Alibaba Group 阿里巴巴集团

ALIBABA SECURITY AGENCY

阿里安全
2015年第三季度移动安全报告

阿里巴巴移动安全

阿里聚安全 阿里安全开放平台

阿里钱盾 钱有盾 盗无门

2015年第三季度移动安全概况

病毒

- 第三季度，总中毒设备量高达4121万，比第二季度增长16%。阿里聚安全病毒库新增样本275.2万，比第二季度增长40%。
- 第三季度，恶意扣费类病毒样本量占比64%，比第二季度增长25%，主要是色情类病毒持续增长，其恶意扣费行为需引起重视。

漏洞

- 安卓16个行业的top10应用中，平均每个应用含73个漏洞，比第二季度增长38%，漏洞问题应引起重视。
- 安卓16个行业top10应用89%都有高风险漏洞，且高风险漏洞量占比约24%，比第二季度略有下降。
- 运营商、电商、社交等行业的top10应用漏洞数量最多，漏洞量均超过700个。

仿冒

- 16个行业top10应用94%存在病毒仿冒，每个应用平均含55个仿冒，比第二季度增长12%。
- 社交、游戏两个行业的仿冒量最高，两者top10应用总仿冒量4477个，占16个行业总仿冒量的51%。

应用安全概览

应用安全病毒情况

- 病毒规模
- 病毒类型
- 感染用户分布
- 典型病毒案例

应用安全漏洞情况

- 应用漏洞
- 系统漏洞
- 重点行业漏洞分析
- 典型漏洞案例

应用安全仿冒情况

- 仿冒规模
- 仿冒风险
- 重点行业仿冒分析
- 典型仿冒案例

1. 病毒情况

病毒规模

- 第三季度，安卓平台平均每7台设备就有1台染毒，总中毒设备量高达4121万，比第二季度增长16% 。
- 第三季度，阿里聚安全病毒库共新增病毒样本量275.2万，比第二季度增长40%。

病毒类型

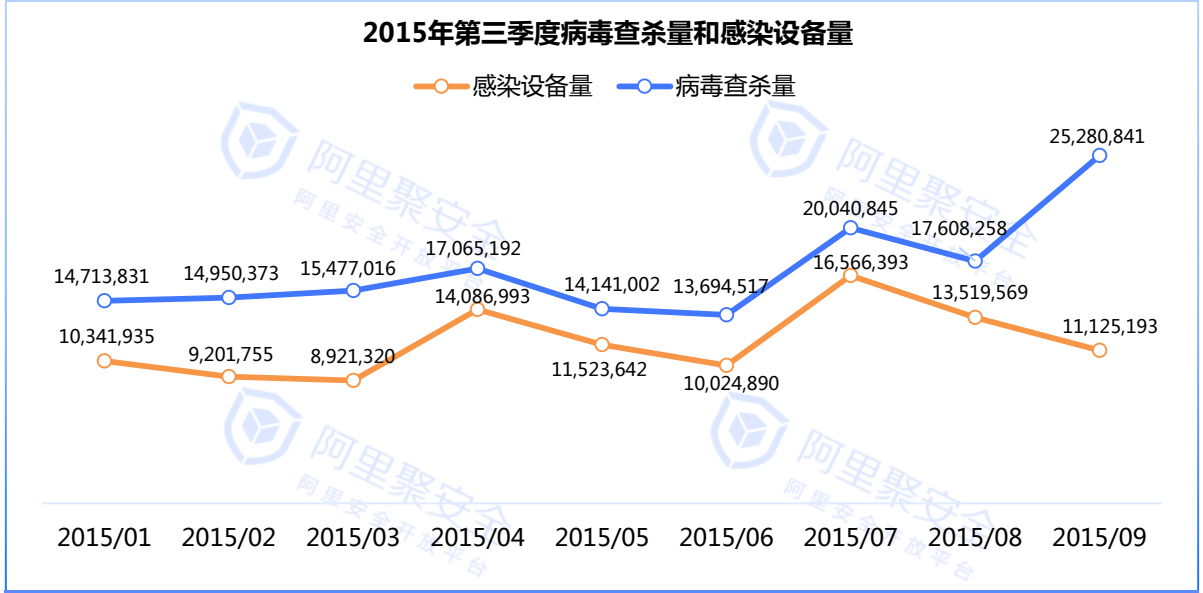
- 第三季度，恶意扣费类病毒样本占比最高，达64.5%，其感染了21.6%的用户量。
- 流氓行为类病毒在样本库中占20.5%，但感染了55.4%的用户量。

感染区域

- 第三季度，广东仍是受病毒感染最严重的地区，设备感染量占全国的14%，贵州是最易被病毒感染的省份，其设备感染率为15%。

1.1 病毒规模

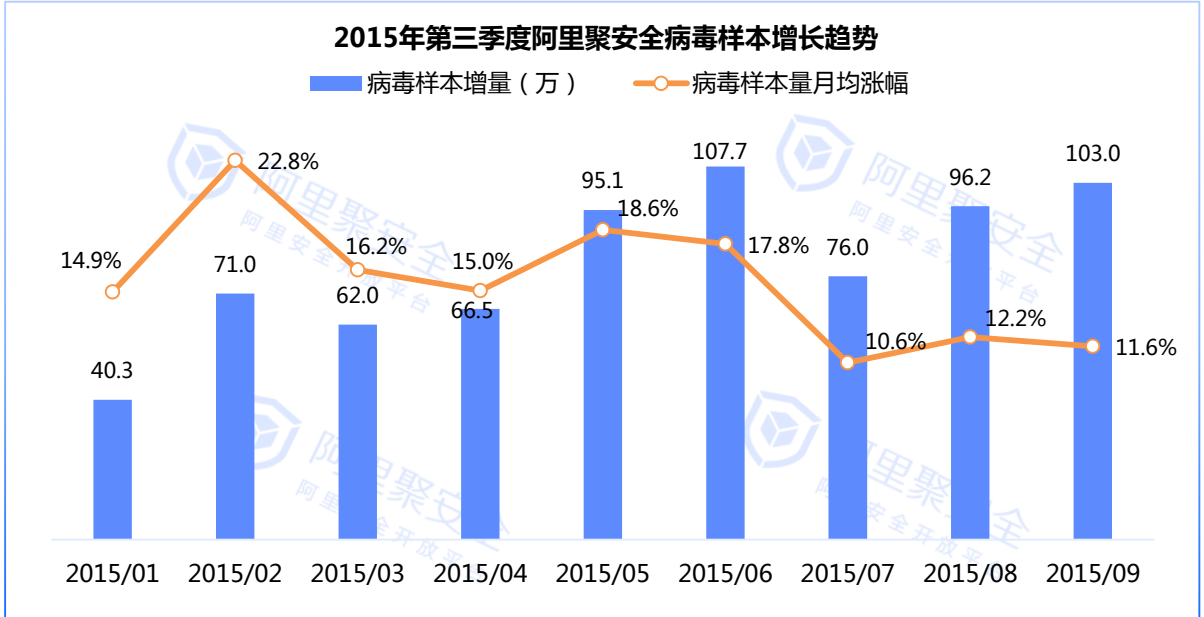
- 2015年第三季度，安卓平台平均**7台设备有1台设备染毒**，总中毒设备量高达**4121万**，比第二季度**增长16%**。
- 2015年第三季度，阿里聚安全病毒扫描引擎共查杀病毒**6293万**次，比第二季度**增长40%**，帮助用户抵御了大量的病毒风险。



数据来源：阿里聚安全 阿里安全开放平台

1.1 病毒规模

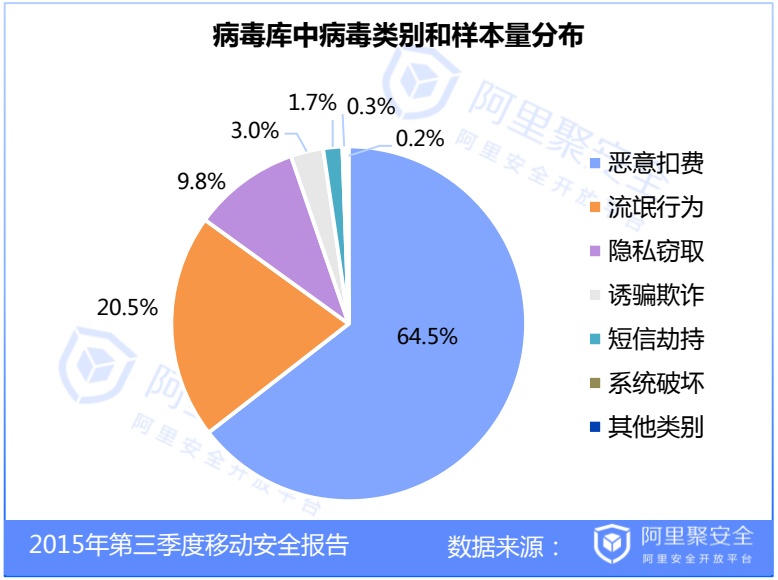
- 阿里聚安全病毒样本库持续增长，2015年第三季度病毒样本量**新增275.2万**，比第二季度**增长40%**。
- 第三季度内，病毒样本月均增长率为12%，平稳增长，但增长速度相比第二季度有所放缓。

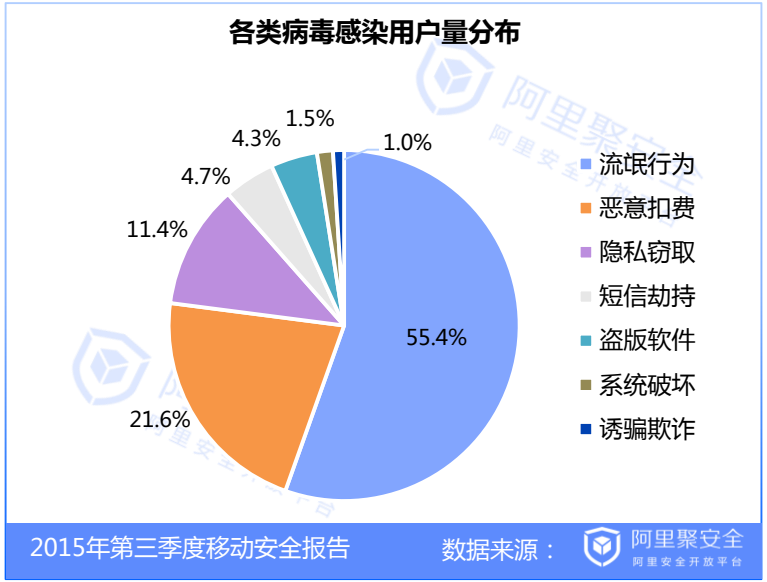


数据来源：阿里聚安全 阿里安全开放平台

1.2 病毒类型

- **恶意扣费类病毒**样本量占比最高，达**64%**，比第二季度上涨25%。第三季度，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，这类病毒具有恶意扣费行为，通过诱惑性的应用图标或应用名称来刺激用户下载，进而实施恶意行为，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。
- 流氓行为类病毒以20%的样本占比，感染了**55%**的用户群体，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。

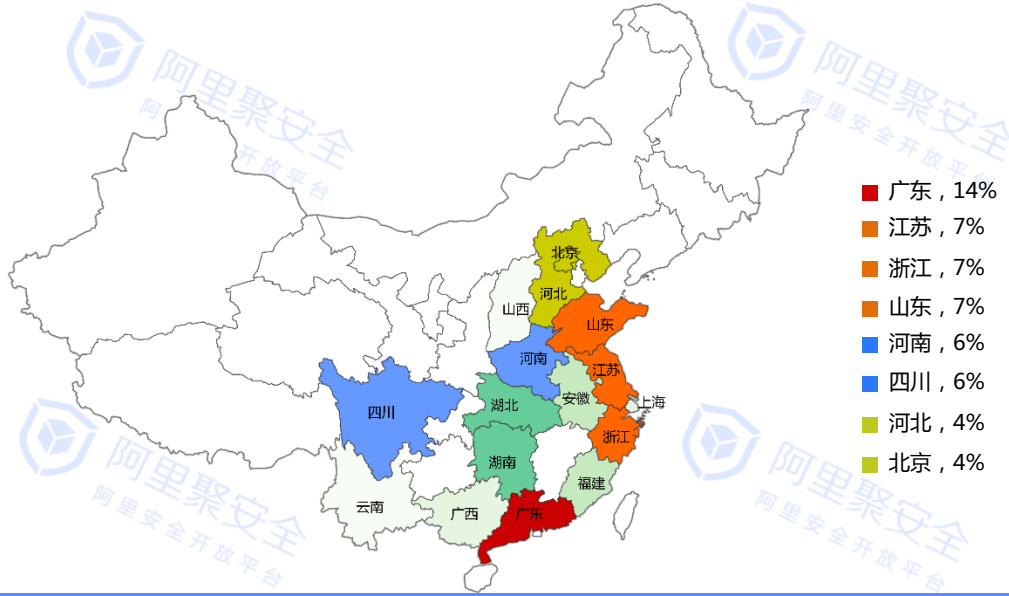




1.3 感染用户分布

- **广东**依然是受病毒感染用户量最多的省份，其第三季度的设备感染量占全国总感染量的**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。

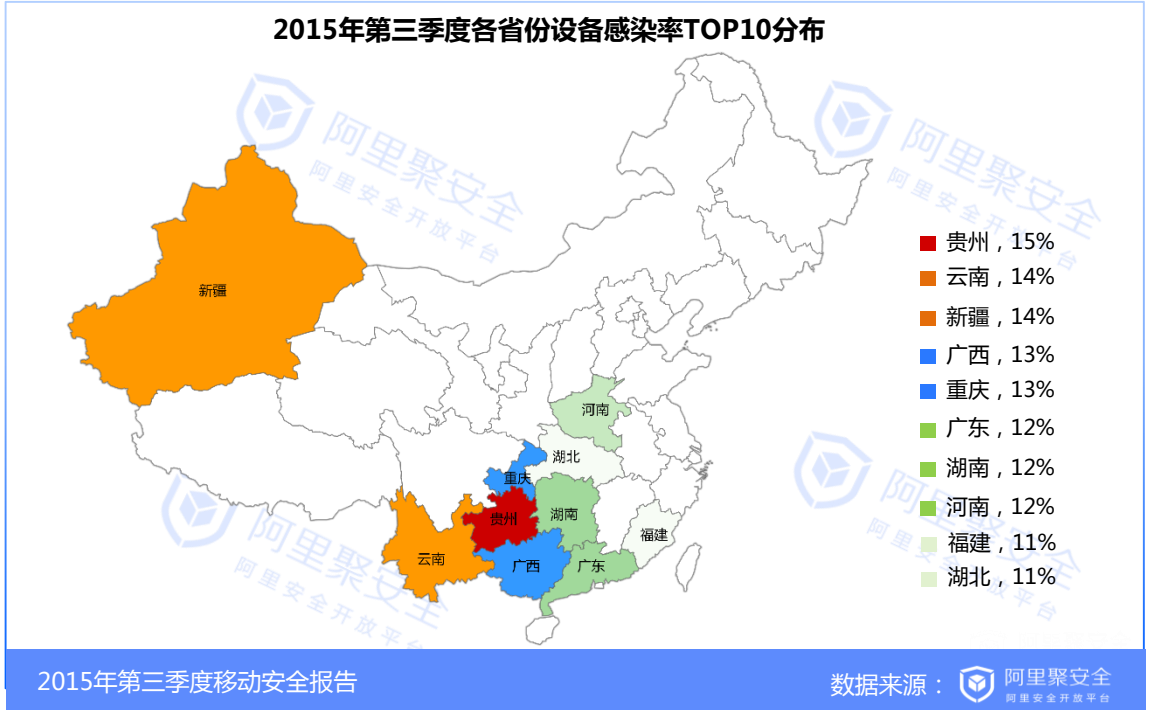
2015年第三季度各省份设备感染量占比分布



数据来源：阿里聚安全 阿里安全开放平台

1.3 感染用户分布

- **全国**手机设备的平均**中毒比例高达13.8%**，即每7台设备就有1台染毒。设备中毒比例最高的省份集中在中西部，贵州、云南、新疆是中毒比例最高的三个省份。
- **贵州**是最易被病毒感染的省份，中毒比例15%，每6台手机就有1台染毒，比全国平均值**高8%**。

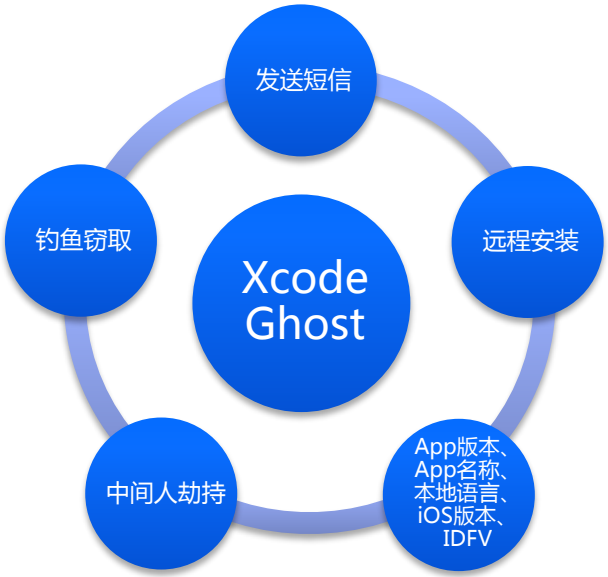


数据来源：阿里聚安全

1.4 典型病毒案例

- **XcodeGhost**是一个感染苹果开发工具的病毒，该工具生成的恶意App成功绕过App Store的检测，可收集敏感信息及下发控制命令，从而执行大量恶意行为，如打开网页、发送短信等。
- XcodeGhost打破了苹果的安全神话，其下架并公示了被污染的**25大应用**，逾**1亿用户**受影响。事件发生后，阿里移动安全发布首篇分析报告，将此病毒命名为XcodeGhost，并持续关注和分析。
- **阿里巴巴所有核心应用不受此病毒感染**，原因是阿里聚安全App风险扫描和漏洞检测响应机制，加上严谨的安全流程服务和统一集成打包上线平台“摩天轮”，保障了阿里巴巴庞大业务的无线安全能力。

XcodeGhost可以做什么



2. 漏洞情况

应用漏洞

- 16个行业的top10应用共有11630个漏洞，均值73个，比第二季度增加37%。
- 16个行业的top10应用89%都有高风险漏洞，且高风险漏洞量占比24%，比第二季度略有下降。

系统漏洞

- 2015年Android系统漏洞持续爆发，总漏洞量97个，同比上涨781%，涨幅迅猛。
- 2015年iOS系统漏洞亦逐步增加，总漏洞量579个，同比上涨101%。
- 越来越多的研究人员关注到Android和iOS系统，google和苹果也逐渐加大了在安全的投入，提交和修复的漏洞逐渐增多，未来，Android和iOS系统将变得更安全。

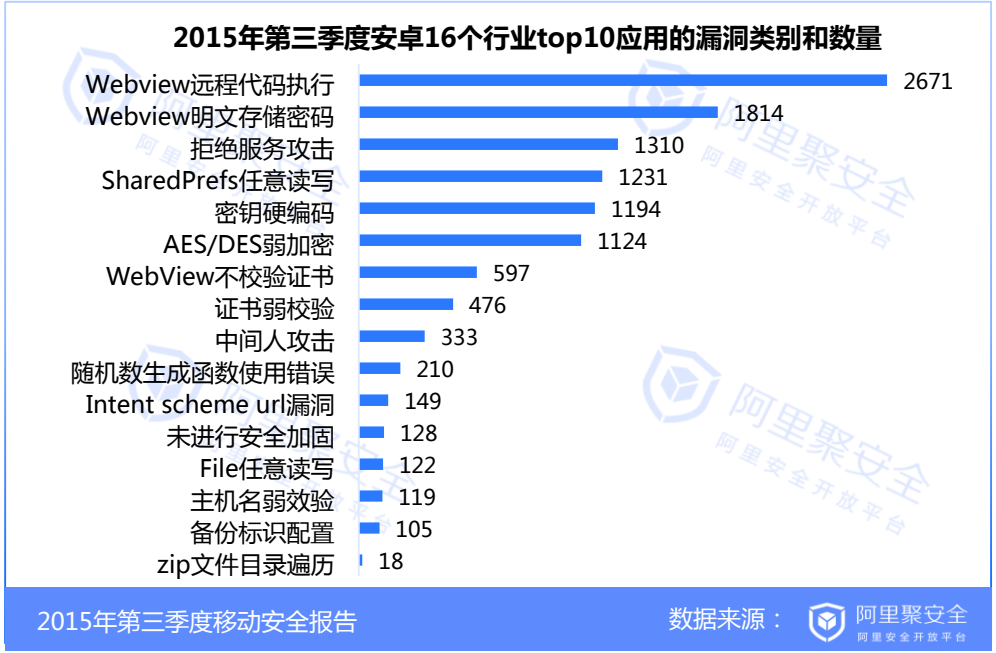
行业漏洞

- 运营商类top10应用的总漏洞量最高，达988个，漏洞风险容易造成用户话费、手机流量等的资损。
- 高危漏洞在金融类top10应用中占比最高，达33%，一旦漏洞被利用，将直接危害用户资产的安全。

- 报告中漏洞分析数据依托于阿里聚安全漏洞扫描引擎，具有多样化检测技术，百万级别漏洞库，100%覆盖已知漏洞，为开发者发现应用的真正威胁。
- 漏洞分析选取的安卓16个行业包括：金融、电商、游戏、运营商、政务、社交、安全、办公、工具、教育、旅游、摄影、生活、新闻、影音、阅读。

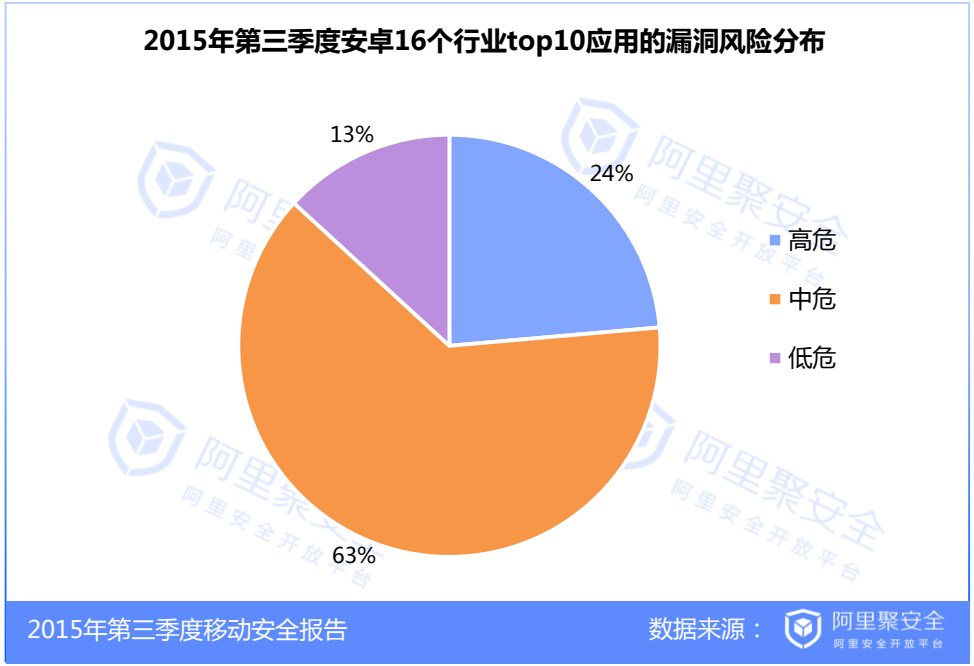
2.1 应用漏洞

- 16个行业的top10应用共有**11630个**漏洞，平均每个应用有**73个**漏洞，比第二季度**增长37%**，且89%的top10应用都有高风险漏洞。
- 11630个漏洞中，Webview远程代码执行漏洞量占23%，比第二季度**增长238%**。Webview远程代码执行漏洞引起的主要原因是调用了Webview的addJavaScriptInterface方法，该方法的安全风险只在安卓sdk版本17及更高版本中才被google修复。 由于sdk 17以下的机型在市场上仍占20%，故很多开发者为了兼容性还将APP支持的最小版本设置在17以下，导致该漏洞量一直不降反升。



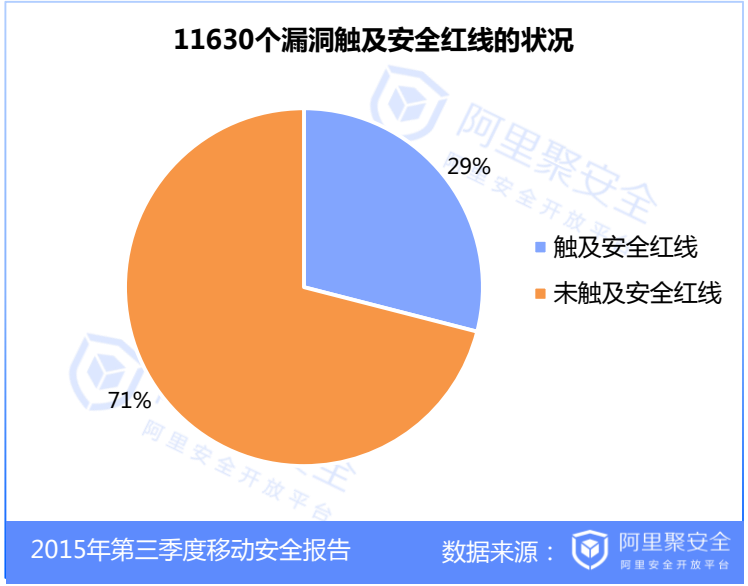
2.1 应用漏洞

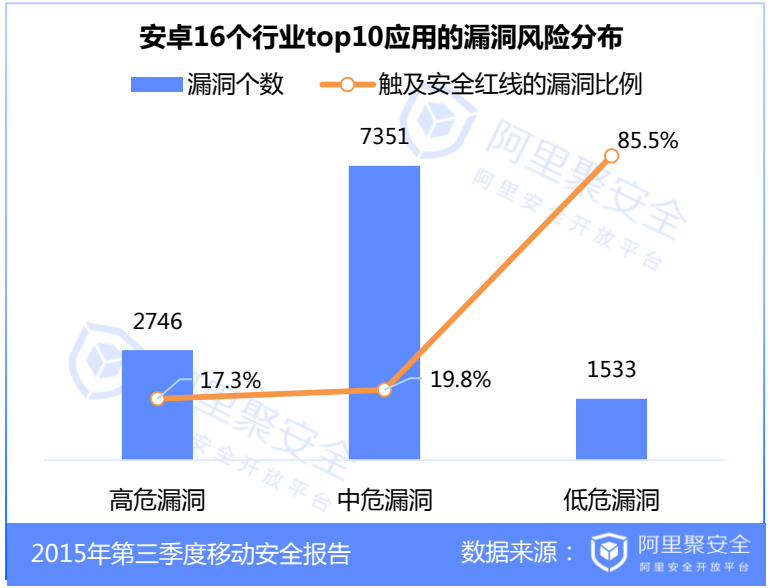
- 11630个风险漏洞中，**24%属于高危漏洞**、63%属于中危漏洞，低危漏洞仅占13%。如高危的Webview远程代码执行漏洞，攻击者利用该漏洞可以根据客户端能力为所欲为，如远程控制用户手机、盗取用户隐私信息等。



2.1 应用漏洞

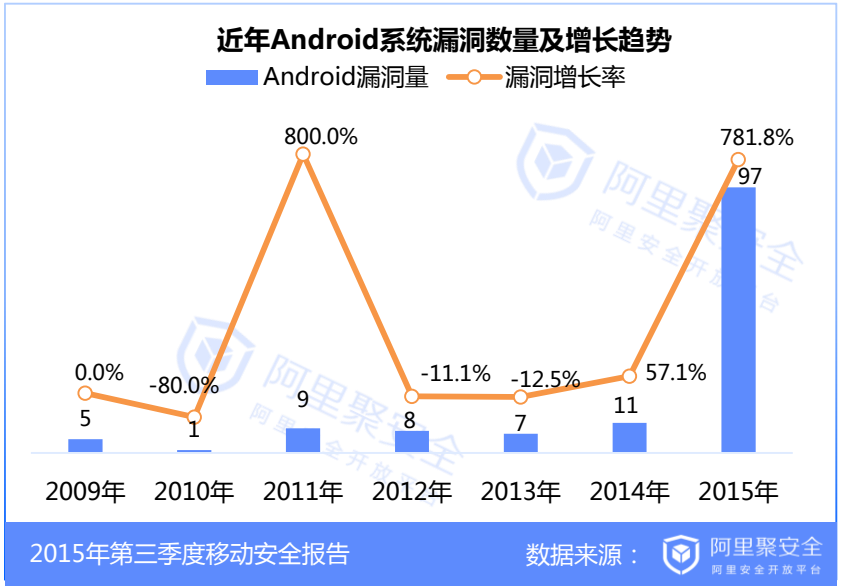
- 11630个风险漏洞中，**29%是触及安全红线**的漏洞，触及红线的漏洞容易被攻击者利用，需尽快修复以免影响应用的安全。
- 高危漏洞、中危漏洞、**低危漏洞**中，触及红线漏洞的占比依次为17.3%、19.8%、**85.5%**。低危漏洞中触及红线的漏洞占比最大，如拒绝服务漏洞，被利用后会造成应用拒绝服务，但其修复成本低，建议开发者尽快自测并修复。

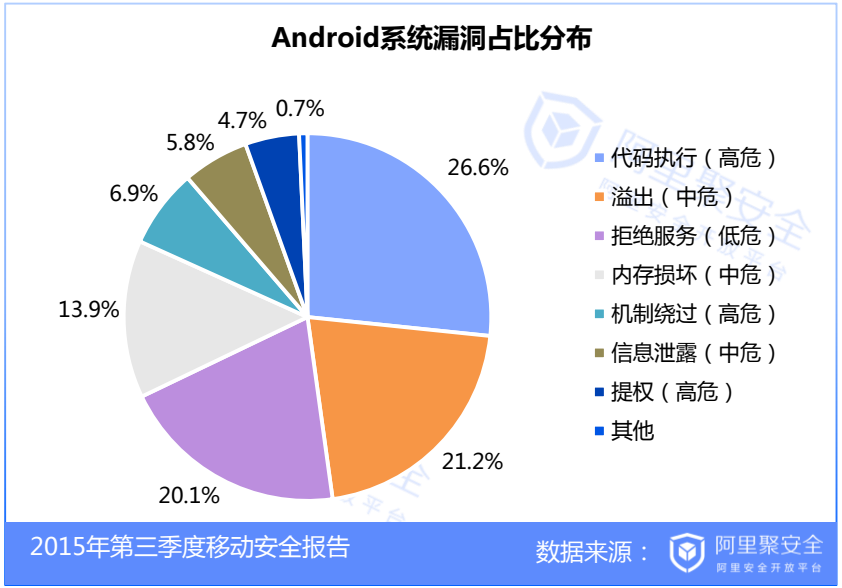




2.2 Android系统漏洞

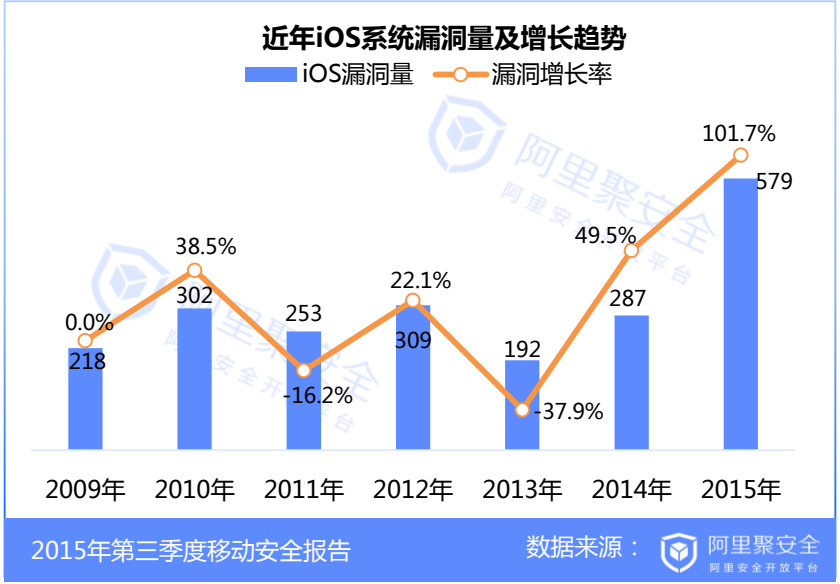
- 2015年Android系统漏洞呈爆发式增长，截至目前总漏洞量**97个**，同比**上涨781%**。2015年Android的系统漏洞量涨幅迅速，主要原因是关注移动安全的研究人员越来越多，很多以前被忽略的系统攻击被发现并从中找到了漏洞提交给google修复，相信未来Android系统会变得越来越安全。
- 2015年Android系统漏洞中，**代码执行**漏洞占比最高，达**26%**，且多数系统漏洞具有组合型，单一漏洞可能存在多种风险。

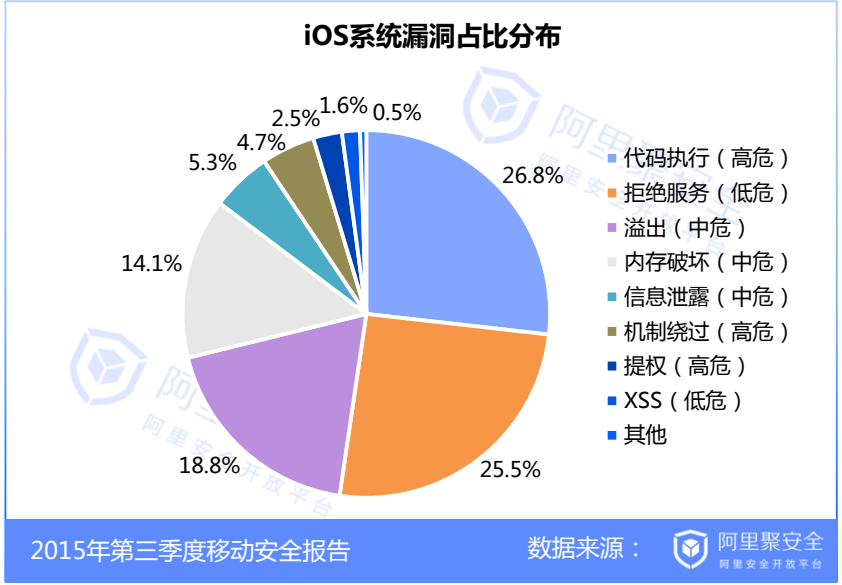




2.2 iOS系统漏洞

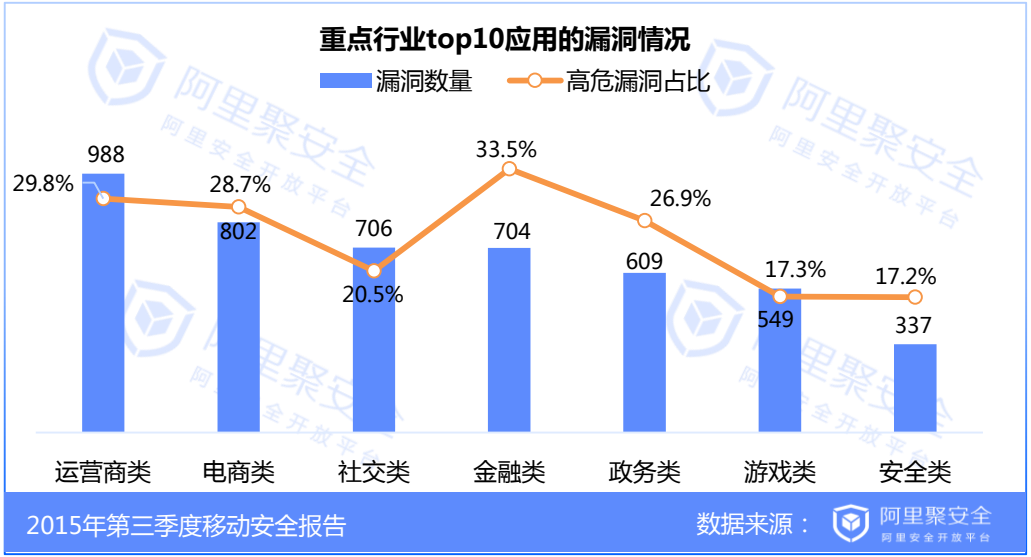
- 2015年iOS系统漏洞持续爆发，截至目前总漏洞量**579个**，同比**上涨101%**。2015年开始，苹果更加重视安全方面的投入，发现和修复了大量漏洞，同时业界越来越多的白帽子加入到苹果的安全研究中，发现漏洞并提交给苹果修复，苹果系统正在变得越来越安全。
- iOS漏洞中**代码执行、拒绝服务攻击**占比最高，分别为26%、25%。





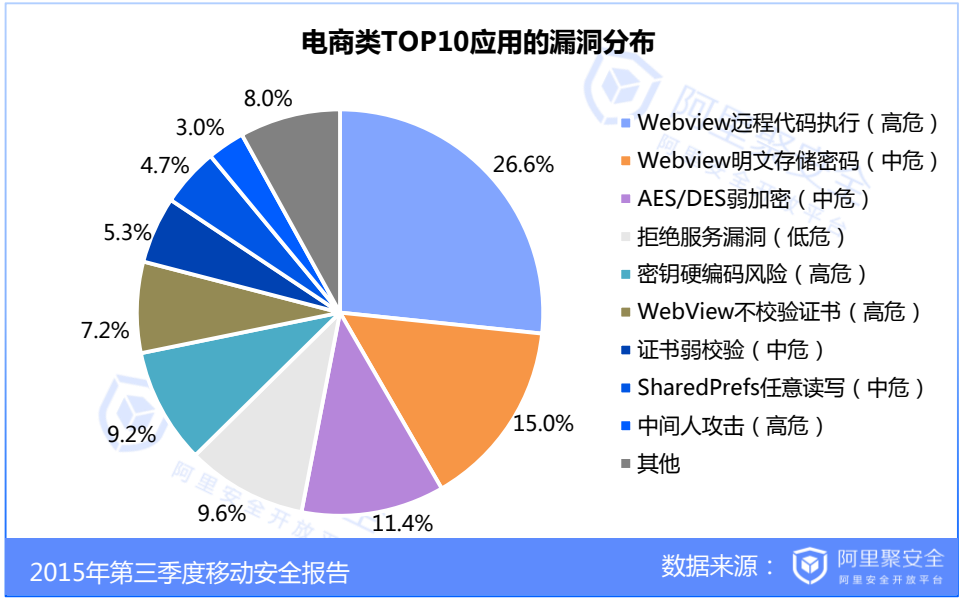
2.3 重点行业漏洞分析

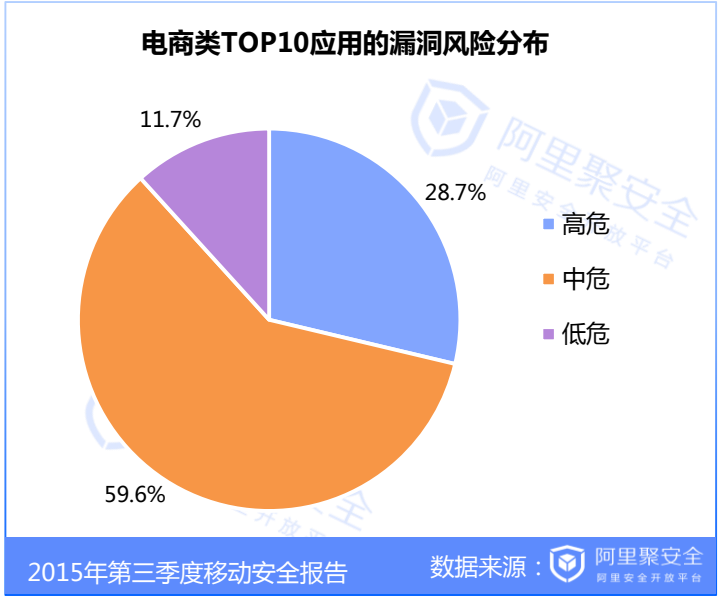
- 以下7个重点行业的top10应用共有4695个漏洞，其中**25%属于高危漏洞**如Webview远程代码执行、密钥硬编码等，可导致用户隐私信息泄露、加密信息被破解。
- **运营商类**top10应用**漏洞量最高，达988个**，且高危漏洞占比近30%。由于运营商类应用与用户话费、流量、积分等息息相关，漏洞若被黑客利用，容易造成用户资金受损，对用户的潜在影响大。
- **金融类**top10应用共704个漏洞，但其**高危漏洞占比最高，约34%**，在7个重点行业中排名第一。由于金融类应用直接与用户财产相关，开发和需引起重视。



2.3 电商行业漏洞分析

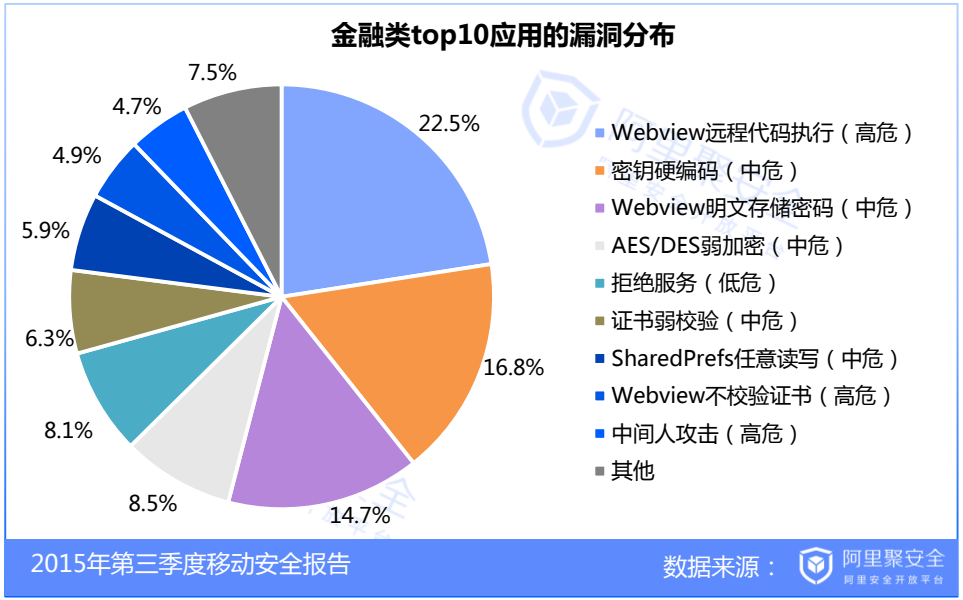
- 电商类top10应用共有**802个漏洞**，平均每个应用含**64个**漏洞，其中约27%是Webview远程代码执行高危漏洞，可导致用户手机被安装恶意扣费软件、通讯录和短信被窃取、手机被远程控制等严重后果。
- 电商类top10应用的802个漏洞中，约**29%是高危漏洞**，比16个行业的高危漏洞均值高21%，且电商类应用与用户资金密切相关，开发者应保持密切关注，采取安全方案尽快修复危险漏洞，确保用户利益和企业信誉不受影响。

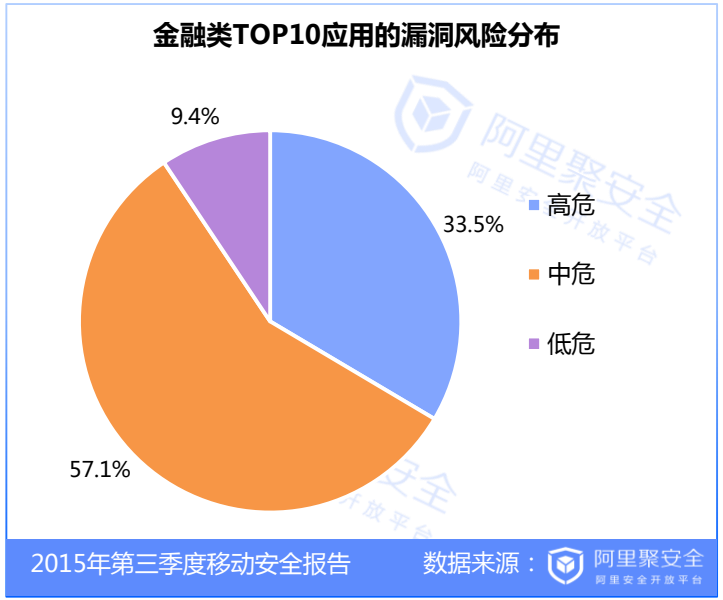




2.3 金融行业漏洞分析

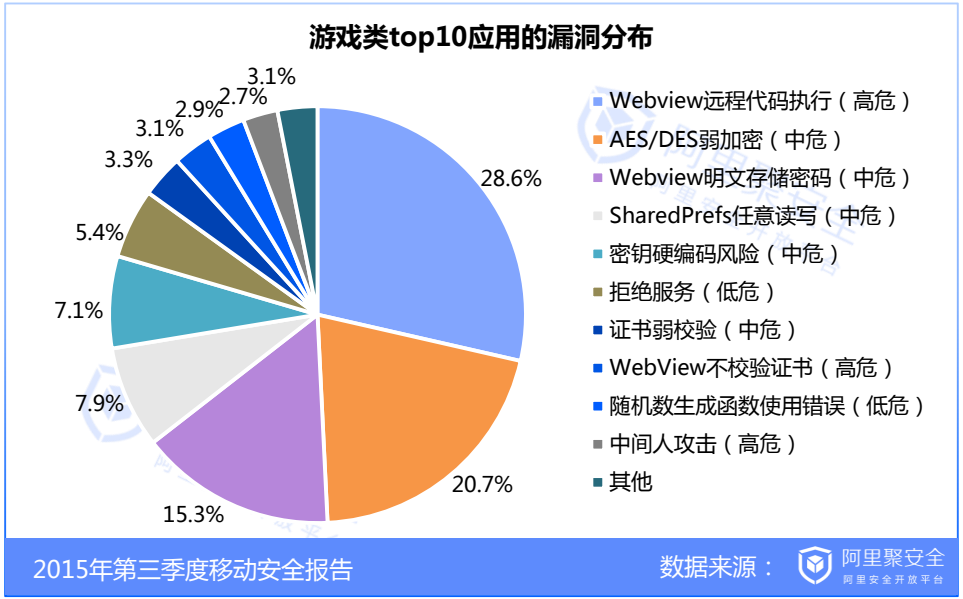
- 金融类top10应用有**704个**漏洞，平均每个含**70个**漏洞，其中22%是Webview远程代码执行高危漏洞，可导致用户手机被安装恶意扣费软件、通讯录和短信被窃取、手机被远程控制等严重后果。
- 金融类top10应用的704个漏洞中，约**34%是高危漏洞**，比16个行业的高危漏洞均值高42%，在7个重点行业中高危漏洞最多。由于金融类应用与用户财产息息相关，存在的漏洞隐患给用户财产带来巨大潜在风险。

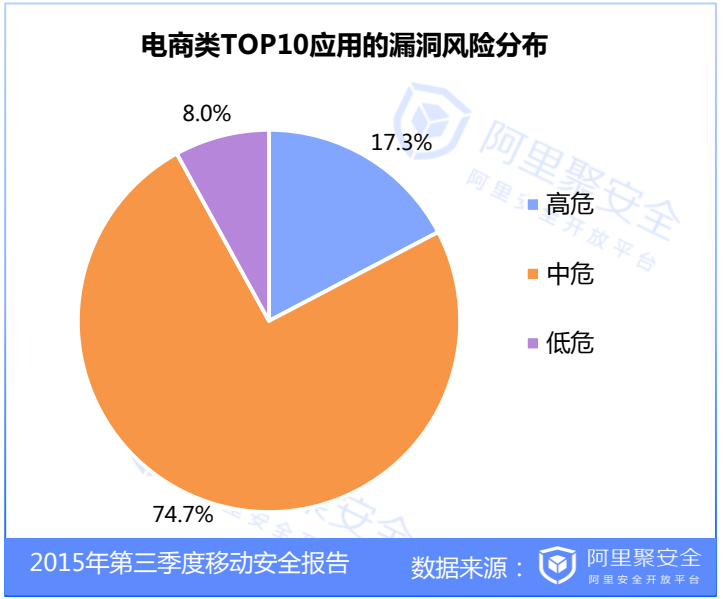




2.3 游戏行业漏洞分析

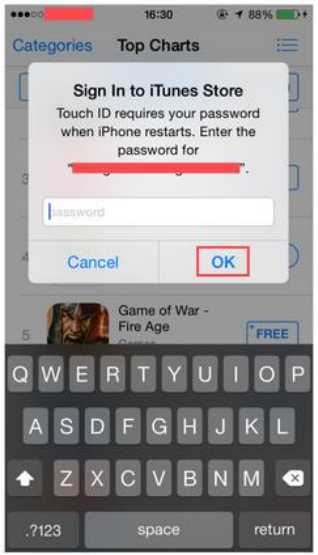
- 游戏类top10应用有**549个**漏洞，平均每个应用含**55个**漏洞。其中29%是Webview远程代码执行高危漏洞，可导致用户手机被安装恶意扣费软件、通讯录和短信被窃取、手机被远程控制等严重后果。
- 游戏类top10应用的549个漏洞中，约**17%是高危漏洞**，比16个行业的高危漏洞均值低29%，在7个重点行业中高危漏洞最少。游戏类应用开发周期短，资金变现快，用户下载量大，存在的漏洞风险亦不容忽视。



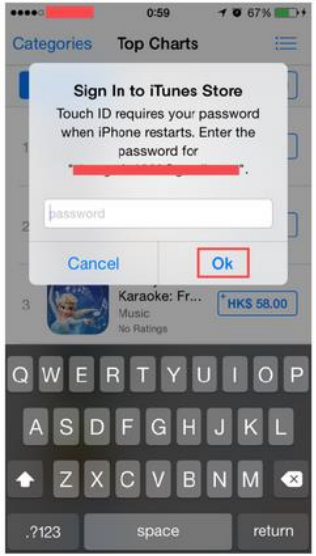


2.4 典型漏洞案例

- 9月发布的iOS 9升级中，Apple修复了阿里移动安全发现的三处漏洞：CVE-2015-5838, CVE-2015-5834, CVE-2015-5868。
- 其中**CVE-2015-5838**漏洞可让黑客在非越狱的iPhone 6上进行钓鱼攻击，并**盗取Apple ID的密码**。由于仿冒的App Store登录框与原版一模一样，用户很难察觉，输入Apple ID的密码后，导致账号被盗。
- CVE-2015-5834和CVE-2015-5868是kernel层的信息泄露和代码执行漏洞，黑客组合两者可以获取内核信息，执行任意代码。



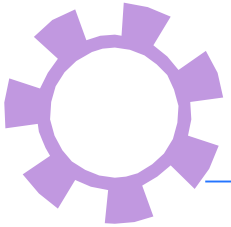
原版的AppStore登录窗口



仿冒的AppStore登录窗口

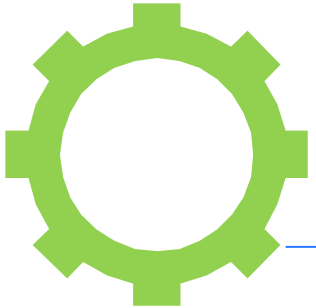
CVE-2015-5838漏洞盗账号原理

3. 仿冒情况



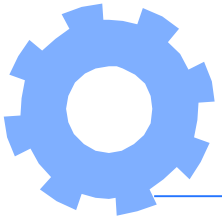
仿冒规模

16个行业top10应用中，94%的应用存在病毒仿冒应用，总仿冒应用量高达8796个，相比第二季度增长12%。



仿冒风险

仿冒病毒应用以恶意扣费、流氓行为、隐私窃取为主，对用户资产、体验、隐私造成影响。



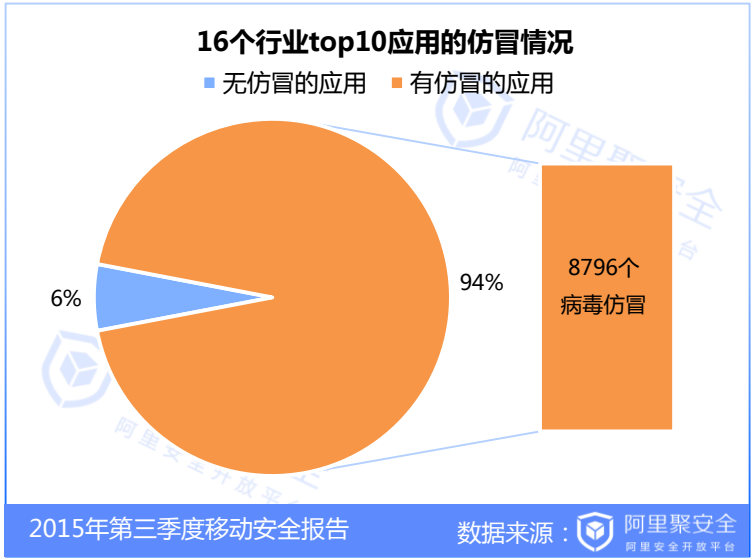
行业仿冒

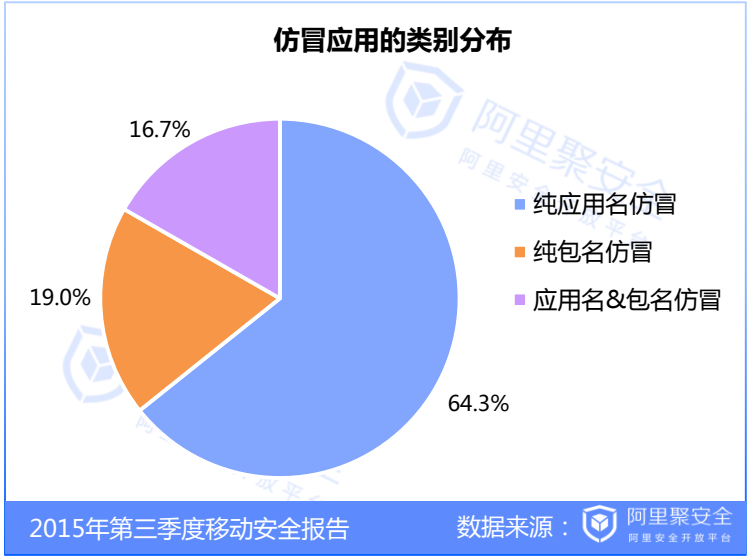
16个行业top10应用中，社交、游戏两个重点行业的仿冒量最高，两者top10应用总仿冒量4477个，占16个行业总仿冒量的51% ，其他行业仿冒量也不容乐观。

- 报告中仿冒分析数据依托于阿里聚安全仿冒检测引擎，可对全网应用渠道进行持续监测，收集仿冒应用、二次打包等各种威胁。
- 仿冒分析选取的安卓16个行业包括：金融、电商、游戏、运营商、政务、社交、安全、办公、工具、教育、旅游、摄影、生活、新闻、影音、阅读。

3.1 仿冒规模

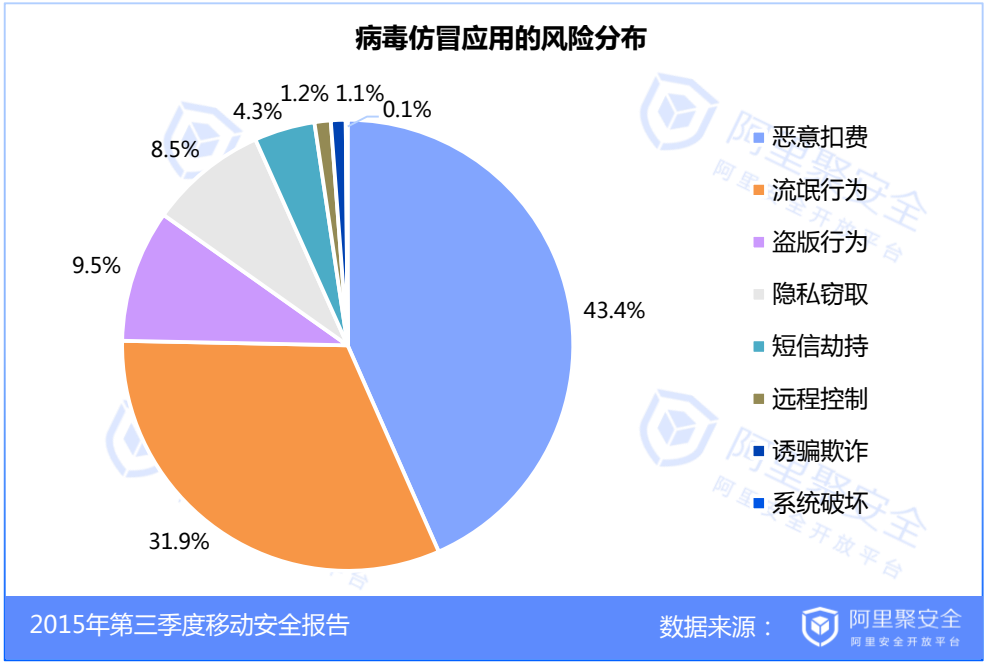
- 16个行业top10应用**96%**存在病毒仿冒，总病毒仿冒量高达**8796个**，平均每个应用的仿冒量达57个，比第二季度**增长12%**。
- 仿冒应用使用的手段中，单纯仿冒正版软件应用名称的仿冒量占64%（5653个），单纯仿冒正版软件包名的仿冒量占19%（1672个），两者结合的仿冒量占17%（1471个），可见不良开发者最喜欢使用正版应用的名称来开发仿冒应用。
- 病毒仿冒应用利用与正版相似的特征，诱导用户下载安装，之后实施相应的病毒行为，对用户的危害极大，用户需谨慎。





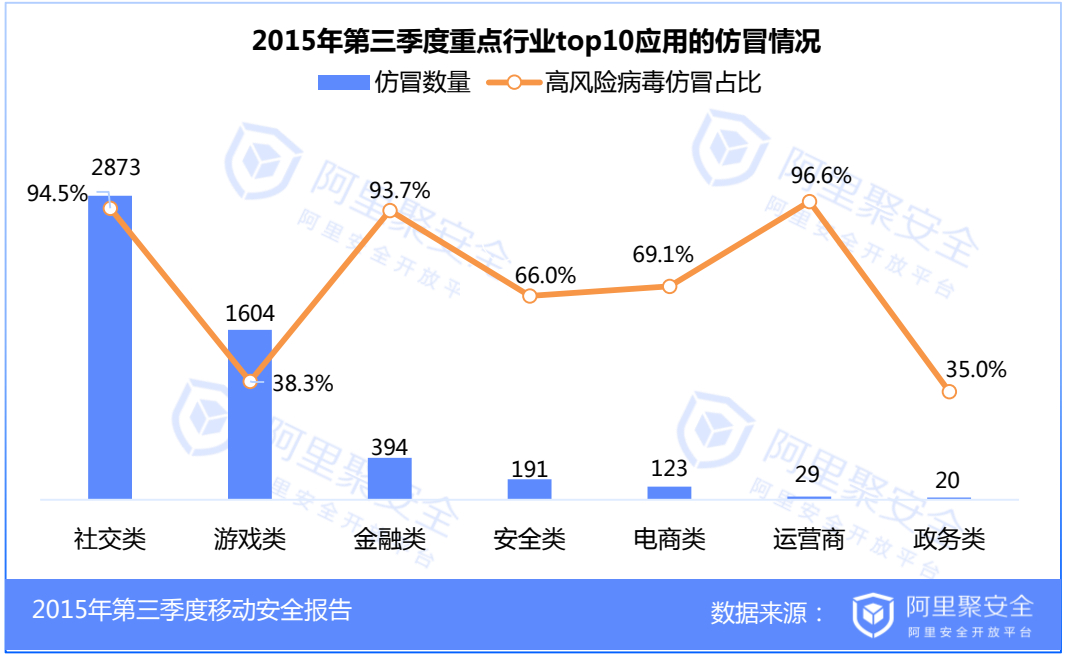
3.2 仿冒风险

- 16个行业top10应用的8796个病毒仿冒中，**恶意扣费**类病毒软件占比高达**43%**，比第二季度**增长18%**。该类病毒应用未经用户允许私自发送短信和扣费指令，对用户的手机，资费造成一定风险，需谨慎使用。
- 流氓行为类病毒仿冒占比32%，比第二季度下降19%。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。



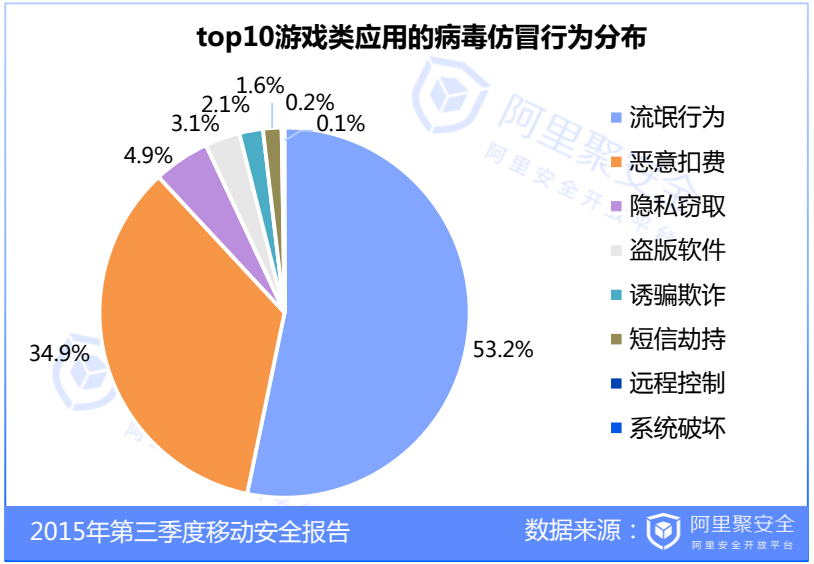
3.3 重点行业仿冒分析

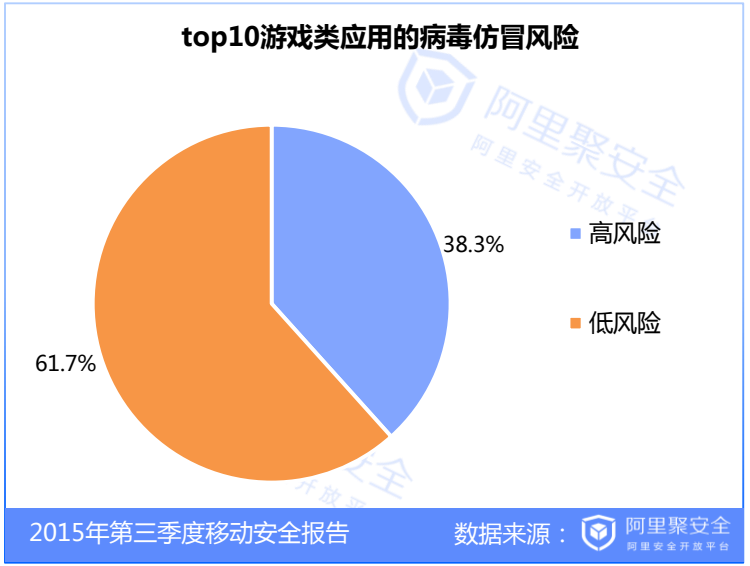
- 以下7个行业top10应用共有5234个病毒仿冒，约占16个行业总仿冒量的**60%**，其中**社交、游戏**类应用是病毒仿冒的重灾区。
- 社交、金融、运营商行业的**高危病毒仿冒占比超90%**，对正版应用开发者和用户都会造成巨大危害，建议正版开发商使用相关安全方案如阿里聚安全来自测应用的仿冒情况，并及早联系各渠道下架。



3.3 游戏行业仿冒分析

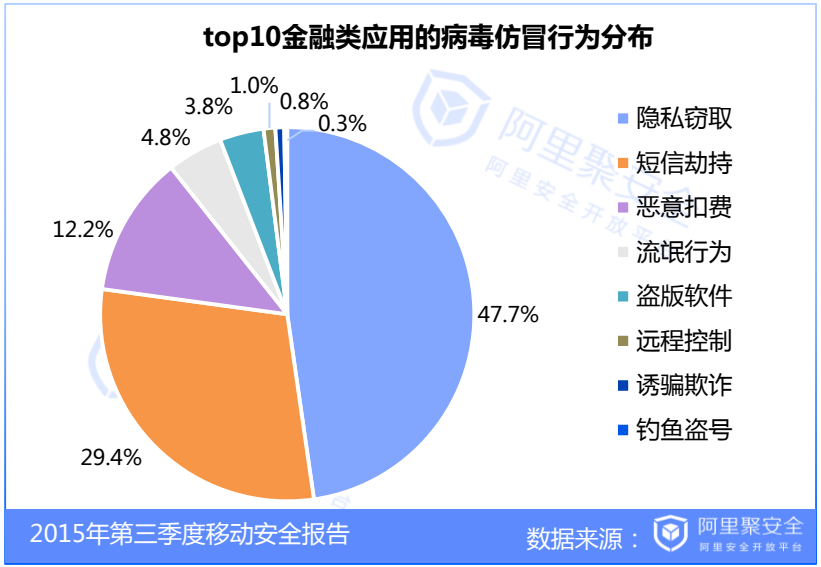
- **100%**的top10游戏类应用含病毒仿冒软件，总**仿冒量1604个**，与第二季度持平，其中38%是高风险的仿冒病毒应用。
- 1604个病毒仿冒应用中，**53%**的仿冒应用具有**流氓行为**，在游戏中弹出骚扰广告、匿名弹窗等，严重影响用户体验。此外**35%**的仿冒应用具有**恶意扣费**行为，容易导致用户手机流量消耗，或游戏账户中的资金受损。
- 游戏应用以数量多、变现快，收益高的特性，易受不良开发者仿冒，影响正版开发者和用户的利益，其仿冒问题应引起重视。

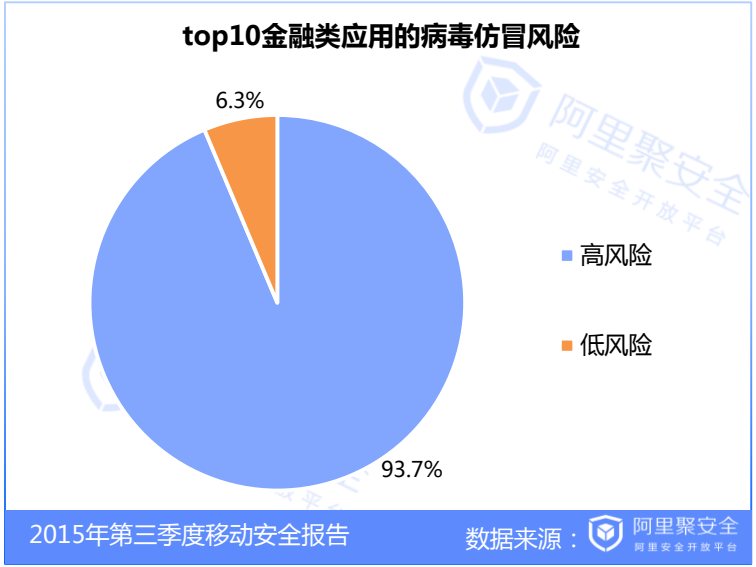




3.3 金融行业仿冒分析

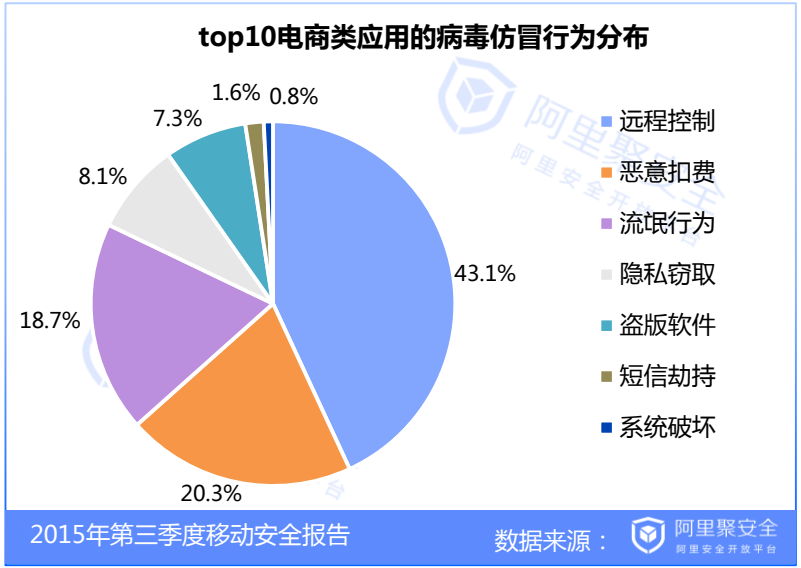
- **100%**的top10金融类应用含病毒仿冒软件，总**仿冒量394个**，比第二季度增长166%。
- 394个病毒仿冒应用中，**94%是高风险**病毒应用，具有隐私窃取、短信劫持、恶意扣费等行为。由于金融类应用涉及用户资产信息，这些高风险仿冒应用对用户的危害极大，需提高警惕。
- 394个病毒仿冒应用中，**48%**的仿冒应用有**隐私窃取**行为，容易造成用户隐私信息泄露，进而影响金融账户资金等。

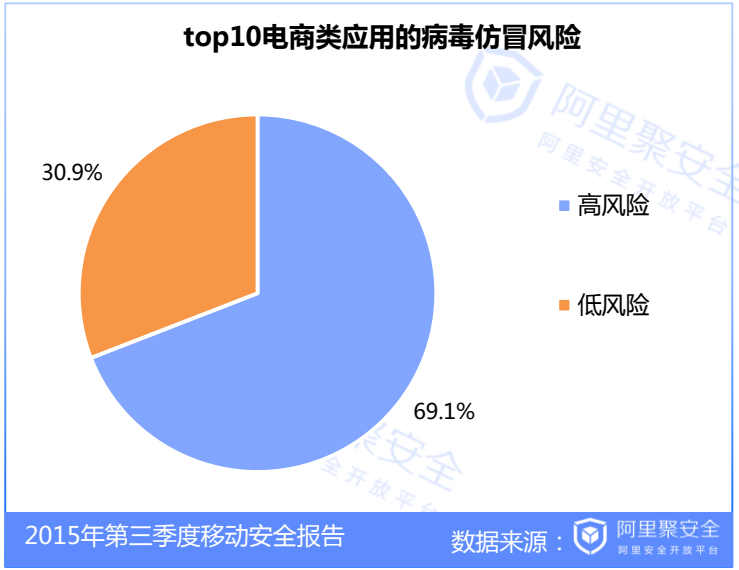




3.3 电商行业仿冒分析

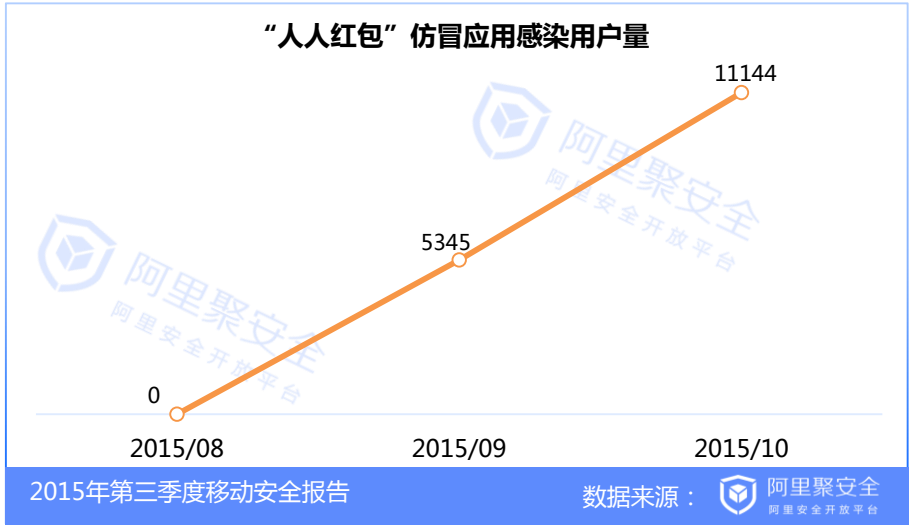
- **90%**的top10电商类应用含病毒仿冒软件，总**仿冒量123个**，且**69%是高风险**病毒应用，具有远程控制、恶意扣费等行为。由于电商类应用涉及用户网购行为、账户资产等敏感信息，这些高风险仿冒应用对用户的危害极大，需提高警惕。
- 123个病毒仿冒应用中，**43%**的仿冒应用有**远程控制**行为，容易导致用户手机被黑客控制，导致隐私信息泄露、账号被盗等风险。

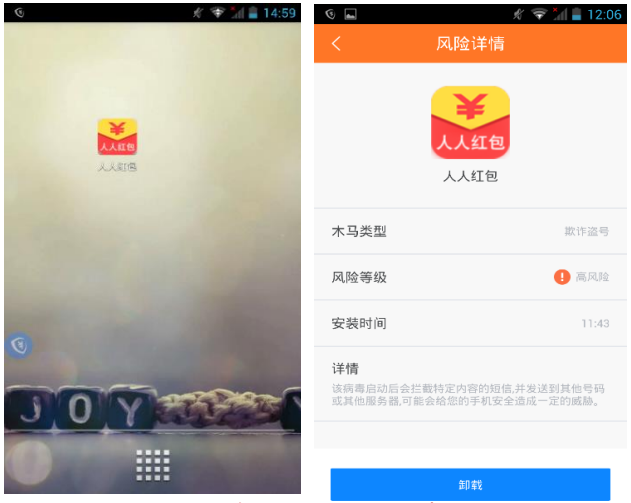




3.4 典型仿冒案例

- **“人人红包”**应用在9月份开始爆发，截至目前已**感染用户量1.6万**，且10月份感染量上涨趋势迅猛。不法分子通过推送节日祝福短信如“xxx，我给你发了一份中秋红包，点击链接下载安装就可领取了。”到用户手机上，诱导用户点击下载安装。
- 一方面，该病毒安装后会隐藏图标不让用户察觉，并私自将用户的收发短信、通讯录等信息发送到远程服务器，还会私自下载推广软件，恶意消耗手机流量，甚至对用户的资产带来风险。
- 另一方面，该病毒会向通讯录联系人群发短信进行传播，好友收到后看到是认识的人发来的短信，误以为真，打开短信中的链接下载安装后被感染，形成放射性传播，导致感染量迅速上升，建议用户提高警惕。

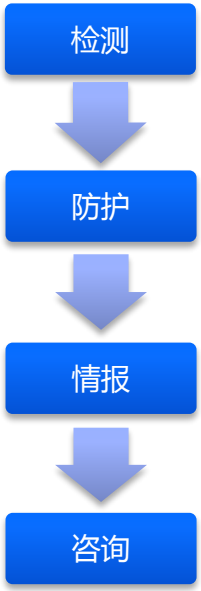




“人人红包”图标及钱盾查杀界面

阿里聚安全-应用安全解决方案

- 针对移动应用存在的安全问题，阿里聚安全提供完整的应用安全解决方案，包括发现风险（恶意代码检测、漏洞检测、仿冒检测）、安全增强（应用加固、安全组件）、风险持续监控等功能，保护移动应用全生命周期的安全风险可控。



恶意代码检测
- 快速检测恶意代码，外包APP安全性检测
- 第三方SDK代码安全性检测

漏洞扫描
- 业界最全的自动化漏扫引擎
- 发现应用自身安全风险，并提供分级机制与修复建议

安全评估服务
- 业界顶尖安全专家团队评估
- 深度渗透移动应用及相关业务，发掘安全隐患

安全沙箱
- 快速组件化接入
- 业界独创的端安全能力
- 亿级应用久经攻防考验

应用加固
- 提供了快速加固，多渠道加固以及自定义加固，对抗各类分析工具
- 实战验证高兼容性、高稳定性、高性能

漏洞响应
- 业界漏洞、安全风险第一时间通报
- 应急响应方案建议

仿冒监测
- 大数据监测全网活跃应用，关注论坛，网盘等高风险渠道
- 多维度仿冒检测能力

应用风险感知
- App环境风险（Root / JB / 模拟器）
- App攻击风险（注入 / 篡改 / 调试）
- 业务风险

行业安全报告
- 季度 / 年度行业安全报告
- 企业与行业安全水平对比

安全流程咨询
- 移动App设计、开发、测试、上线、运营全流程安全咨询
- 上线安全标准与规范培训

更多详情请登录阿里聚安全官网：http://jaq.alibaba.com

移动安全发展趋势

移动互联网的病毒、漏洞、仿冒等安全问题由来已久，且业界已经有较多成熟的独立解决方案，但随着互联网的发展、智能设备的普及，未来以个人或家庭为中心的小生态将出现，它承载着人类生产生活的所有信息，而安全将面临更大的挑战。

■ **智能设备蓬勃发展，万物互联的美好愿景背后，安全问题日益凸显**

据Gartner和麦肯锡的预测数据显示，2015年全球连接到互联网上的设备将达49亿台，2020年或将超过260亿台，智能汽车、手机、手环、医疗设备、家电等智能设备逐渐普及到人类生产生活中，他们在为人类带来便利生活的同时，也存在巨大的安全隐患，设备厂商不够重视安全、智能设备系统多样化等都让安全问题日益凸显，这种案例已经屡见不鲜。如2015年7月，菲亚特克莱斯勒美国公司宣布召回140万辆配有Uconnect车载系统的汽车，黑客可通过远程软件向该车载系统发送指令，进行各种操作如减速、关闭引擎、让刹车失灵等，严重危害人身安全。2015年8月的黑帽大会和世界黑客大会上，包括汽车在内的各种智能设备都被爆出安全漏洞，黑客利用安全漏洞可以控制智能手机、汽车、交通红绿灯，甚至搭载有智能狙击镜的高级狙击步枪，让人惊叹不已。

移动安全发展趋势

■ 互联网安全边界日益模糊，挑战越来越大

IOT的发展给个人生活和企业带来巨大便利，万物互联及相关产业已成为全球科技界最具发展潜力的领域。快速发展的互联网、多样化的智能设备和系统、不够重视安全设计的设备生产等问题逐渐导致风险扩大，主要表现在：

- 安全的复杂性：物理实体和信息数据之间的壁垒正在被打破，安全不再局限于网络中虚拟信息本身，财产、隐私、甚至生命都已经成为安全的一部分，互联网安全已经不仅仅存在于互联网上，而在于所联的万物。
- 安全防护的挑战：对企业来说哪些位置需要安全控制、哪些边界需要划清、如何部署有效的控制，都需要专业的风险发现和控制方案。
- 硬件问题的修复不像在服务器或桌面系统中升级安装补丁那么方便，大多数智能设备的修复和缓解将变得更为复杂，弄清楚如何快速修复多样性设备的系统安全将成为挑战。

未来，互联网的发展使安全风险无处不在，如何发现并解决好这些安全问题，保护广大用户的权益是阿里巴巴移动安全团队一直努力的方向，面对庞大复杂的万物互联世界，我们会与智能硬件、互联网服务平台等产业链相关厂商紧密配合，提供有针对性的安全方案，推动行业平稳健康发展。

安全建议

阿里聚安全
阿里安全开放平台

◆阿里聚安全

阿里聚安全是面向开发者和企业的安全开放平台，具备应用安全解决方案，和业务风控服务，护航业务健康发展，共创安全生态。

- 风险检测：恶意代码检测、漏洞扫描、仿冒检测
- 安全方案：应用加固、安全沙箱
- 持续监控：ROOT环境监测、模拟器检测、人机检测、调试检测、篡改检测、注入检测
- 业务风控：垃圾注册、账号被盗、营销作弊、渠道作弊

阿里钱盾
钱有盾 盗无门

◆阿里钱盾

阿里钱盾着力保护移动端用户的网购及资金交易安全，首创网购全流程安全防护。用户可通过下载阿里钱盾，保护手机安全，如网购资金、隐私信息等。

版权声明

本季度报告由阿里移动安全团队撰写，数据来源于阿里聚安全和阿里钱盾的监测数据。报告中所有的文字、图片、表格所有权归阿里移动安全所有，任何组织或个人，不得使用本报告中的信息用于任何商业目的、复制、改编或发布。若需引用，请注明出处，且不得对本季报进行有悖原意的引用或改版。

阿里聚安全微信公众号

阿里移动安全官方微博：http://weibo.com/alimobilesecurity

阿里聚安全：http://jaq.alibaba.com

阿里钱盾：http://qd.alibaba.com

阿里聚安全微信公众号：阿里聚安全

阿里钱盾微信公众号：阿里钱盾