Alibaba Group 阿里巴巴集团

ALIBABA SECURITY AGENCY

阿里安全
2015年第二季度移动安全报告

阿里巴巴移动安全

阿里聚安全
移动安全开放平台

阿里钱盾
钱有盾 盗无门

病毒

- 2015年第二季度，安卓平台受病毒感染设备与第一季度相比小有增长，平均约8.7台设备有1台设备染毒。
- 恶意扣费类病毒样本占比最高，但在感染用户量方面，流氓行为类病毒超过恶意扣费类成为感染用户数占比最高的病毒类型。
- 广东依旧是染毒用户量最多的省份，贵州的人均染毒比例最高。

漏洞

- 16个行业的top10应用100%存在漏洞风险，平均每个应用含53个漏洞。
- 热门应用漏洞以拒绝服务漏洞为主，占比达22%，容易造成APP拒绝服务。
- 影音类、生活类、旅游类、工具类等行业的top10应用漏洞数量最多，平均漏洞量超过80个。

仿冒

- 16个行业top10应用中，86.3%的应用存在仿冒，每个应用平均含49个仿冒。
- 仿冒病毒应用以流氓行为、恶意扣费为主，影响用户体验，费用莫名被扣等。
- 16个行业的top10应用中，金融、社交、购物、新闻、影音、游戏类应用100%被仿冒，社交类应用仿冒量最高。

目录

1. 病毒情况

病毒规模

- 2015年第二季度，安卓平台平均约8.7台设备就有1台设备染毒，与上一季度相比小有增长，但总中毒设备量高达2877万，比上一季度增长96.2%。
- 2015年第二季度，阿里聚安全病毒库共新增病毒样本量266.6万，比上一季度增长59.6%。

病毒类型

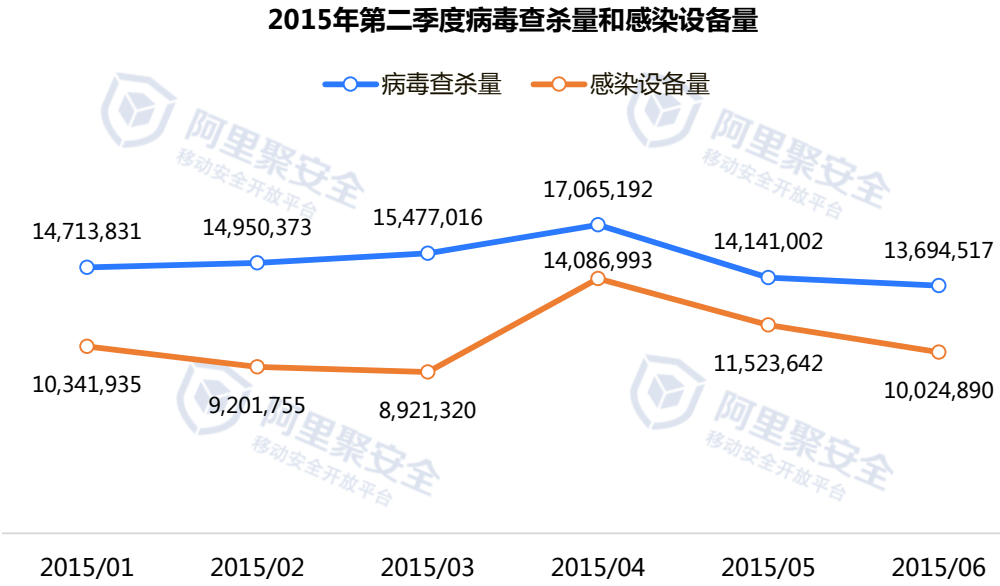
- 第二季度恶意扣费类病毒样本占比最高，达52%。
- 流氓行为类病毒超过恶意扣费类成为感染用户占比最高的病毒类型。

感染区域

- 第二季度，广东仍是受病毒感染最严重的地区，感染量占全国的13.6%，比一季度上涨8%。贵州是最易被病毒感染的省份，其设备感染率为15.2%。

1.1 病毒规模

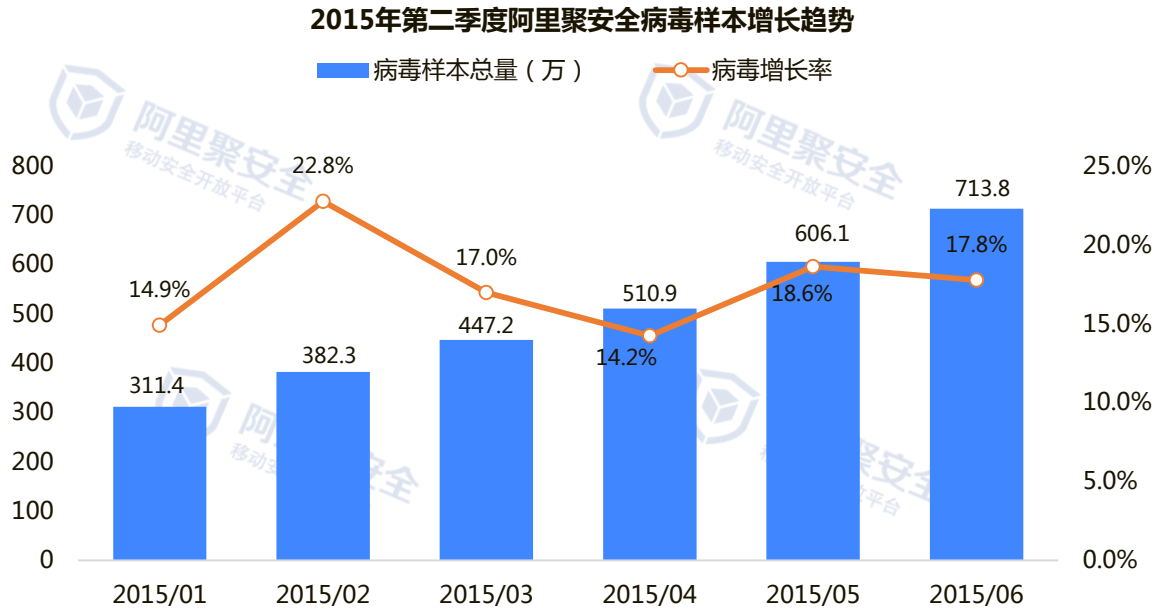
- 2015年第二季度，安卓平台平均约**8.7台设备有1台设备染毒**，总中毒设备量高达**2877万**，比上一季度**增长96.2%**。
- 2015年第二季度，设备感染量呈逐月下降趋势，但仍应保持关注。
- 2015年第二季度，阿里聚安全病毒扫描引擎共查杀病毒**4490万**次，帮助用户抵御了大量的病毒风险。



数据来源：阿里聚安全监控数据

1.1 病毒规模

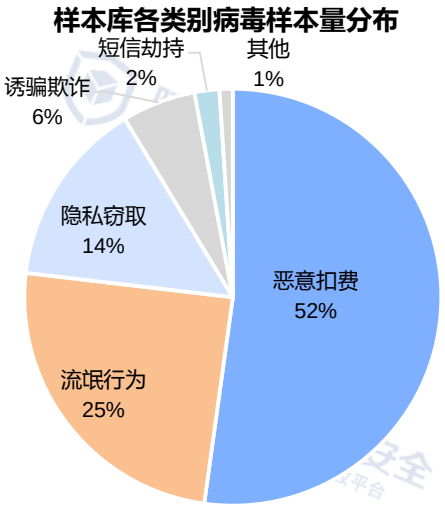
- 阿里聚安全病毒样本库持续增长，2015年第二季度新增**266.6万**病毒样本量，比上一季度**增加59.6%**。第二季度内的月均增长率为16.8%，呈平稳增长趋势。

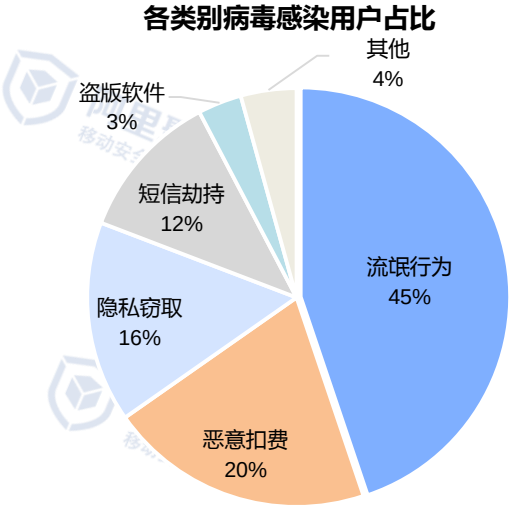


数据来源：阿里聚安全监控数据

1.2 病毒类型

- **恶意扣费类病毒**样本占比最高，达**52%**，与上一季度持平，其感染用户占比为20%。由于此类病毒能够直接获益，因此备受黑客青睐，用户需提高警惕。
- 流氓行为类病毒以25%的样本占比，感染了**45%**的用户群体，其对用户造成的骚扰和危害不容忽视。
- 隐私窃取类病毒感染用户占比为16%，比上一季度下降33%。
- 短信劫持类病毒感染用户占比为12%，比上一季度**上涨75%**，其感染趋势的迅猛程度可见一斑。





数据来源：阿里聚安全监控数据

1.2 病毒类型

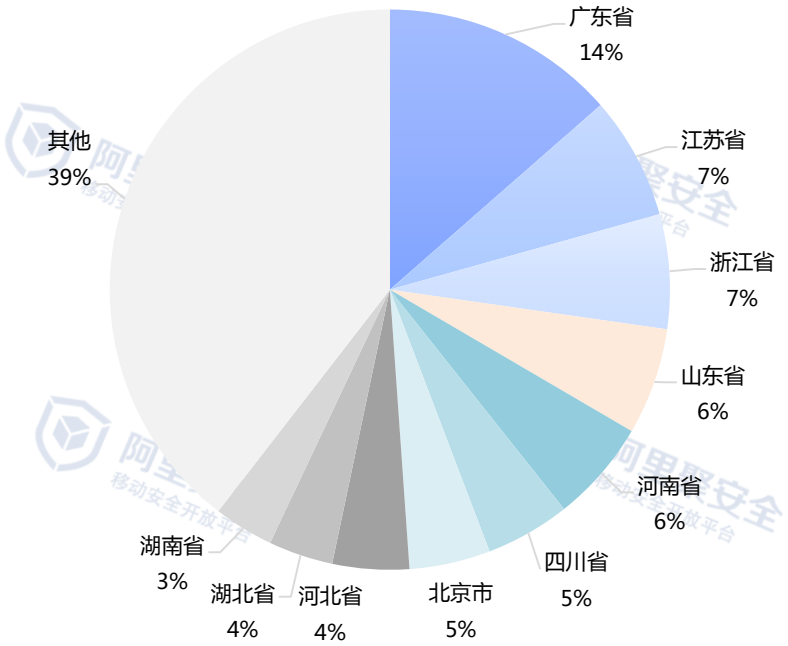
病毒名	病毒类型	感染量	病毒描述
消灭糖果星星	流氓行为	1085321	该软件包含可疑行为，启动后可能会给您的手机安全造成一定的威胁。
成人快播	短信劫持	659822	该病毒启动后私自发送短信，拦截相关短信，可能与付费有关，请谨慎使用！
果汁四溅	流氓行为	658310	该软件包含可疑行为，启动后可能会给您的手机安全造成一定的威胁。
香艳视频	恶意扣费	614604	该木马存在扣费陷阱，以及会下载广告应用自动安装，可能会对您造成一定的风险，请谨慎使用。
喜羊羊快跑	短信劫持	547184	该软件会私自拦截用户短信并删除，可能与付费相关，请谨慎使用。
微小秘	流氓行为	330518	该软件具有影响用户操作体验的行为，可能会给您的手机安全造成一定的威胁。
avi视频	恶意扣费	326935	该应用启动后会拦截并回复相关短信，可能会订购相关付费业务，给您带来经济上的损害！
gplayer	系统破坏	323259	该病毒启动后隐藏图标，私自发送短信，获取隐私信息，运行相关敏感代码，可能会对您的利益造成损害，请谨慎使用！
无码神播	恶意扣费	313551	该病毒具有启动后未经用户允许私自发送短信等恶意行为，可能会给您的手机造成一定的经济损失。
Screen Filter	系统破坏	310411	当调节屏幕至完全黑暗的时候会造成手机假死的情况，而应用本身未给予用户提示，也未设置快捷键恢复默认亮度，请谨慎使用。
微秘书	流氓行为	296963	该软件具有影响用户操作体验的行为，可能会给您的手机安全造成一定的威胁。

数据来源：阿里聚安全监控数据

1.3 感染用户分布

- **广东**是受感染用户量最多的省份，其第二季度的设备感染量占全国总感染量的**14%**，广东，江苏，浙江成为设备感染量最多的TOP3省份。

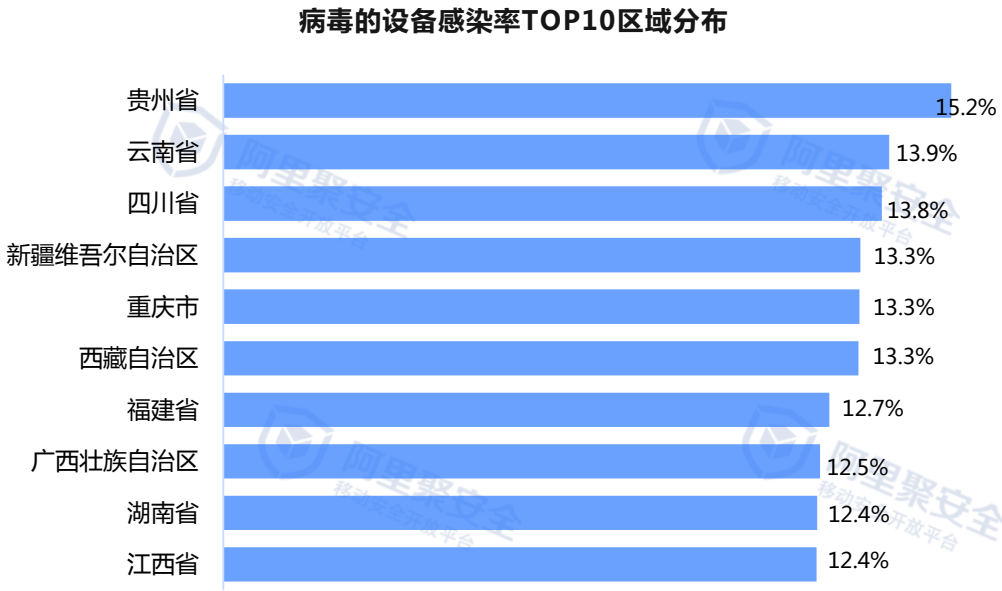
2015年第二季度各省份设备感染量占比分布



数据来源：阿里聚安全监控数据

1.3 感染用户分布

- **贵州**是最易被病毒感染的省份，每6.6台手机就近1台染毒，比全国平均值高**31%**。染毒设备比例最高的省份多分布在中西部，贵州、云南、四川是中毒比例最高的三个省份。全国**平均中毒设备比例高达11.4%**。



数据来源：阿里聚安全监控数据

2. 漏洞总体情况

应用漏洞

- 16个行业的top10应用共有8515个漏洞，均值53个，比上一季度增加77%。
- 16个行业的top10应用100%有漏洞，且高风险漏洞占32%，比上一季度略有下降。

系统漏洞

- Android系统漏洞近年居高不下，2015年系统漏洞量同比上涨15%，风险高。
- iOS系统漏洞近年持续爆发，2015年iOS漏洞量环比上涨60%，iOS也不再安全。

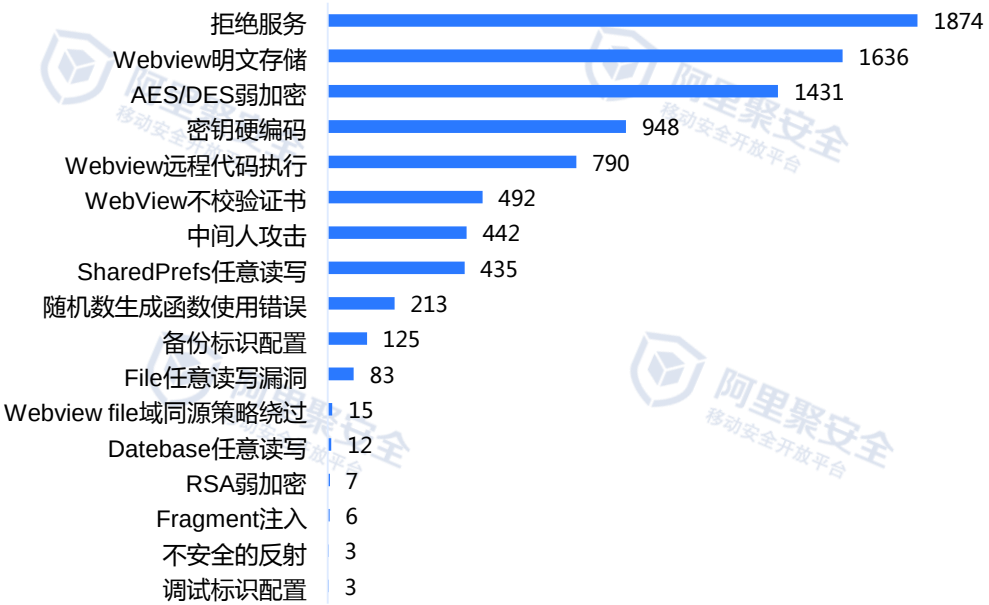
行业漏洞

- 影音、生活、旅游类的应用漏洞总量最多，由于用户量大，漏洞潜在的影响也较大。
- 金融、工具、旅游类的高危漏洞占比最高，均占40%左右。

2.1 应用漏洞

- 安卓16个行业的top10应用共有**8515个**漏洞，平均每个应用有**53个**漏洞，比上一季度增加**77%**，增长量非常迅速。
- 16个行业的top10应用**100%**都有漏洞，且以拒绝服务为主，相比上一季度**增长107%**。在业界爆出Android APP通用拒绝服务漏洞后，阿里聚安全的漏洞扫描引擎快速增加该扫描能力，帮助开发者发现安全隐患。

2015年第二季度安卓16个行业top10应用的漏洞类别和数量

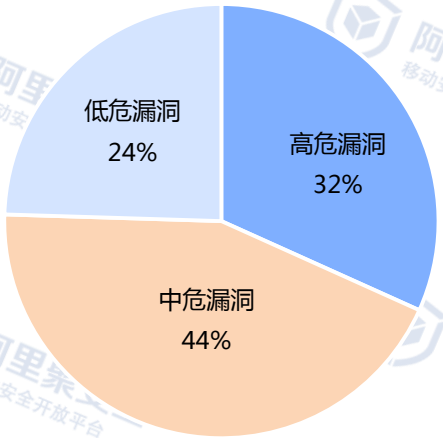


数据来源：阿里聚安全监控数据

2.1 应用漏洞

- 8515个风险漏洞中，**32%属于高危漏洞**、44%属于中危漏洞，低危漏洞仅占24%，可见移动应用漏洞问题的严峻性。

安卓16个行业top10应用的漏洞风险分布

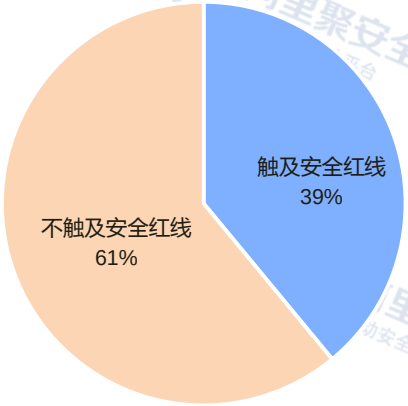


数据来源：阿里聚安全监控数据

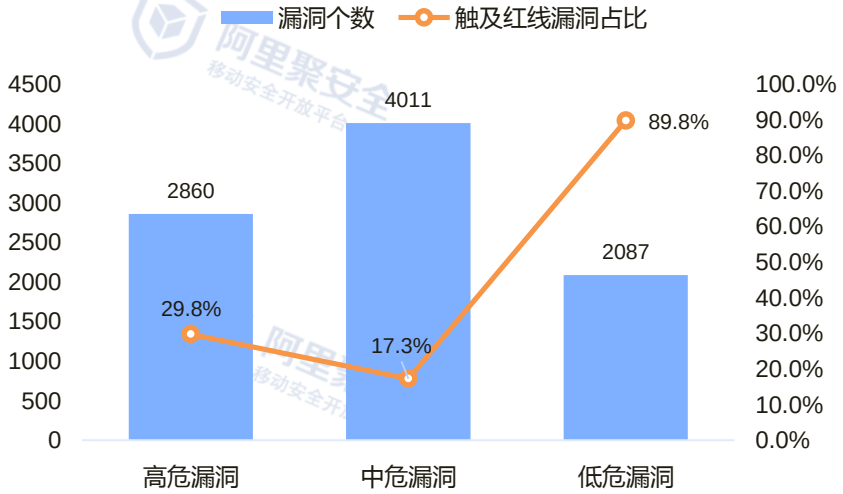
2.1 应用漏洞

- 8515个风险漏洞中，**39%**属于**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APP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29.8%、17.3%、**89.8%**。在低危漏洞中触及红线漏洞的占比最大，如拒绝服务漏洞，被利用后会造成APP拒绝服务，但其修复成本低，建议开发者快速修复。

8515个漏洞触及安全红线的情况



安卓16个行业top10应用的漏洞风险分布

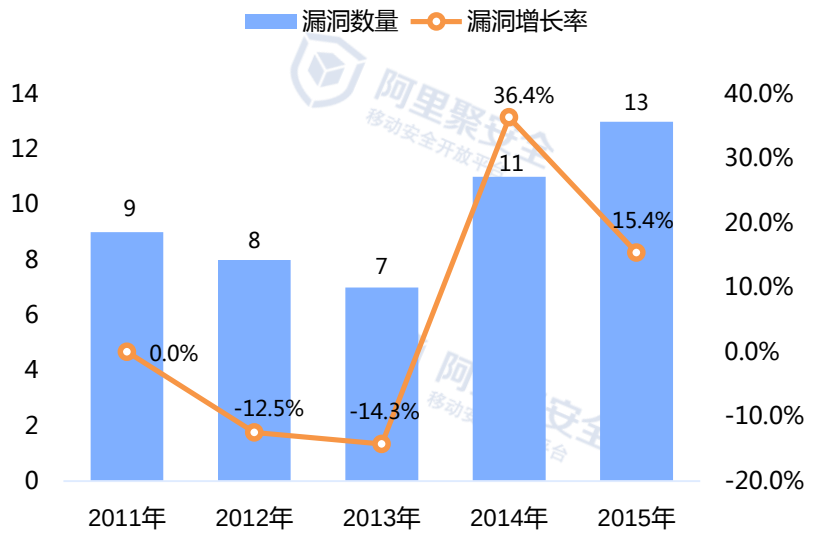


数据来源：阿里聚安全监控数据

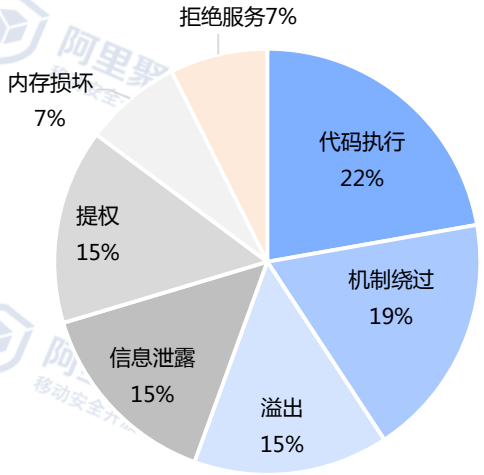
2.2 系统漏洞

- Android系统漏洞近年居高不下，2015年系统漏洞量同比上涨**15.4%**，风险依旧严峻。
- 2015年Android系统漏洞中，**代码执行**漏洞占比最高，达**22%**。
- 多数系统漏洞具有组合型，单一漏洞可能存在多种风险。

近年Android系统漏洞量趋势



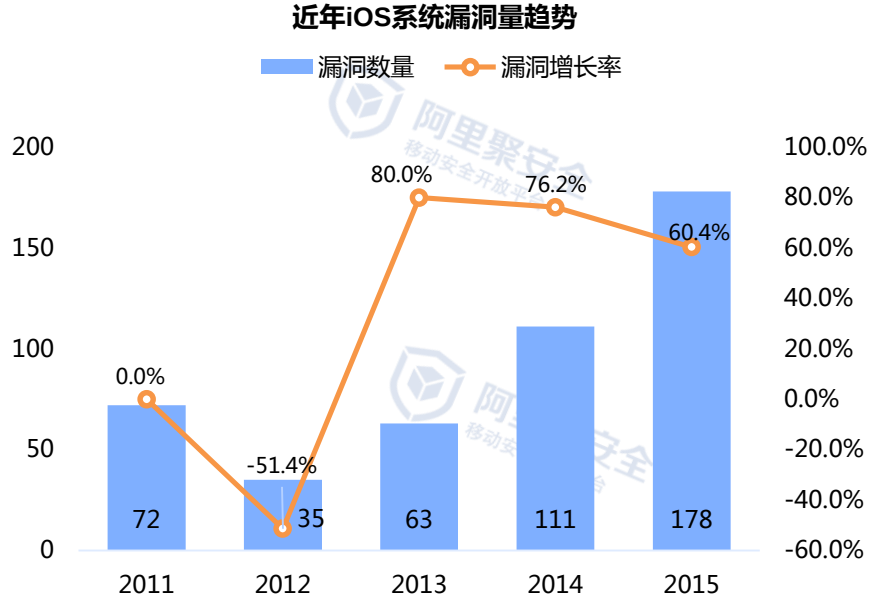
Android系统漏洞分类

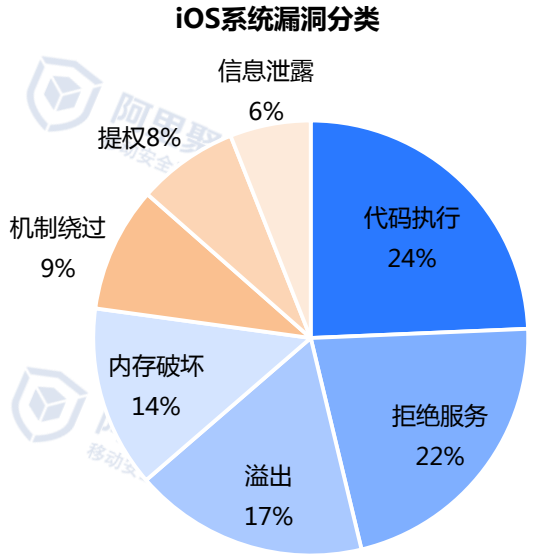


数据来源：阿里聚安全监控数据

2.2 系统漏洞

- iOS系统漏洞近年持续爆发，2015年iOS漏洞量同比**上涨60.4%**，iOS也不再安全。
- iOS漏洞中**代码执行、拒绝服务攻击**占比最高，分别为24%、22%。
- 由于iOS系统安全机制比较复杂，iOS的攻击或者越狱需要多种类型漏洞配合进行。





数据来源：阿里聚安全监控数据

2.3 典型漏洞案例

CVE-2015-3636

CVE-2015-3636漏洞（又名Pingpong），安卓4.4以后的机型和部分安卓4.3的机型都受到影响。恶意应用可以利用该漏洞直接获得系统最高权限（root）。

通用拒绝服务漏洞

安卓系统所有版本都会受到影响，安卓系统提供Intent机制来协助应用间的交互与通讯，调用的组件在处理Intent数据时，没有进行异常捕获，当处理空数据、异常或者畸形数据时会导致应用奔溃。

2.3 典型漏洞分析

CVE-2015-3636漏洞：

- 该漏洞存在于Linux Kernel自身的核心代码中，因此大多数的安卓机型都存在这一漏洞。但由于系统权限方面的限制，在安卓4.3之前的机型和部分安卓4.3的机型上无法利用该漏洞。
- 恶意应用利用这一漏洞，可以在后台直接获得系统最高权限，从而进一步实行恶意行径。可导致用户手机被远程控制，信息泄露等危害。

CVE-2015-3636漏洞恶意行径原理

数据来源：阿里聚安全监控数据

2.3 典型漏洞分析

通用拒绝服务漏洞：

- 安卓系统提供Intent机制来协助应用间的交互与通讯，系统将Intent传给调用的组件。
- 调用的组件在处理Intent数据时，没有进行异常捕获，导致在空数据、异常或畸形数据处理时，致应用崩溃。
- 此漏洞会影响安卓系统的所有版本，不仅会导致应用的防护功能被绕过或失效，也可被攻击者攻击导致应用崩溃，造成损失。

构造畸形Intent发送adb命令或嵌入攻击代码 → 通用拒绝服务 → APP崩溃

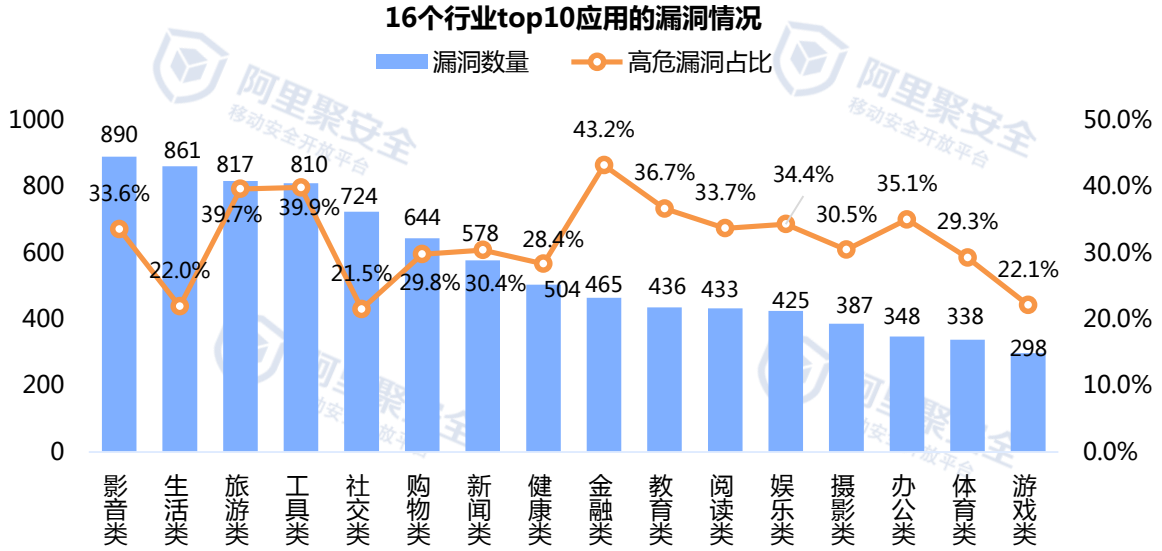
通用拒绝服务漏洞原理

数据来源：阿里聚安全监控数据

2.4 重点行业漏洞分析

16个行业的top10应用**100%**含漏洞，平均漏洞数量**53**个，可看出热门应用的安全漏洞不容乐观。

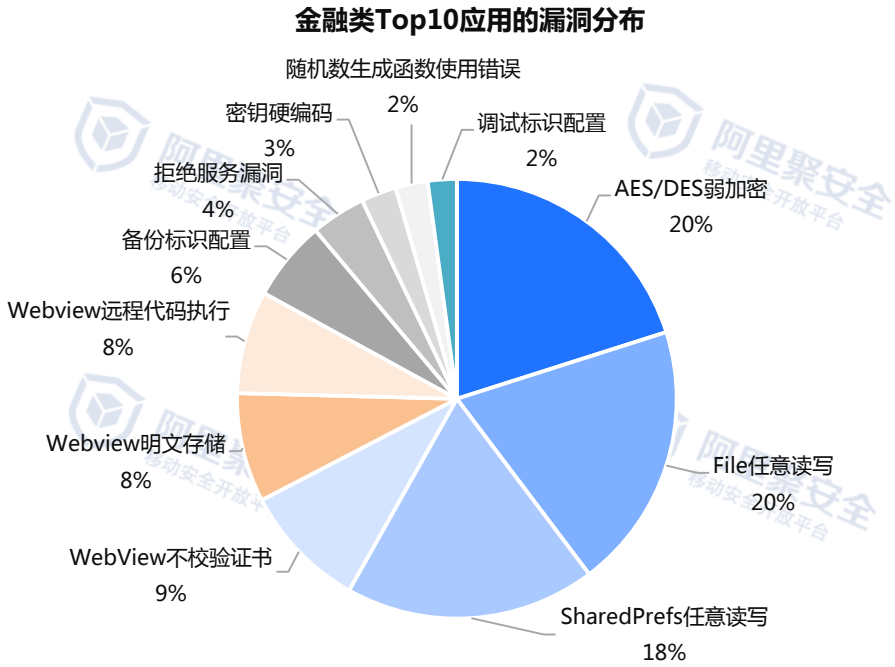
- 16个行业的top10应用共有8515个漏洞，其中**32%**属于高风险漏洞如**Webview远程代码执行**、本地存储密钥等，可导致用户隐私信息泄露。
- 热门行业如影音、生活类等，漏洞数量最大，但**金融类应用**的高风险漏洞占比最高，达**43%**，由于与资金相关，对用户的潜在影响大。



数据来源：阿里聚安全监控数据

2.4 重点行业漏洞分析

- 金融类top10应用有**465个**漏洞，平均每个含**46个**漏洞。其中**20%是AES/DES弱加密风险**，可导致用户应用加密被破解；18%是SharedPrefs任意读写漏洞，可导致用户个人身份信息、密码等敏感信息泄露。

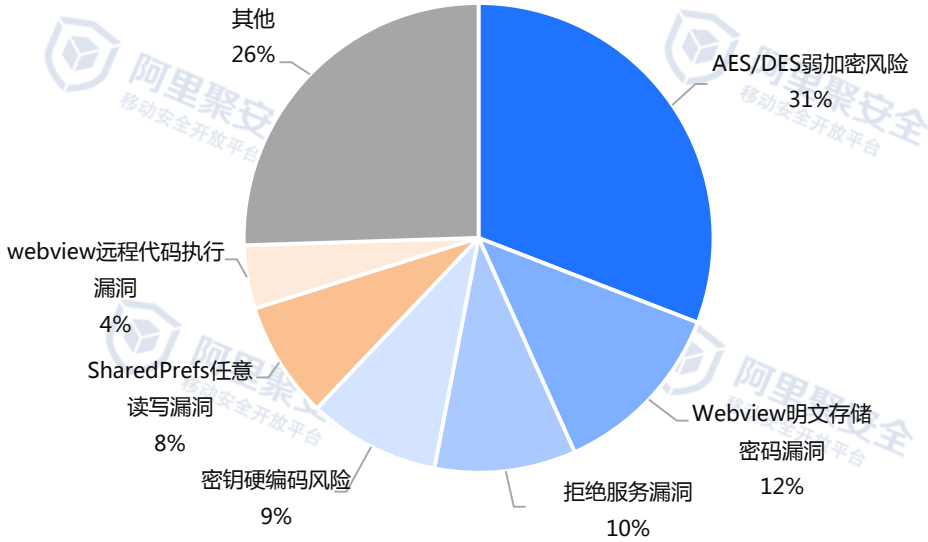


数据来源：阿里聚安全监控数据

2.4 重点行业漏洞分析

- 游戏类top10应用有**298个**漏洞，平均每个应用含**30个**漏洞。其中**31%是AES/DES弱加密风险漏洞**，可导致用户应用加密被破解；12%是webview远程代码执行漏洞，可导致用户手机被远程控制、隐私泄露等风险。

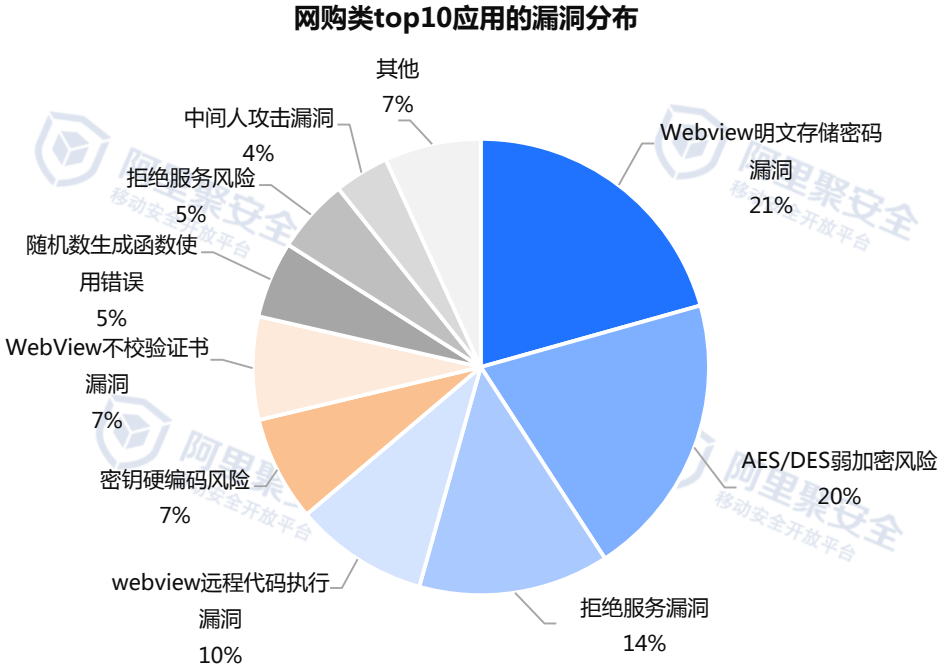
游戏类Top10应用的漏洞分布



数据来源：阿里聚安全监控数据

2.4 重点行业漏洞分析

- 网购类top10应用有**644个**漏洞，平均每个含**64个**漏洞。其中**21%是Webview明文存储漏洞**，可导致用户账号密码泄露；20%是AES/DES弱加密风险漏洞，可导致应用加密被破解。

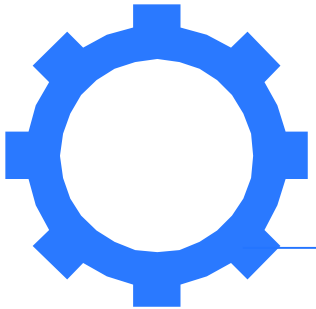


数据来源：阿里聚安全监控数据

3. 仿冒情况

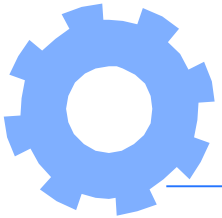
规模

16个行业top10应用中，86.3%的应用存在仿冒，总仿冒应用量高达7866个，相比上一季度增长24.3%。



风险

仿冒病毒应用以流氓行为、恶意扣费为主，对用户造成骚扰，且用户资费莫名被扣。



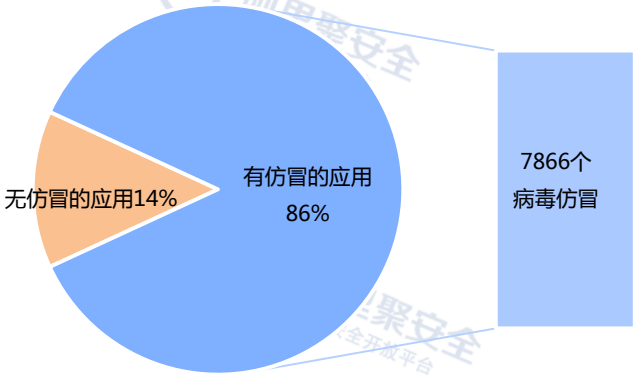
行业

16个行业top10应用中，社交、游戏、影音、购物、金融类APP的仿冒量最为惊人，几乎100%被仿冒，其他行业的仿冒情况也不容乐观。

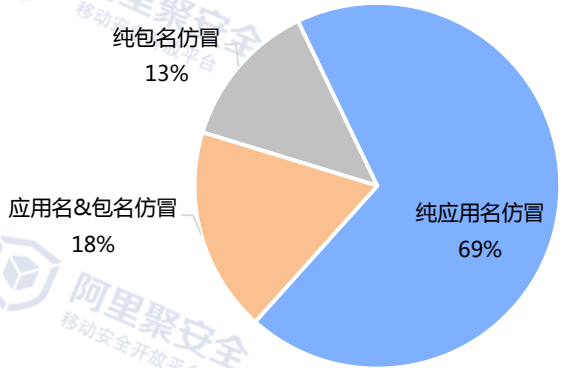
3.1 仿冒规模

- 选取16个行业的安卓top10共160个应用，进行仿冒检测，结果显示**86%**的应用存在仿冒，总仿冒量高达**7866个**，平均每个应用的**仿冒量高达49**个，相比上一季度增长**22%**。
- 各类仿冒应用中，单纯仿冒正版软件应用名称的仿冒应用量**5415个**，占比69%；单纯仿冒包名的仿冒应用量**1043个**，占比13%；两者都仿冒的量为**1423个**，占比18%。可见应用名称的仿冒最受盗用者喜欢，且此类仿冒应用最容易误导用户下载进而获利。

16个行业top10应用的仿冒情况



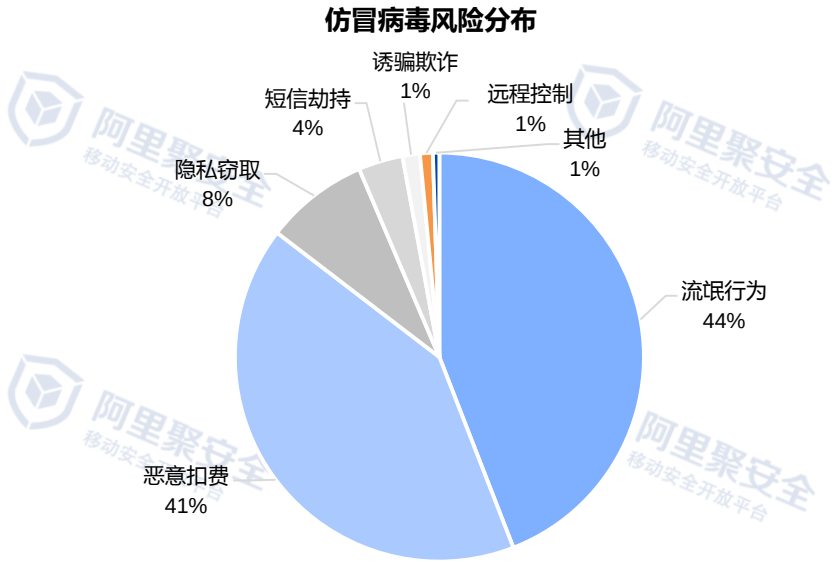
仿冒应用类别分布



数据来源：阿里聚安全监控数据

3.2 仿冒风险

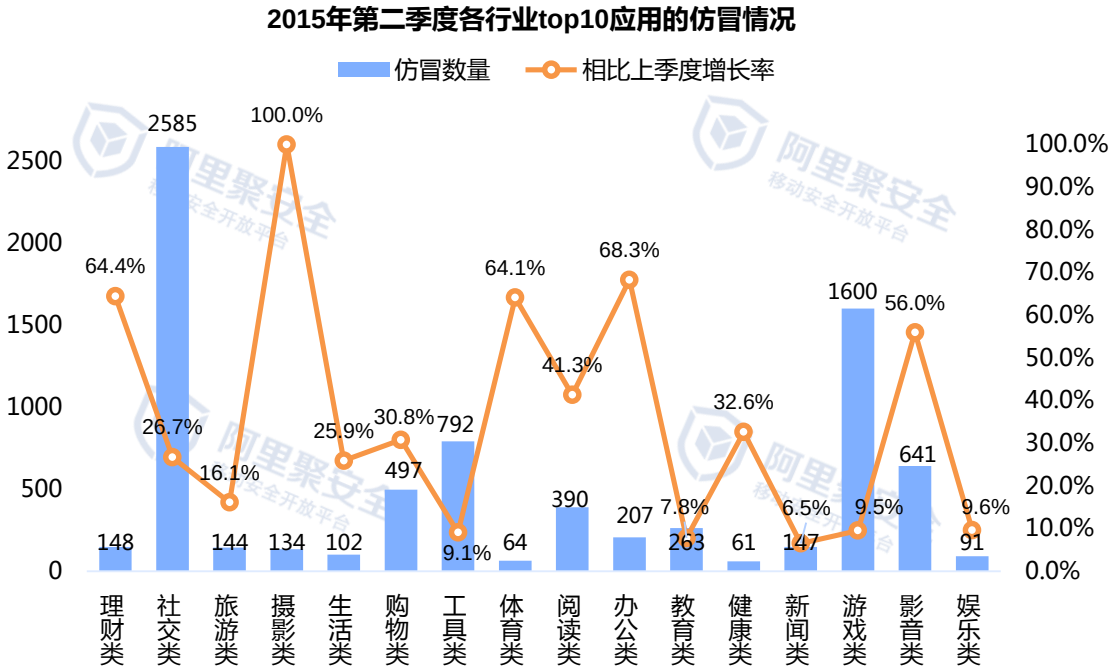
- 16个行业top10应用被检测出来的7866个仿冒软件中，**流氓行为**类软件占比高达**44%**，相比上一季度增长38%；其次是恶意扣费类仿冒软件，占比为41%，相比上一季度上涨34%。



数据来源：阿里聚安全监控数据

3.3 行业仿冒情况

- 分析16个行业各top10应用的仿冒情况，可以看出**社交、游戏、工具**类应用是仿冒的重灾区，且仿冒量比上一季度有增无减。
- 在16个行业top10应用中，每个行业的仿冒量相比上一季度均有增长，对正版应用开发者和用户都会造成影响。

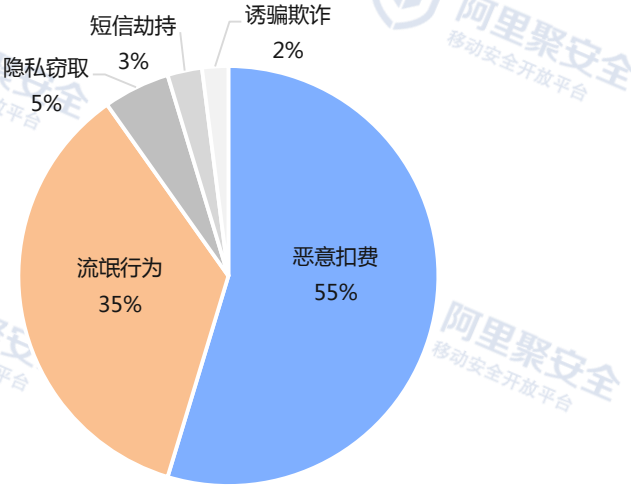


数据来源：阿里聚安全监控数据

3.4 重点行业仿冒分析

- Top10游戏类应用中，**100%**的应用含病毒仿冒软件，**仿冒总量1600个**，平均每个应用有160个病毒仿冒，仿冒总量比上一季度上涨**10%**。
- 1600个病毒仿冒应用中，**55%**的病毒应用具有**恶意扣费**行为，容易造成用户游戏账号中的资金损失。游戏行业以其数量多、收益快的特性，易受不良开发者仿冒，影响正版开发者和用户的权益，其仿冒问题的严重性不容忽视。

Top10游戏类应用的病毒仿冒风险

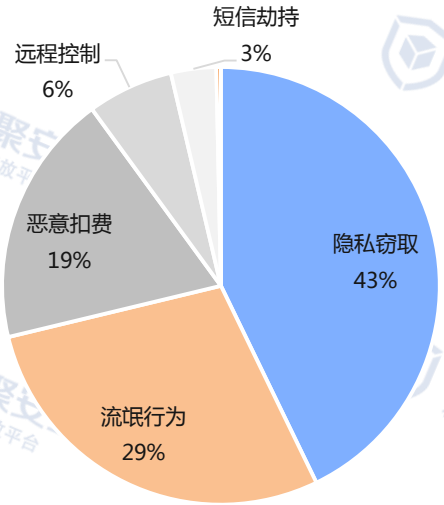


数据来源：阿里聚安全监控数据

3.4 重点行业仿冒分析

- Top10购物类应用中，**100%**的应用含病毒仿冒软件，**仿冒总量497个**，平均每个应用有50个病毒仿冒，仿冒总量比上一季度上涨**31%**。
- 497个仿冒应用中，**43%**的仿冒应用有**隐私窃取**行为，容易造成用户敏感信息泄露，进而导致资金受损。

Top10购物类应用的病毒仿冒风险

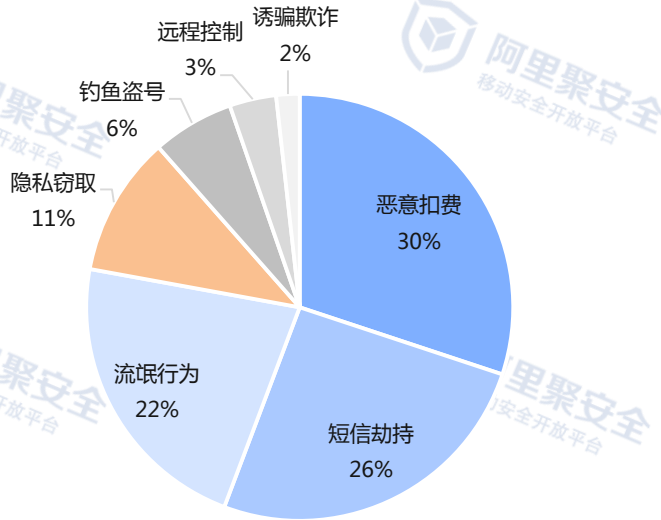


数据来源：阿里聚安全监控数据

3.4 重点行业仿冒分析

- Top10金融类应用中，**100%**的应用含病毒仿冒软件，**仿冒总量148个**，平均每个应用有15个病毒仿冒，仿冒总量相比上一季度上涨了**64%**。
- 金融类应用的仿冒应用量虽不多，但**增长率高达64%**，且过半的病毒仿冒具有恶意扣费和短信劫持行为，可对用户造成巨大损失。

金融类应用仿冒情况



数据来源：阿里聚安全监控数据

安全建议

阿里聚安全
移动安全开放平台

◆ 阿里聚安全

阿里聚安全是以移动应用安全为核心的一站式解决方案开放平台，保障应用健康。

- 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

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

阿里聚安全公众号：阿里聚安全

阿里钱盾公众号：阿里钱盾