手机品牌的发展，带动本地市场的强劲消费，一人持有多部手机的现象逐渐普遍起来，这些因素都导致广东手机用户的高染毒量。病毒感染的区域总体呈现出以中东部发达省份为主，西部为辅的格局，病毒制造者重点依然瞄准东部沿海手机用户来掘金。

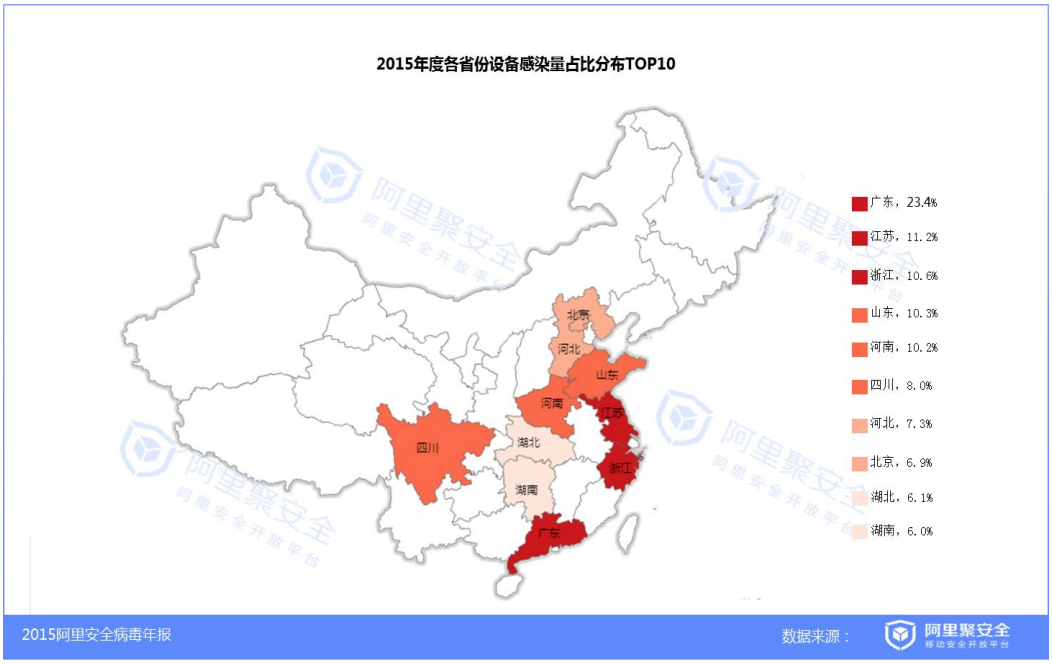


图 5 2015 年用户感染病毒 Top 区域分布

2015 年设备中毒比例最高的省份集中在中西部，贵州、新疆、四川是中毒比例最高的三个省份。其中，贵州是最易被病毒感染的省份，中毒比例达 23%，每 4.3 台手机就有 1 台染毒，比全国平均值高 6%。

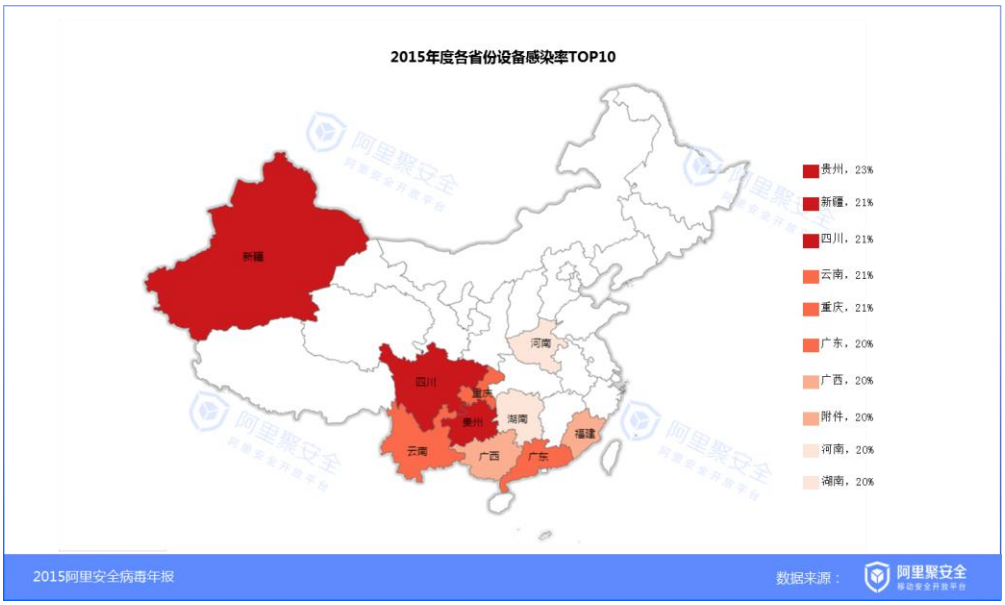


图 6 病毒感染率的用户区域分布

1.3 95%的热门移动应用存在仿冒应用

为分析移动应用行业的仿冒情况，我们在第三方应用市场分别下载了 18 个行业的 top10 应用共计 180 个，并利用阿里聚安全仿冒检测引擎对这批样本进行监测，得出了以下分析结论。18 个 APP 行业分别为：社交类、游戏类、影音类、摄影类、工具类、金融类、阅读类、旅游类、生活类、教育类、娱乐类、新闻类、安全类、办公类、电商类、健康类、运营商、政务类。

仿冒监测结果显示，这 180 个行业热门应用中，约 95%的应用都存在病毒仿冒，总病毒仿冒量高达 11963 个，平均每个热门应用的仿冒量达 66 个。

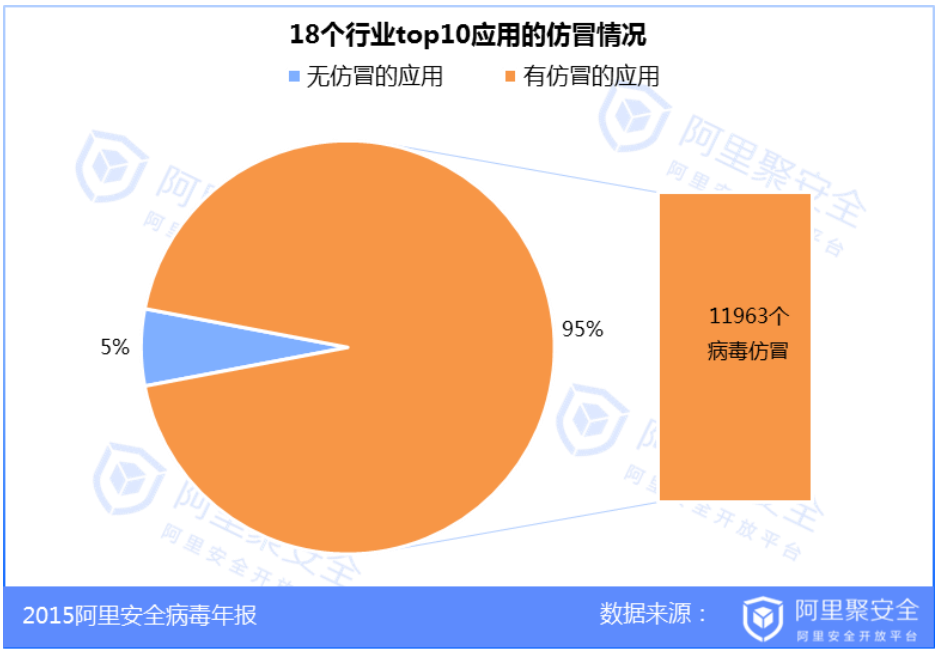


图 7 18 个行业 Top10 Android 应用的病毒仿冒情况

在技术手法上，11963 个病毒仿冒应用中，纯粹仿冒正版软件应用名称的占 71%（8403 个），纯粹仿冒正版软件包名的仿冒量占 15%（1845 个），两者结合的仿冒量占 14%（1616 个），可见不良开发者最喜欢利用正版应用的名称来开发仿冒应用。仿冒软件利用与正版应用相似的特征，诱导用户下载安装，之后实施相应的病毒行为，对用户的危害极大，用户需谨慎使用，尽量在官方渠道进行下载。

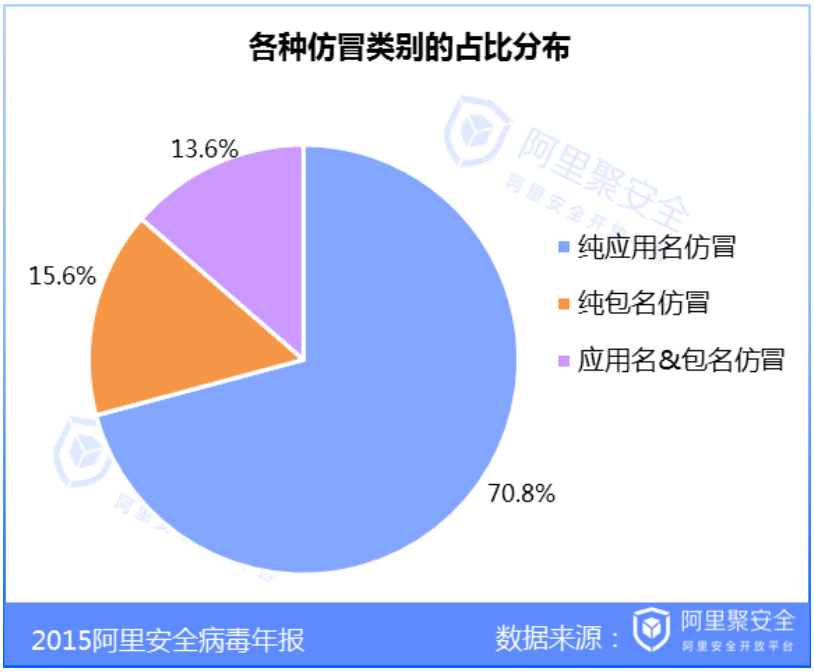


图 8 18 个行业 Top10 应用的仿冒软件采取的仿冒技术

1.4 社交类应用仿冒量最高

18 个行业中社交类应用的仿冒量达 4958 个，占总仿冒量的 41%，且这些仿冒应用中 96%都具有高风险的病毒行为，如恶意扣费、短信劫持等。游戏类应用的仿冒量次之，占总仿冒量的 16%，且这些仿冒应用中 34%的仿冒软件具有高风险病毒行为。值得注意的是，运营商类应用虽然仿冒量较少，只占总体仿冒量的 0.4%，但其 98%的仿冒应用都有高风险行为，不法分子容易伪造成各大运营商来行使欺骗行为。

可以看出，热门行业如社交、游戏、工具、金融等是仿冒的重灾区，这些仿冒软件对正版应用开发者和用户都会造成巨大危害，建议正版开发商使用阿里聚安全的扫描引擎来发现仿冒情况，并及早联系各渠道进行下架，维护自己的权益和名誉。此外，建议用户在官方渠道下载正版应用，以免受骗。

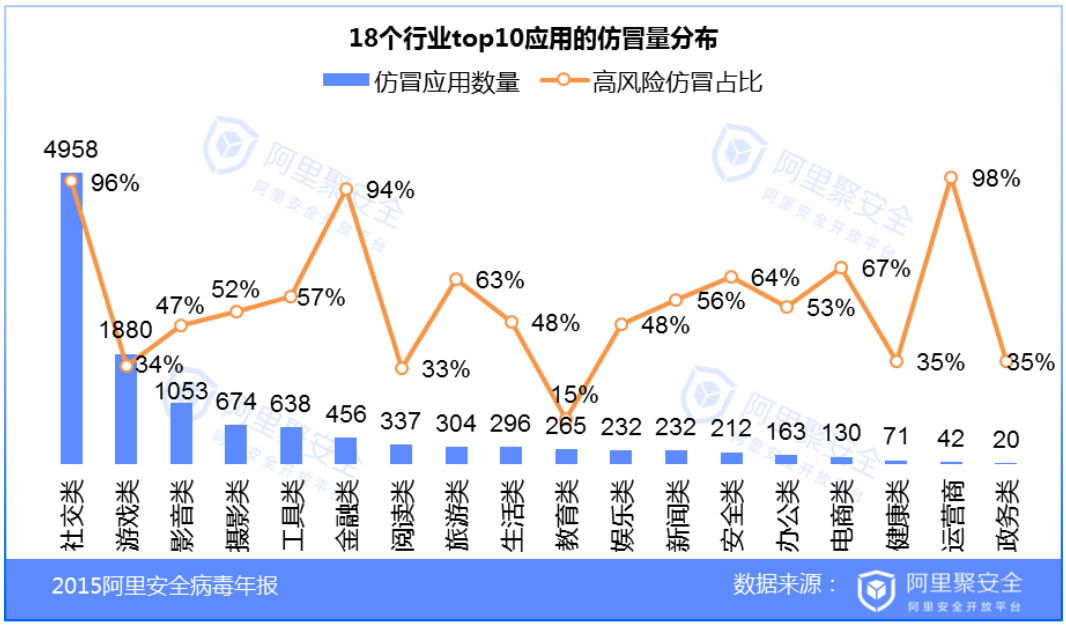


图 9 18 个行业 Top10 应用的仿冒数量

18 个行业 Top10 应用的 11963 个病毒仿冒中，具有恶意扣费行为的仿冒软件占比高达 50%，流氓行为类的病毒仿冒占比 30%，该类病毒会匿名弹窗、恶意推送广告，诱导用户下载广告应用，严重影响用户操作体验。

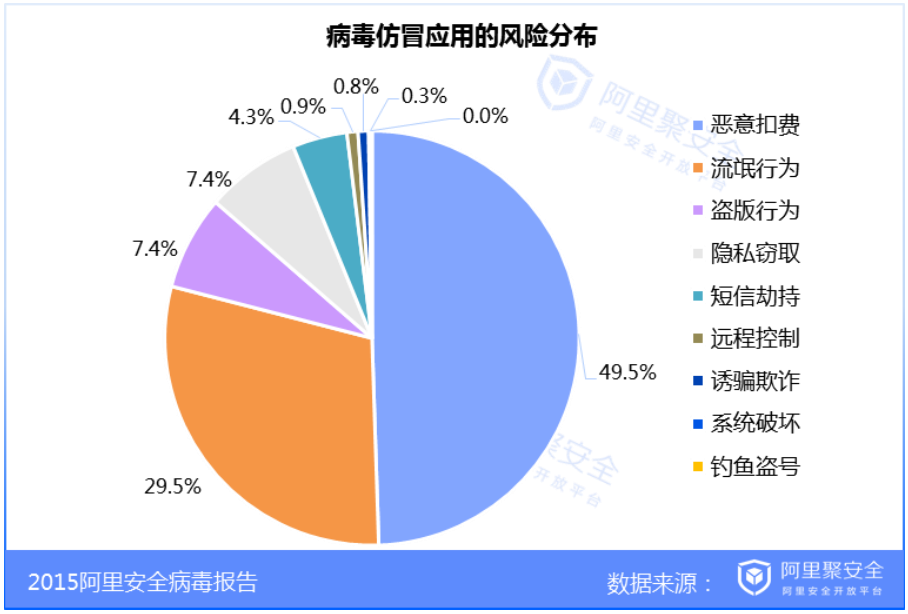


图 10 18 个行业 top10 应用仿冒软件的恶意行为分布

1.5 游戏、金融等热门应用 100%含仿冒软件

游戏类 Top10 应用中，100%应用含病毒仿冒软件，总仿冒量 1880 个，在 18 个 APP 行业中排名第二，且其中 33%的仿冒应用具有高风险的病毒行为。

1880 个病毒仿冒应用中，59%的仿冒应用具有流氓行为，在游戏中弹出骚扰广告、匿名弹窗等，严重影响用户体验。此外 31%的仿冒应用具有恶意扣费行为，容易导致用户手机流量消耗，或游戏账户中的资金受损。

游戏应用以数量多、种类杂、变现快、收益高的特性，容易成为不良开发者争相仿冒的对象，影响正版开发者和用户的利益，其仿冒问题应该引起重视。

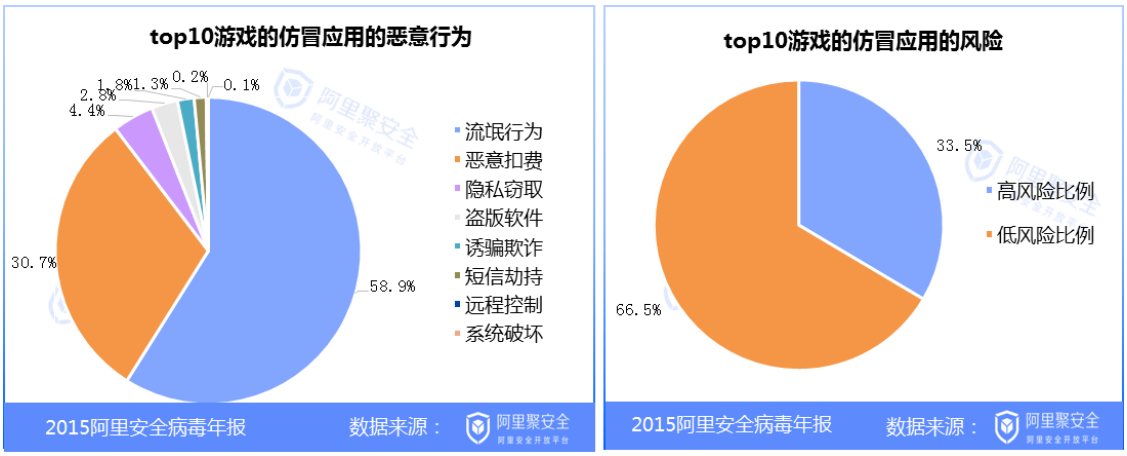


图 11 游戏行业 Top10 应用的仿冒软件的恶意行为分布

金融类 Top10 应用中，100%应用含病毒仿冒软件，总仿冒量 456 个，在 18 个行业中排名第 6，且 94%的仿冒应用具有高风险病毒行为。

456 个病毒仿冒应用中，48%的仿冒应用有隐私窃取行为，31%的仿冒应用有短信劫持行为，隐私窃取、短信劫持等病毒容易造成用户隐私信息泄露，影响金融账户资金，对用户危害极大，需谨慎使用。

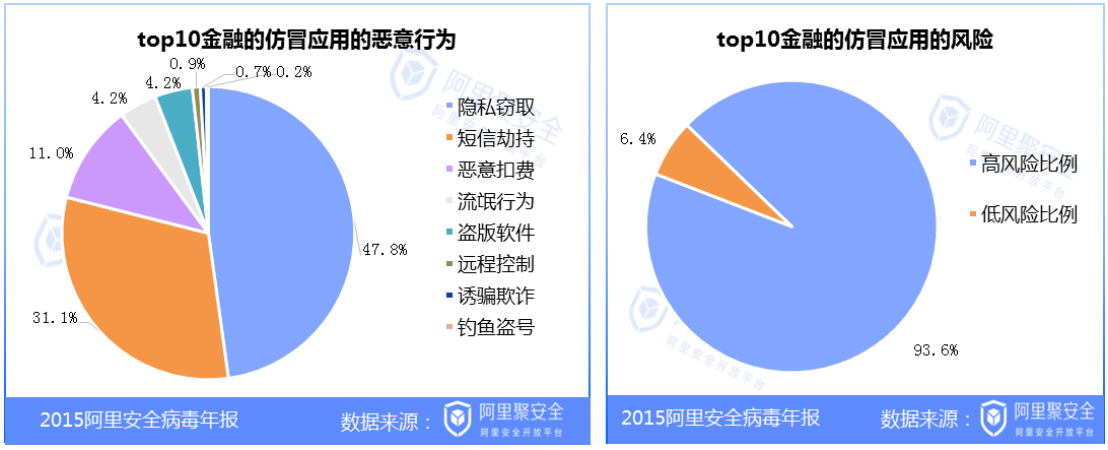


图 12 金融行业 top10 应用的仿冒软件的恶意行为分布

电商类 Top10 应用中，90%的应用含病毒仿冒软件，总仿冒量 130 个，在 18 个行业中排名 15，且 67%是高风险病毒应用。

130 个病毒仿冒应用中，41%的仿冒应用有远程控制行为，容易导致用户手机被黑客控制，引起隐私信息泄露、账号被盗等风险。由于电商类应用涉及用户网购行为、账户资产等敏感信息，这些高风险仿冒应用对用户的危害极大，需提高警惕。

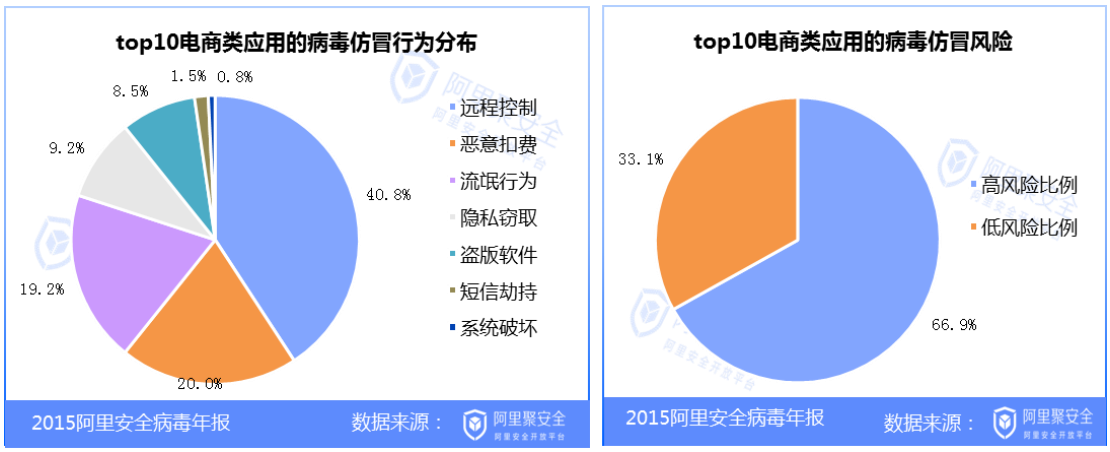


图 13 电商行业 Top10 应用的仿冒软件的恶意行为分布

第二章 2015 年病毒的典型行为

2.1 病毒不再依赖设备权限

大多数用户认为 Android 设备没有 root 过，就是安全的，即使感染恶意代码，恶意代码也没有高权限进行恶意操作。然而 2015 年 8 月，全球范围内大量用户感染自带 root 工具包的恶意应用，影响包括 Android 5.0 及以下系统的设备。该病毒感染设备后，会根据设备相应的系统进行 root 提权操作，随后静默安装恶意应用。此类病毒给用户造成了巨大的困扰，用户也纷纷反馈手机中莫名奇妙被下载了其他软件，手机即使恢复出厂设置，问题仍然无法解决。

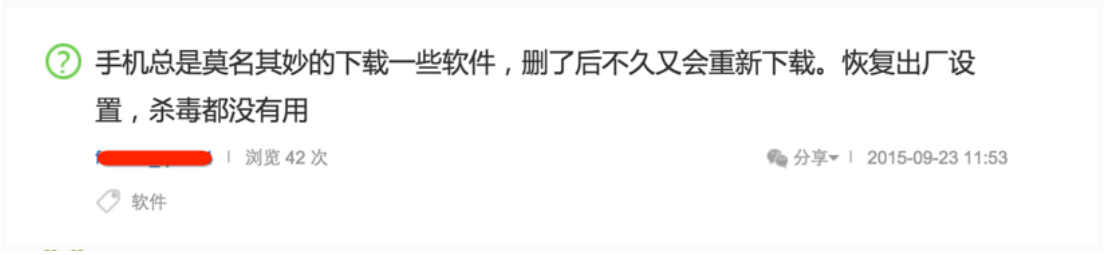


图 14 网友反馈

此类恶意应用不再依赖设备 root，而是通过云端或本地配置 root 工具包，对设备强行 root。我们发现 root 工具包除利用已知系统漏洞外，甚至还使用了某些安全厂商的 root 提权组件以提升 root 成功率。这类病毒为了保持自身的持久性和模糊性使用了大量自我保护手段，包括配置 C&C（指令和控制服务器）、规避 Google Play 检测、类加载代码混淆、将恶意应用植入系统分区、修改开机执行的恢复脚本、隐藏图标、激活设备管理权限防卸载等。下面是该类病毒的典型运行流程：

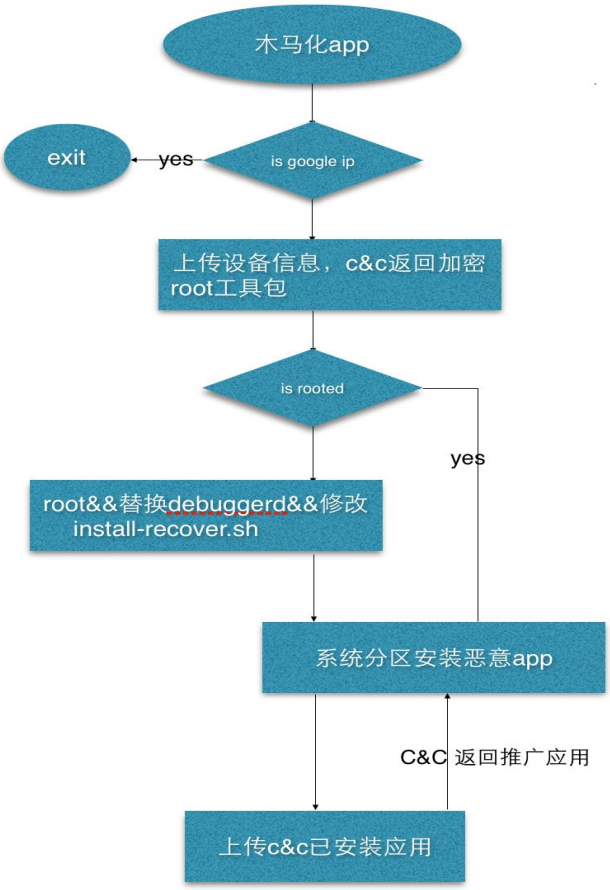


图 15 病毒运行流程

此类病毒木马的特点：

1. 规避 Google Play 检测

恶意应用的传播渠道包括各大游戏交友论坛、色情网站、以及 Google Play。而木马化的应用是怎么上传至 Google Play 的呢？病毒制造者使用多种方法躲避 Google 检测：

a) 检测病毒自身运行环境的 IP，若映射到 Google Bouncer，恶意代码将不会执行。由于自身配置 C&C 服务器，病毒作者可以完全控制恶意代码执行；

b) 延迟启动恶意代码，开启定时器，利用动态加载技术，反射执行恶意代码；

c) 使用第三方加固；

2. C&C 服务器

配置云端远程命令和控制服务器，可以灵活控制恶意代码的执行，规避 Google Bouncer 和杀毒软件的检测，病毒窃取被感染的设备隐私信息并上传到 C&C 服务器，同时获取相应的控制指令，或恶意应用包。用户发现自己的设备被感染后，恶意攻击者完全可以通过服务器指令清理攻击现场，取证非常困难。

3. 利用设备漏洞，对手机提权

影响的设备包括 Android 5.0 以及以下系统。恶意应用通过两种方式进行提权：通过

C&C 服务器下载 root 工具包进行提权、自身携带加密的 root 工具包提权。提权包除了利用包括编号为 CVE-2013-6282、CVE-2014-3153、CVE-2014-7911、CVE-2014-4322、CVE-2015-3636 在内的多个设备漏洞，也包括某些安全厂商的提权组件。

4. “打不死的小强”

通过替换 debuggerd、修改 install-recover.sh，保证植入的 rom 病毒即使刷机也不死。此类病毒包括“伪万年历”、“Ghost Push”、”Kemoge”、“百脑虫”。具体的行为分析可参考《“伪万年历”Root Exploit 恶意应用分析》(点击查看详情)。

2.2 以植入木马为目的的诈骗事件层出不穷

近年来，电信诈骗非常猖獗。相比往年，今年诈骗事件呈上升趋势，并且诈骗手法也更具欺骗性、多样性。典型的电信诈骗是通过伪基站伪造银行或者移动运营商的官方客服短信，短信中包含木马链接，或者冒充用户比较信任的司法机关给用户打电话，引导用户访问某个钓鱼网站。不管是哪种方式，其共同特点都是利用社会工程学诱骗用户安装木马并套取用户的个人资料。当这些诈骗团伙获取到用户个人信息后会假称用户的好友或是用户本人，对用户或其亲友实施诈骗，许多人根本无法辨别其真伪，据悉，2015 年这类诈骗手段成功率相对较高。

统计数据显示，今年具有短信拦截行为的木马感染设备量高达 200 万，下图是 2015 年用户感染量趋势图。

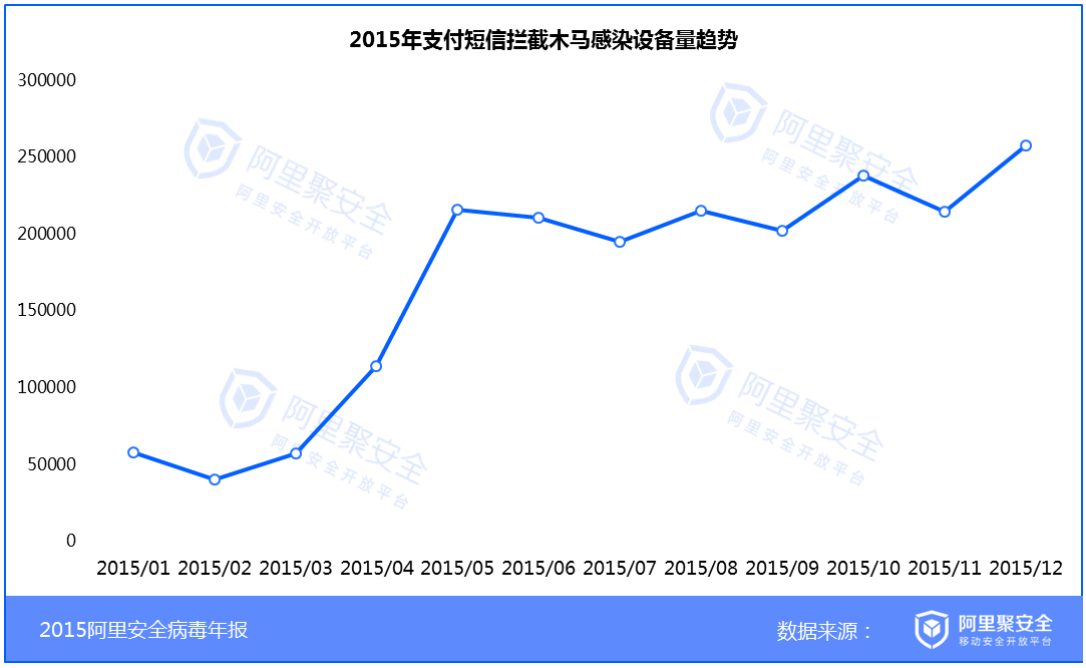


图 16 具有短信拦截行为的木马感染用户量

全国手机设备支付短信拦截木马中毒比例最高的省份集中在中南部，广东、河南、山东

是中毒比例最高的三个省份。

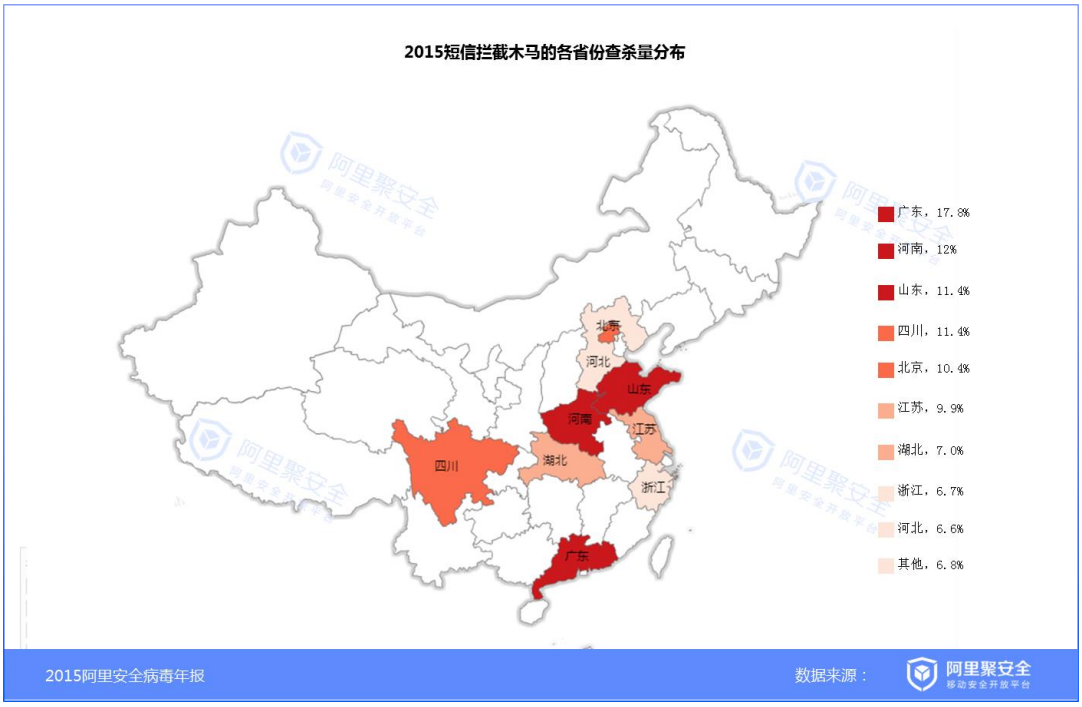


图 17 支付短信木马感染的用户区域分布

从以上图 17 可见年末是“短信拦截木马”感染的高峰期，根据阿里钱盾防骗平台的监测结果，此类诈骗短信通常包含“积分兑换”、“银行客户端升级”、“车辆违规”、“学生成绩单”、“相片”、“老公出轨”、“老婆出轨”等涉及社会热门事件的关键词。这类短信主要通过钓鱼网址诱骗用户网银信息（银行卡号，卡号交易密码，姓名身份证，开户预留手机号），诱骗用户安装“短信拦截木马”。

图 18 诈骗短信

图 19 钓鱼网址

由于电信诈骗具有操作门槛低，牟利空间大的特点，为保证木马制作者获得源源不断的利益，黑市上逐渐形成了与木马免杀保护相关产业。免杀保护手段一般包括使用加固技术进行代码保护、设定木马使用有效期、校验签名防止重新打包等。

深入分析发现，“短信拦截木马”背后是一个完整的非法营销产业链，包括：

a) 社工人员负责收集社会热门事件，对定向群体发送感兴趣信息；

b) 木马开发者编写短信拦截木马，贩卖木马给黑产组织，包括配置黑产组织的邮箱、手机号码或云端服务器，用以上传受骗用户信息（银行卡号，身份证，姓名，手机联系人，拦截的短信等）；

c) 分发传播组织利用伪基站发送诈骗信息、制作钓鱼网址、以及利用联系人转发诈骗短信；

d) 洗料分赃实时对拦截的短信分析，收集贩卖用户信息。

图 20 “短信拦截马”的产业链环节

2.3 黑产旁门左道

2015 年，从阿里聚安全扫描引擎检测到的病毒中发现，部分攻击者利用用户喜闻乐见的噱头或者社会热门事件趁机而入。据统计，利用 Android 辅助功能（Accessibility Service）作恶和锁屏勒索，是病毒在 2015 年呈现出来的两大新的恶意行为。

1. 利用 Android 的辅助功能实施恶意行为

年末的抢红包热门事件同样被黑产组织盯上，大量非法“抢红包”应用出现在各大论坛和第三方应用渠道。黑产组织以“自动抢红包”、“WiFi 信号增强”等用户痛点需求作为诱饵，引导用户开启辅助服务，进而控制手机。部分木马甚至直接用“自动抢红包”作为应用名，用户一旦安装，便立即隐藏图标，并在后台恶意监控手机就设备，这类木马多是“短信拦截木马”的变种。

Google 开发辅助功能的初衷是帮助肢体有障碍的人自动控制移动设备。因此很多自称实现“自动抢红包”功能的应用，都要求用户授予其辅助功能。然而目前该功能却被攻击者恶意利用来进行恶意应用推广、安装。木马引导开启辅助功能图如下：

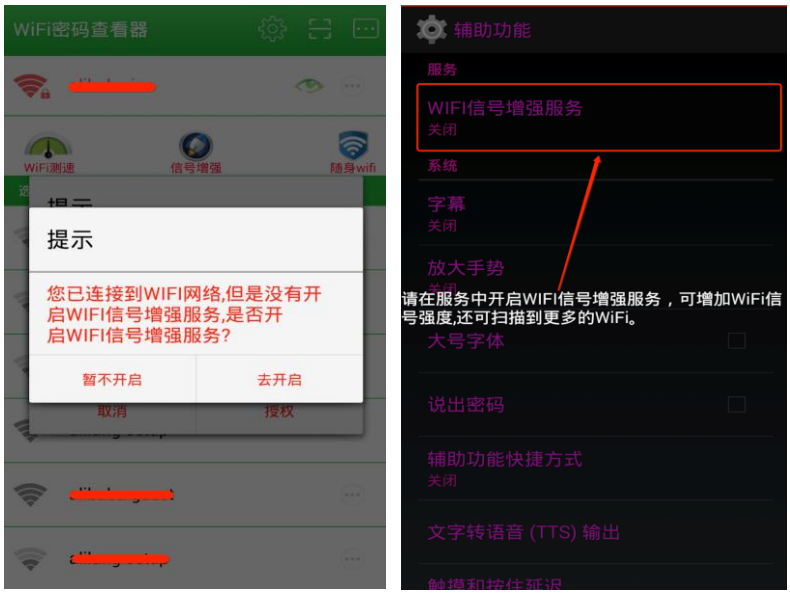


图 21 引导用户开启辅助功能

病毒具体的行为分析可参考《滥用 Accessibility service 自动安装应用》文章。在此提醒用户到正规渠道下载抢红包应用。

2. 锁屏勒索

2015 年 5 月出现大量锁屏勒索恶意应用，该类应用多伪装成游戏外挂、QQ 刷钻等软件。病毒启动后强制锁屏，即使用户重启手机也无济于事，病毒制造者有意将自己联系方式留在锁屏界面，等用户联系时进行恐吓、诈骗钱财。使用的锁屏技术大多数通过控制 WindowManager.LayoutParams 的 flags 属性制作一个特殊的全屏 View 并置顶，然而对于普

通用户只有通过联系锁屏中留下的 QQ 号码并支付费用才能解锁手机。

下面是与“兮颜”聊天的过程：

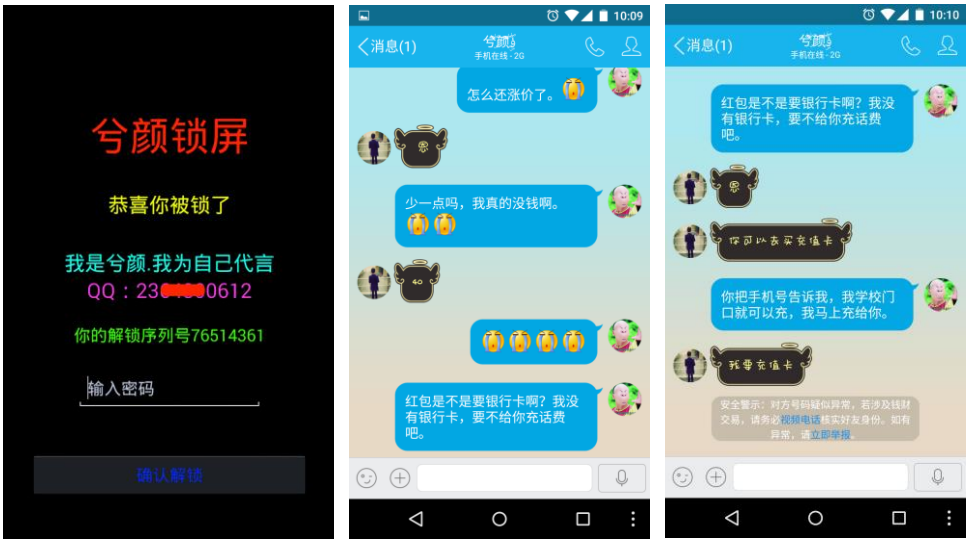


图 22 锁屏解锁过程

2.4 色情诱惑类病毒重出江湖

从 2015 下半年开始，阿里移动安全团队发现大量色情类病毒重新开始在某些论坛或应用市场上泛滥，通过诱惑性的应用图标或应用名称来刺激用户下载，数月期间就感染了近 100 万用户。这类病毒具有恶意扣费、窃取隐私、强制推送并安装其他恶意软件等行为，由于此类病毒能够直接获益，备受不法分子青睐，用户需提高警惕。

图 23 “魅影杀手”色情诱导类病毒应用图标

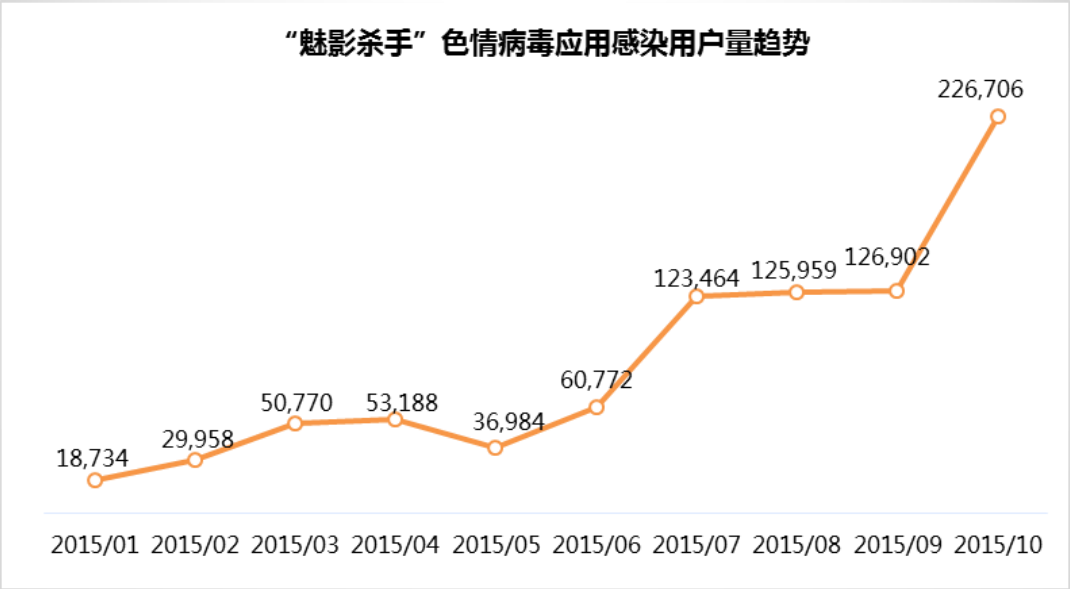


图 24 “魅影杀手”色情诱导类病毒感染用户量趋势

这类病毒具有以下特点：

1. 使用代码加固技术，把恶意代码加密，运行后再从内存中解密出来；
2. 安装后伪装成系统组件，同时将自身安装隐藏在系统目录下，防止卸载的同时也躲避了部分安全软件的查杀；
3. 通过云端服务器配置不断创建虚假快捷方式、弹对话框、伪造通知栏等方式，强制推送安装其它恶意软件。

由于该类色情类应用开发和制作流程简单，推广成本低，并且市场空间巨大，能够在短时间内产生经济效益，因此吸引了大批不法分子参与其中进行利益分成，并且逐渐形成了一条完善的黑色产业链。色情应用的开发者通过极低的推广费用，把样本上传到某些网络推广平台，例如小众的 Android 市场、应用推广平台、色情网站、部分游戏或者游戏外挂网站等。由于这类色情应用本身的诱骗特性，容易激发用户的好奇心下载安装。一旦成功安装到用户手机上，它们会在后台偷偷订购一些移动运营商的收费服务，同时向用户手机推送更多恶意推广软件，这样黑产一方面参与电信收费项目的提成，另一方面还获得了更多的广告流量分成。

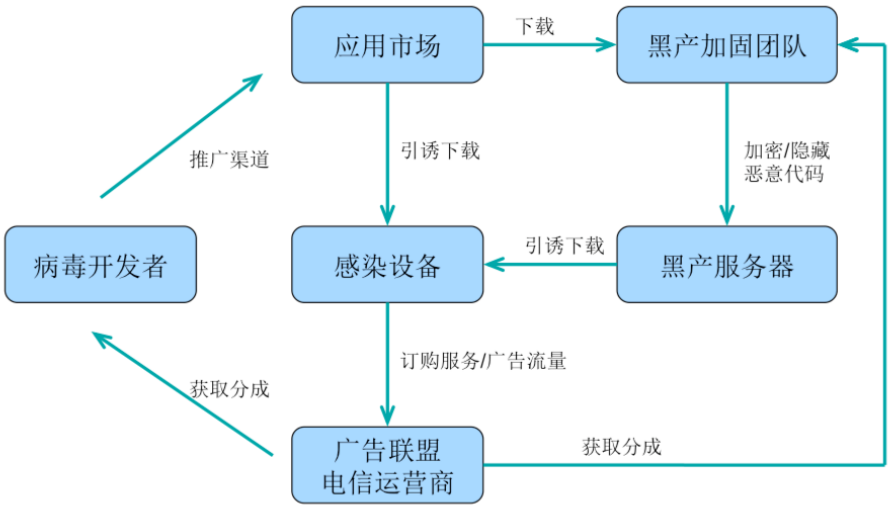


图 25 “魅影杀手”色情诱导类病毒黑产利益链条

2.5 恶意应用类型更加广泛

1. 病毒制造者开始对热门应用下手，不再只钟爱色情类和系统类应用

对比 2014 年与 2015 年截获的新增恶意样本，发现今年恶意应用不再仅钟爱色情、系统类应用，而是对广受用户青睐的应用下手。这一变化的原因是，黑产已考虑到恶意程序成功安装的问题，将广受用户欢迎的应用木马化。从用户的角度来看，修改后的程序看似一个合法的应用，而的确在许多情况下，它们会提供相同的功能和用户体验。但是在后台，它们会检测自身运行系统并试图发起攻击，包括获取 root 权限、上传用户设备信息、静默安装恶意应用等。

2. 广告插件触及灰色地带

往年广告应用占比最多的是频繁推送广告和静默下载，主要造成用户流量消耗，拦截短信、上传用户信息和静默安装占比较小。但 2015 年呈现恶意广告插件上升趋势，恶意广告主要表现为以下几点

a) 大量恶意应用以色情内容为诱饵，不断推送各种恶意广告；

b) 利用辅助服务功能，进行无 root 静默安装；

c) 广告 SDK 包越来越大，权限滥用，出现间谍类广告，上传用户短信，手机联系人等信息；

d) 广告插件附带 root exploit，进行静默安装；

3. 黑产热门事件响应

Hacking Team 泄密事件 RCS Android 间谍软件包被披露，在随后几天就发现黑客利用

公开的间谍代码；优衣库试衣间的不雅视频在网络上广泛传播，在成为热门话题的同时，网络黑客团队也趁机而入，制作大量的“优衣库视屏”相关病毒木马；黑产伪基站利用社会热点事件，如包含“跑男”、“好声音”等的钓鱼拦截，诱骗用户点击下载；种种事件映射出黑产具备精干的作业团队、强大的用于攻击的基础设施、专业的恶意代码编写小组，以及快速响应的社会热门事件跟踪团队等。

第三章 2016 年移动病毒发展趋势

1. 利用加固技术隐藏恶意代码逐渐盛行

传统的反病毒引擎多数采用特征码查杀技术，使用加固技术加密后的恶意代码在运行时从内存中解密，可以绕过静态扫描特征码技术，从而实现免杀。

一方面，由于移动应用加固技术门槛逐渐降低，代码加固成了木马对抗安全软件最常用的手段，在巨大的利益驱使下，甚至催生出了黑产加固链条。另一方面，安全加固作为很多安全厂商的主打产品，它同时也是一把双刃剑，在保护开发者版权的同时，也给了不法分子很多便利。目前我们发现很多木马使用了安全厂商提供的免费加固服务。不仅如此，木马青睐的“壳”呈现出集中化趋势：部分安全厂商的加固平台由于没有使用反病毒引擎过滤包含恶意代码的应用，导致其加固方案被肆意用于木马开发。因此，我们认为所有安全厂商在提供加固解决方案的同时有责任接入专业的恶意代码扫描服务，防止自己的安全产品助纣为虐。

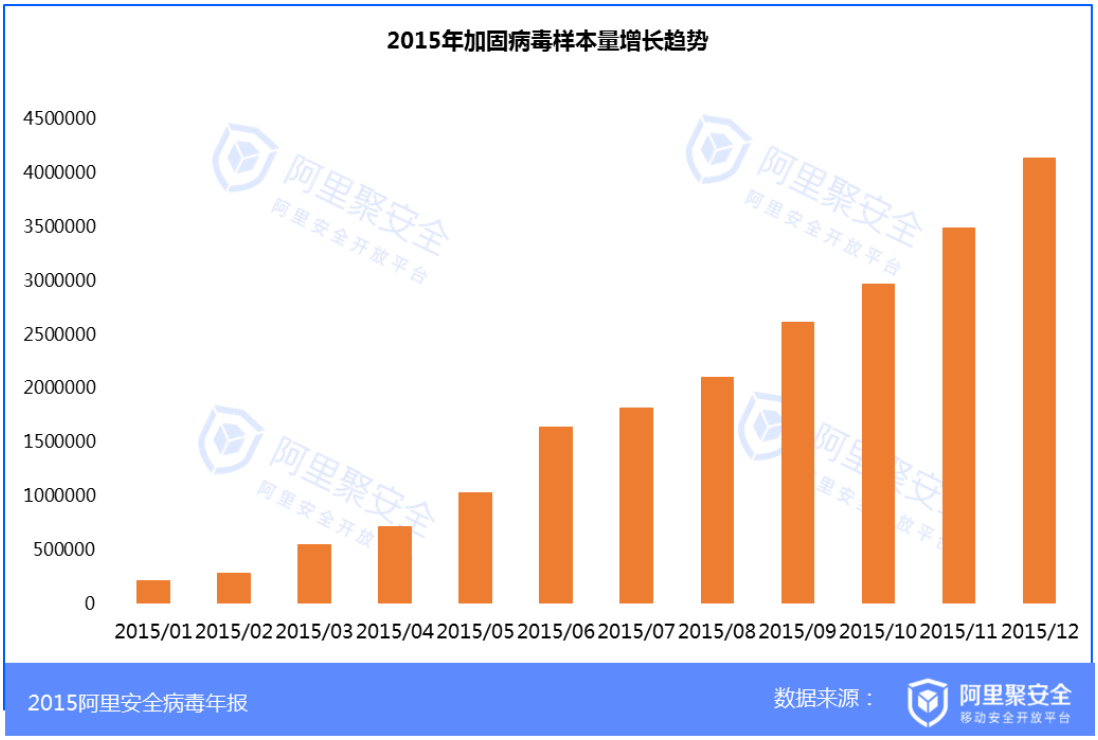


图 26 加固木马的样本量增长趋势

2. 未 root 过的设备不再安全

众所周知，root 过或者越狱过的设备由于系统沙盒限制可以被突破，其安全性会大大降低，因此一般建议普通用户尽可能不要 root 自己的手机。然而随着一个又一个的系统漏洞被披露，以及对应的 root exploit 被公开，给作恶者以可乘之机。阿里移动安全团队发现有恶意软件利用开源的 root exploit 强行获取系统 root 权限进行恶意推广，一旦应用被

植入系统分区，普通用户根本无法卸载。不排除将来病毒会以这种方式向系统分区植入其它病毒，达到长期驻留在用户手机伺机作案的目的。

3. 广告插件开始触及恶意行为灰色地带

广告插件能够帮助移动应用开发者直接将流量进行变现。为了提升广告转化率，我们发现部分插件开发商开始跨越行业底线，加入了流氓推广的行列，例如在桌面强行 push 安装应用快捷方式、自带提权工具包把推广的应用植入系统导致无法卸载、利用 Android 辅助功能 API 实现静默安装等。为了躲避检测，这些恶意广告插件从云端下载加密的恶意代码，在本地解密后动态加载，代码执行完成后再清理现场，导致用户利益受到侵害后溯源取证变得非常困难。

阿里聚安全微信公众号

阿里聚安全官网

阿里聚安全官网：http://jaq.alibaba.com

官方邮箱：mobilesecurity@service.alibaba.com