2015年第一季度移动安全报告

阿里聚安全
移动安全开放平台

阿里巴巴移动安全

阿里钱盾
钱有盾 盗无门

病毒

- 2015年第一季度，安卓平台受病毒感染设备呈上升趋势，平均7.6台设备就有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。
- 第一季度，色情类病毒样本量和感染量增长非常显著。

漏洞

- 100%的top160应用存在漏洞风险，每个应用平均含30个漏洞。
- 热门应用漏洞以Webview明文存储为主，占比达26%，容易造成用户密码泄露风险。
- 金融、购物、工具、影音等行业的top10应用漏洞数量最多，漏洞量均超过335个。

仿冒

- 79.4%的top160应用存在仿冒，每个应用平均含40个仿冒。
- 仿冒病毒应用以流氓行为和恶意扣费为主，会影响用户体验，或费用莫名被扣。
- 16个行业的应用中，社交类应用100%被仿冒，仿冒量最为惊人，游戏，金融，购物等重点行业的仿冒情况也不容乐观。

目录

1 病毒情况

规模

- 2015年第一季度，安卓平台受病毒感染设备呈上升趋势，平均7.6台设备就有1台设备中毒，总中毒设备量高达1466万。
- 2015年第一季度，阿里聚安全病毒库共新增病毒样本量172万，同比增长173%，季度内月均涨幅超过100%。

类型

- 第一季度内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。
- 短信劫持类病毒的防范意识明显增强，感染用户占比明显下降。

区域

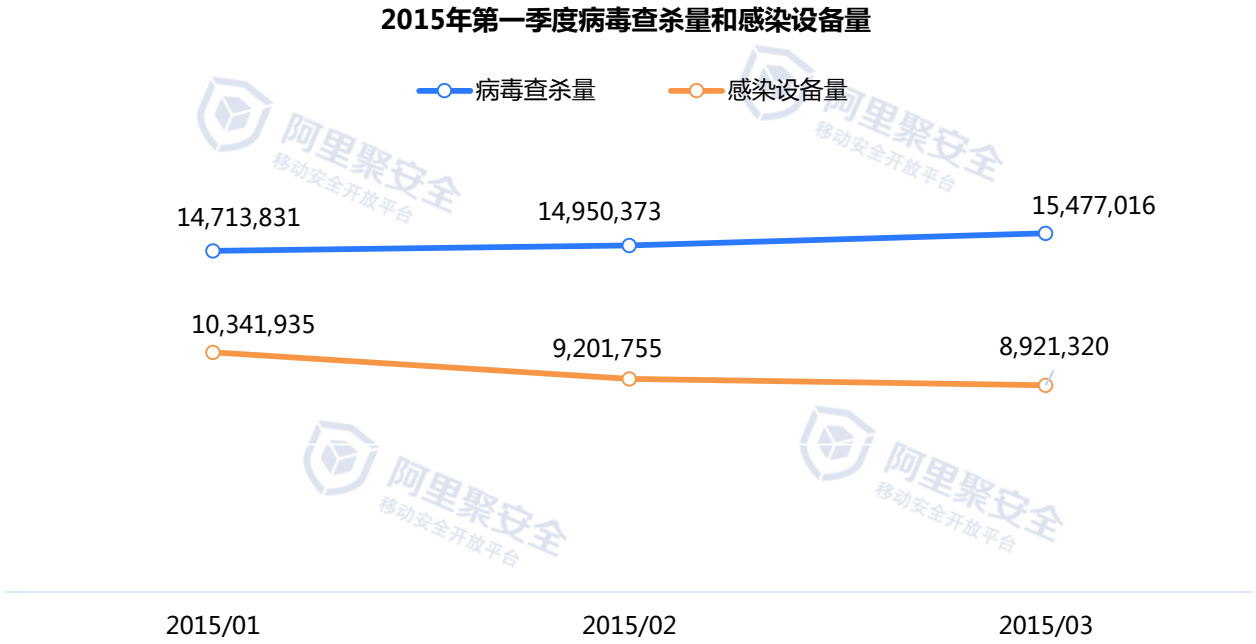
- 第一季度，广东仍旧是受病毒感染最严重的地区，感染量占全国的12.6%，相对去年占比略有上升。贵州是最易被病毒感染的省份，其设备感染率为16%。

色情

- TOP50的热门病毒中，色情类感染用户占比31%，比上一季度的样本量占比上涨了19%，感染用户量上涨了23%

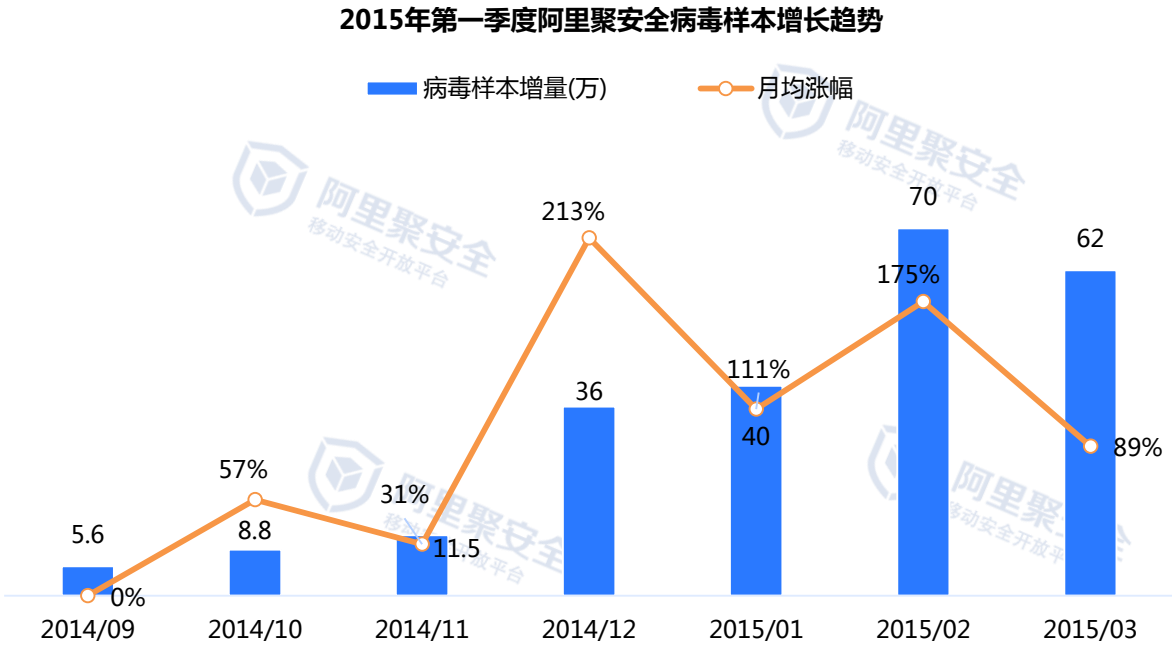
1.1 病毒规模

- 2015年第一季度，安卓设备的病毒感染量高达**2406.6万**，平均**7.6台**安卓设备就有**1台被感染**，风险形势不容乐观。
- 阿里聚安全病毒扫描引擎共查杀病毒**4514万**个。帮助用户抵御了大量的手机病毒风险。



1.1 病毒规模

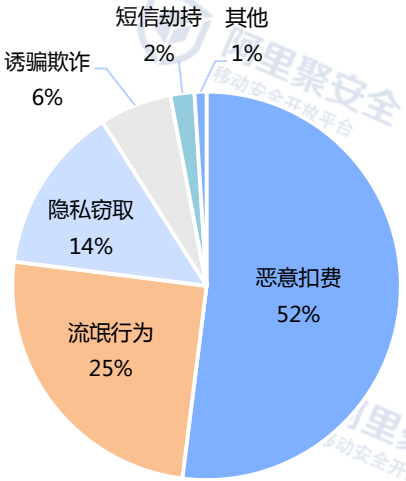
- 阿里聚安全病毒样本库持续增长，2015年第一季度新增**172万**样本量，相对上一季度增加了**173%**，季度内月均增长也高达**125%**，如此快速的增长也反映了移动互联网的安全形势之严峻。



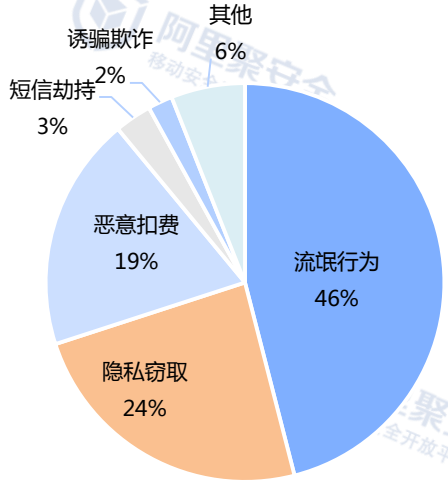
1.2 病毒类型

- **恶意扣费**类病毒样本占比仍旧最高，占比达**52%**，相比上一季度上涨**23%**。由于此类病毒能够直接获益，因此备受黑客青睐，但其感染用户占比下降至23%，略有下降。
- **流氓行为**类病毒感染用户占比最高，**达46%**。
- **隐私窃取**类病毒感染用户占比上升明显，达**24%**，同比**上涨85%**。
- 短信劫持类病毒感染用户占比下降明显，本季度仅占3%，相对上季度**下降81%**，主要原因是此类风险的安全教育已经在各大媒体传播。

样本库各类别病毒样本量分布



各类别病毒感染用户占比



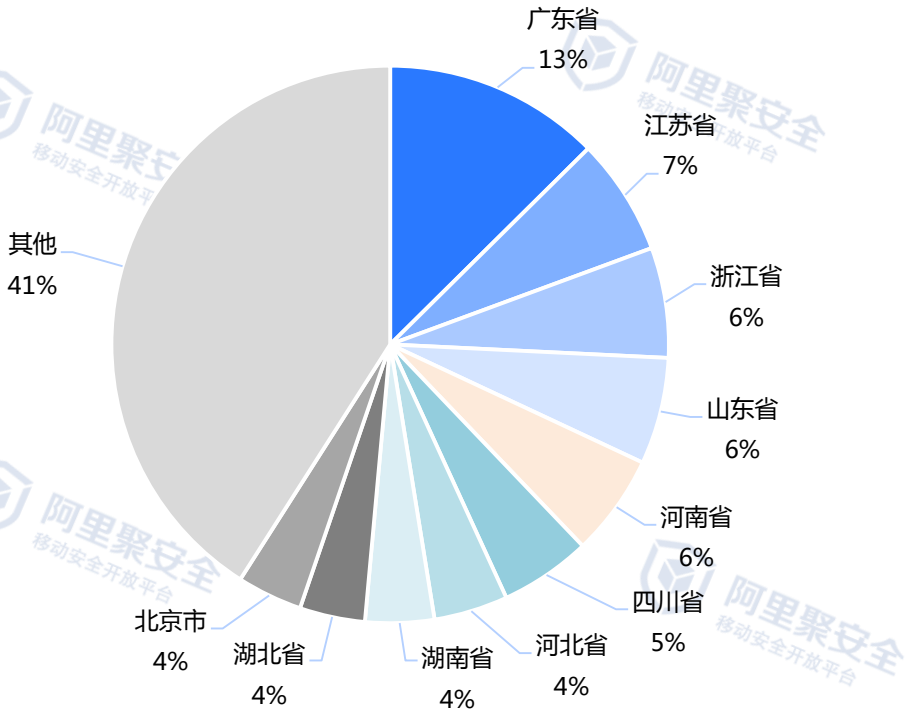
1.2 病毒类型

应用名称	感染量	病毒类型	恶意行为描述
消灭糖果	544,511	流氓行为	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。
成人影音	435,519	恶意扣费	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。
快播无码	123,300	隐私窃取	该病毒启动后未经用户允许私自收集用户隐私信息，可能会给您的手机造成一定的隐私泄漏。
极品影音	103,592	恶意扣费	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。
成人影院	80,885	恶意扣费	该软件含有风险代码，启动后会触发可能引起扣费的功能，可能会对您的手机造成一定的风险，请您谨慎使用。
午夜高清	76,236	恶意扣费	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。
诱辣影院	70,390	恶意扣费	该木马存在扣费陷阱，会读取用户短信窃取用户隐私，会打开流量开关私自下载其它木马应用安装，请谨慎使用。
无码视频	59,225	流氓行为	该病毒具有严重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。
成人快播	59,178	恶意扣费	该软件含有风险代码，启动后会触发可能引起扣费的功能，可能会对您的手机造成一定的风险，请您谨慎使用。
涩爱小姐	50,095	隐私窃取	该病毒启动后未经用户允许私自收集用户隐私信息，可能会给您的手机造成一定的隐私泄漏。
成人影院	49,801	恶意扣费	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。
极致快播	48,682	流氓行为	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。

1.3 感染用户分布

- **广东**是受感染用户量最多的省份，其第一季度的设备感染量占全国总感染量的 **13%**，广东，江苏，浙江成为受感染设备最多的TOP3省份。

各省份设备感染量占比分布



1.3 感染用户分布

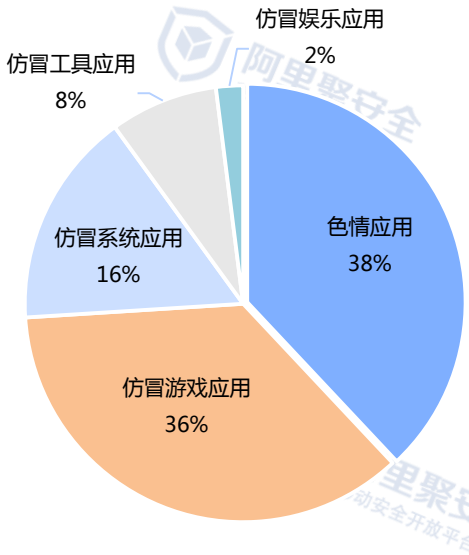
- **贵州**是最易被病毒感染的省份，每6台手机就近1台染毒，比全国平均值高**25%**。染毒设备比例最高的省份多分布在中西部，贵州、西藏、云南是中毒比例最高的三个省份。全国平均中毒设备比例高达**13%**。

病毒的设备感染率top10区域分布

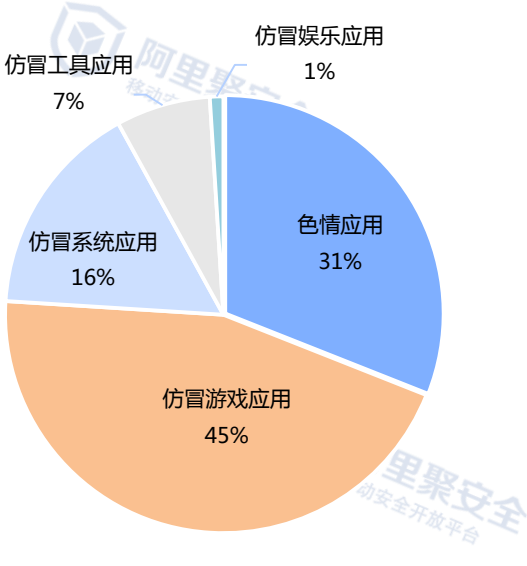
1.4 重点病毒分析

- 分析一季度感染量 TOP50 的病毒，样本量中，色情类病毒应用占比最高，达**38%**，其常常运用诱惑极大的名称如“成人影音”、“快播无码”等来吸引用户下载。
- 在TOP50的热门病毒中，色情类感染用户占比**31%**，比上一季度的样本量占比上涨了**19%**，感染用户量上涨了**23%**。

感染量top50的病毒样本分布



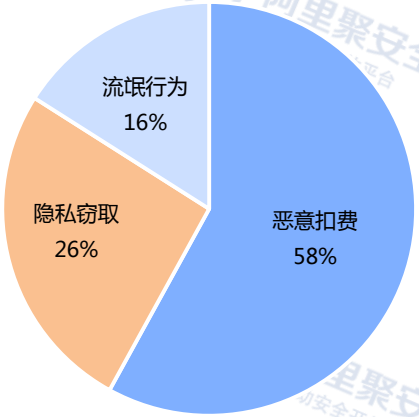
top50病毒感染用户量分布



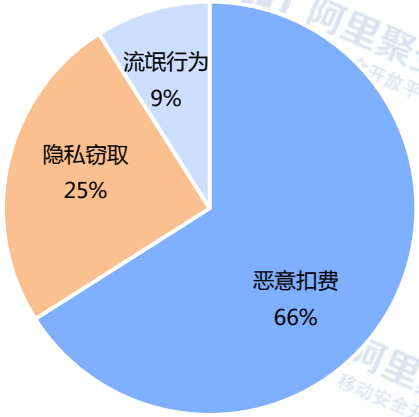
1.4 重点病毒分析

- TOP色情类病毒风险以恶意扣费、隐私窃取、流氓行为为主。
- 恶意扣费是色情类病毒的第一大风险类型，病毒样本量占比高达**58%**，感染的用户量占比更是高达**66%**，这一类风险能够在用户毫不知情的情况下，通过定制SP服务等引起扣费。
- 隐私窃取类的风险也较大，样本量和感染量占比均超过**25%**，此类能未经用户允许直接收集和传输用户隐私信息。

色情类病毒样本的风险分布



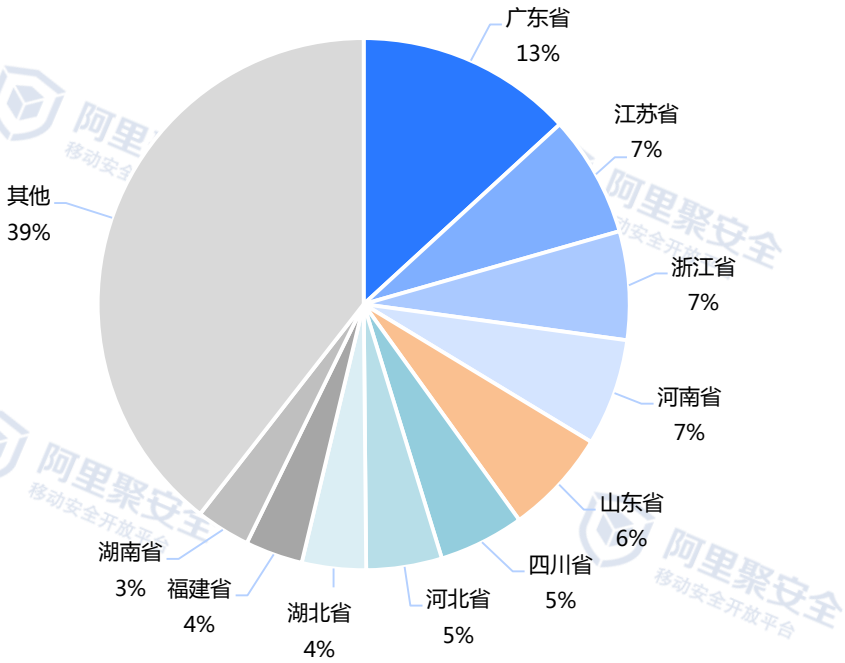
色情类病毒用户感染量占比分布



1.4 重点病毒分析

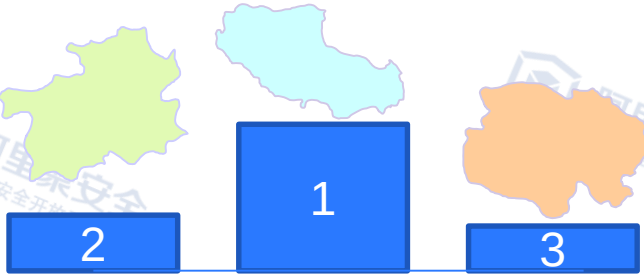
- 分析色情应用的各省份感染量占比可见，结果类似整体病毒感染量分布，广东省依旧是色情病毒感染量占比最高的省份，达到了**13%**，而且广东，江苏，浙江也是色情病毒感染最多的三个省份，合计占比高达**27%**。

色情类病毒用户感染量的省份分布

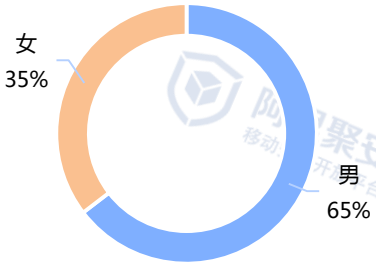


1.4 重点病毒分析

- 根据阿里移动安全的监控，西藏，贵州，青海是色情病毒感染比例最高的省份，他们相对全国平均感染率分别高了50.3%、43.7%、 43.9% 。
- 色情类病毒的中毒人群集中在男性，约占据了整体病毒受害者中的65%。
- 色情病毒感者集中在19-25岁，这部分人群占到了整体中毒者45.5%。



色情类病毒中毒男女比例占比



45.5%

19-25岁

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4,775个漏洞，均值30个。
- 100%的top160应用有漏洞，高风险漏洞占44%。

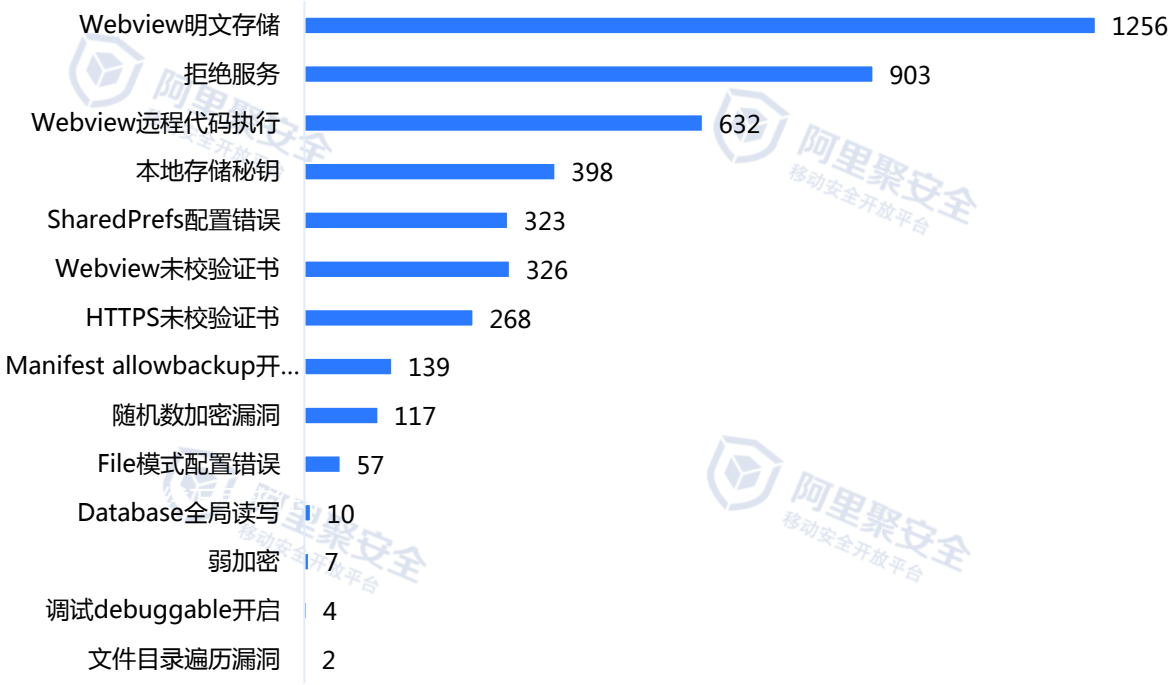
行业漏洞

- 金融、影音、生活行业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。

2.1 应用漏洞

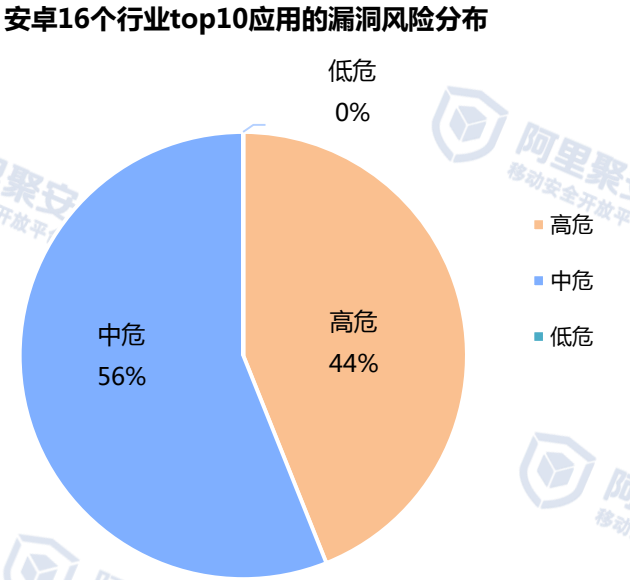
- 安卓各行业top160应用共有**4,775个**漏洞，平均每个应用有**30个**漏洞。
- **100%**的top160应用含有漏洞，且以Webview明文存储漏洞为主。

安卓16个行业top10应用的漏洞类别和数量



2.1 应用漏洞

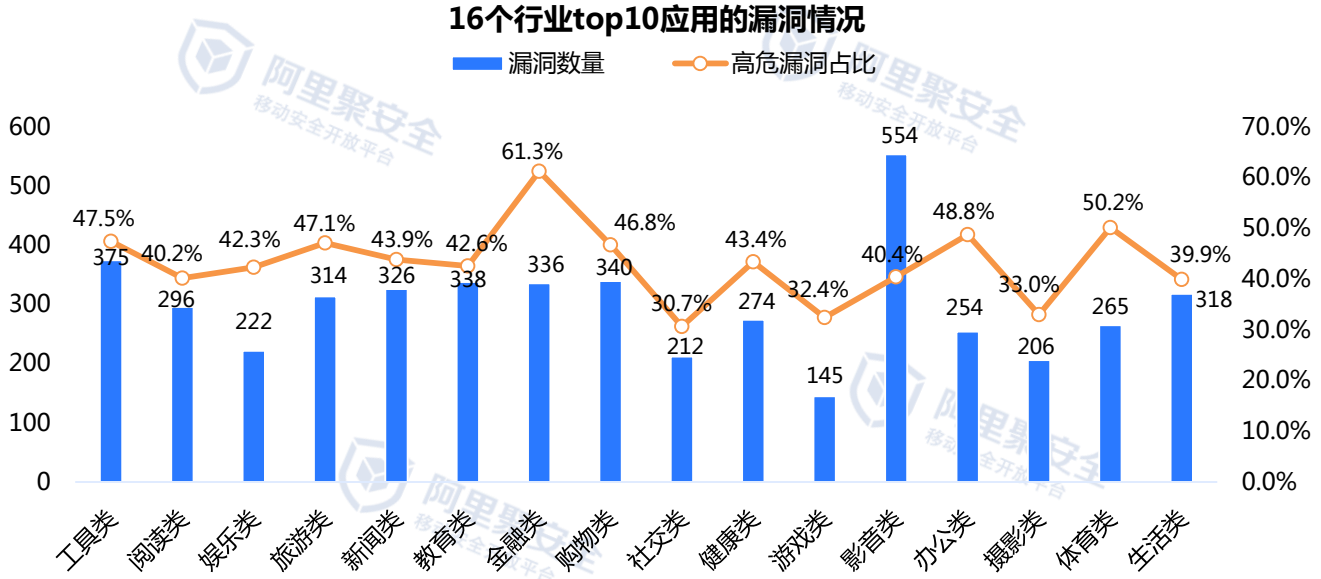
- **4,775个**风险漏洞中，**44%属于高危漏洞**、56%属于中危漏洞，可见移动应用漏洞问题的严峻性。



2.2 重点行业漏洞分析

100%的top160应用含漏洞，**平均漏洞数30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4,775个漏洞，其中43%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。
- 热门行业如金融、影音等，漏洞数量大，高风险漏洞占比亦超40%，对用户的潜在影响大。

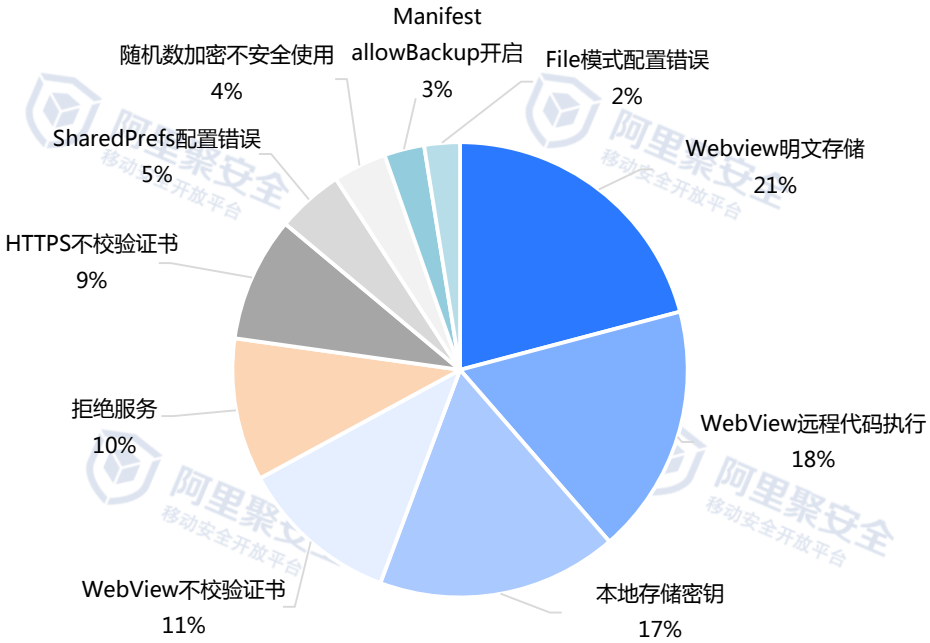


数据来源：阿里聚安全监控数据

2.2 重点行业漏洞分析

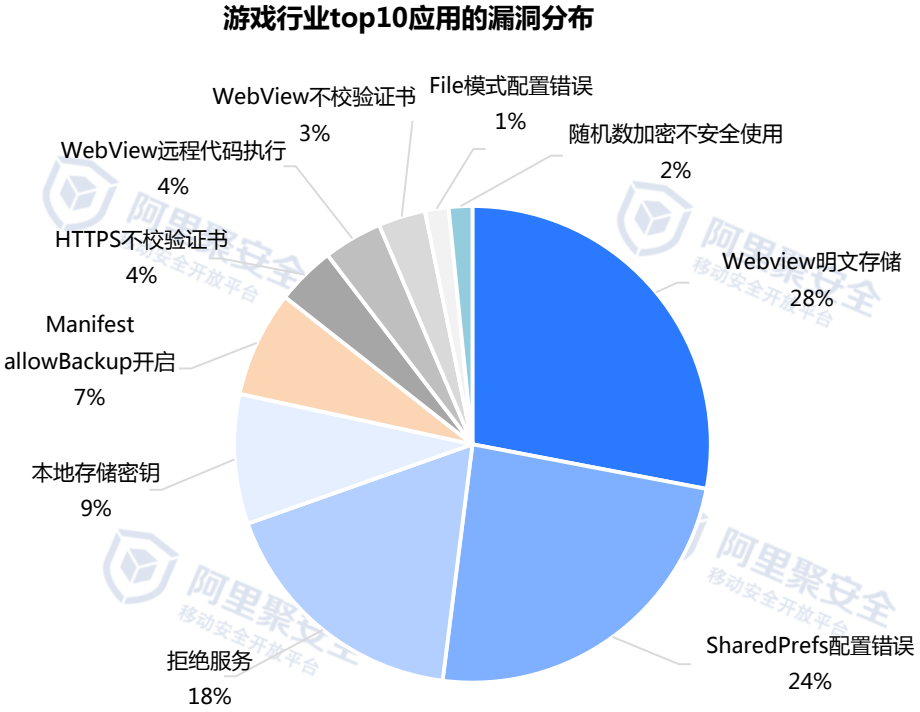
- 金融行业top10应用有**336个**漏洞，平均每个含**34个**漏洞。其中**21%是Webview明文存储**漏洞，可导致用户账号密码泄露；**18%是Webview远程代码执行**漏洞，可导致用户手机被远程控制、隐私泄露等风险。

金融行业top10应用的漏洞分布



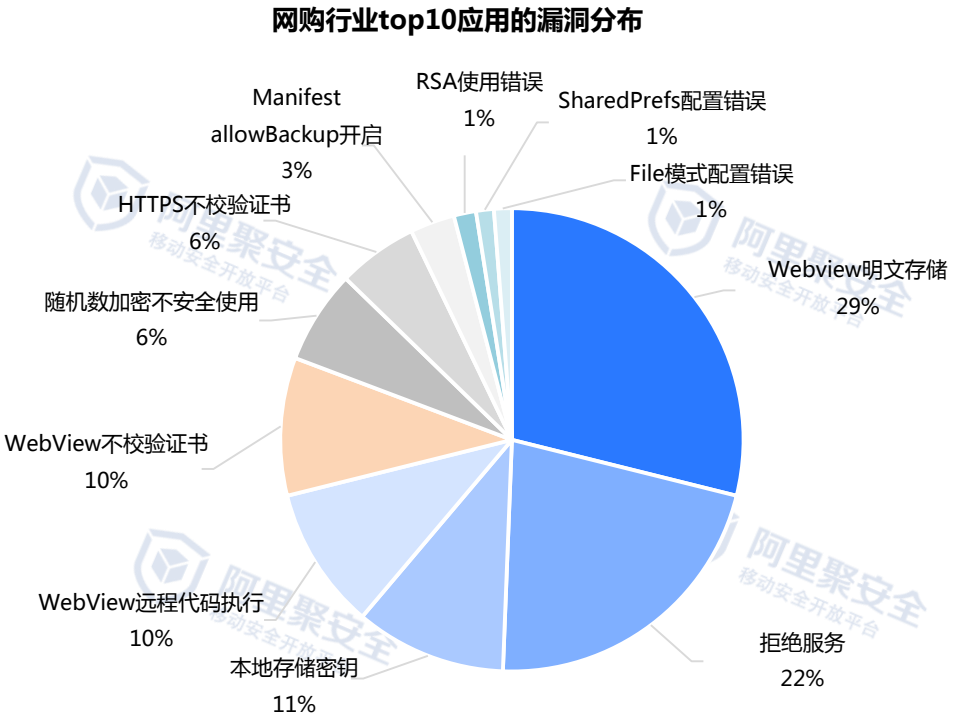
2.2 重点行业漏洞分析

- 游戏行业top10应用有**145个**漏洞，平均每个含**15个**漏洞。其中**28%是Webview明文存储**漏洞，可导致用户账号密码泄露；**24%是SharedPrefs配置错误**漏洞，可导致用户个人身份信息、密码等敏感信息泄露。



2.2 重点行业漏洞分析

- 网购行业top10应用有**340个**漏洞，平均每个含**34个**漏洞。其中**29%是Webview明文存储**漏洞，可导致用户账号密码泄露；**22%是拒绝服务**漏洞，可导致特定恶意数据被写入组件造成应用崩溃，从而拒绝服务，影响应用开发者和用户体验。



3 仿冒情况

规模

- 79.4%的top160应用存在仿冒，总仿冒应用量高达6329个。

风险

- 仿冒病毒应用以流氓行为和恶意扣费为主，会影响用户的应用体验，或话费莫名被扣。

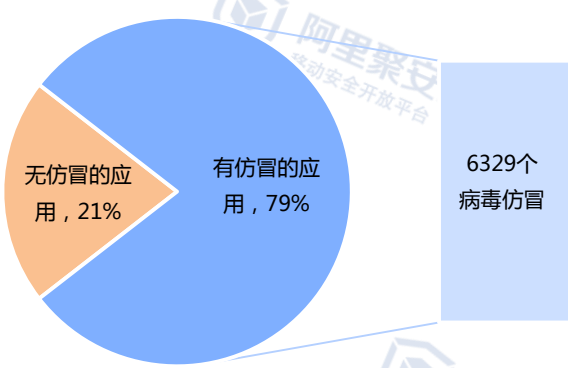
行业

- 16类应用的top160中，社交类应用仿冒数据最为惊人，100%被仿冒，平均被仿冒量高达204个。游戏，金融，购物等重点行业的仿冒情况也不容乐观。

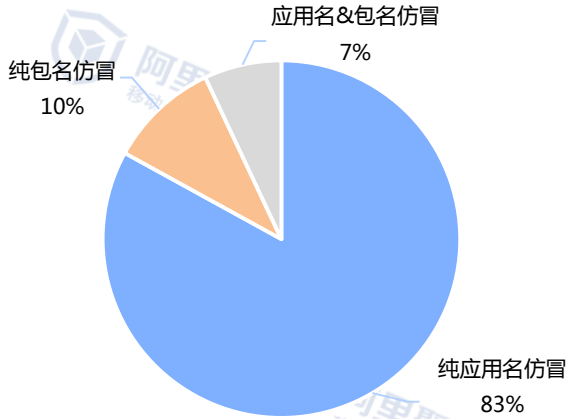
3.1 仿冒规模

- 选取涵盖16类应用行业的安卓top160应用，进行仿冒检测，结果显示**79.4%**的应用存在仿冒，总仿冒量高达**6329个**，平均每个应用的仿冒量高达**40个**。
- 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**5253个**，占比83%；单纯的包名仿冒应用量为**633个**，占比10%；两者都仿冒的量为**443个**，占比7%。可见应用名称的仿冒最受盗用者喜欢，而且此类仿冒应用最容易导致普通用户误下载。

top160应用的仿冒情况

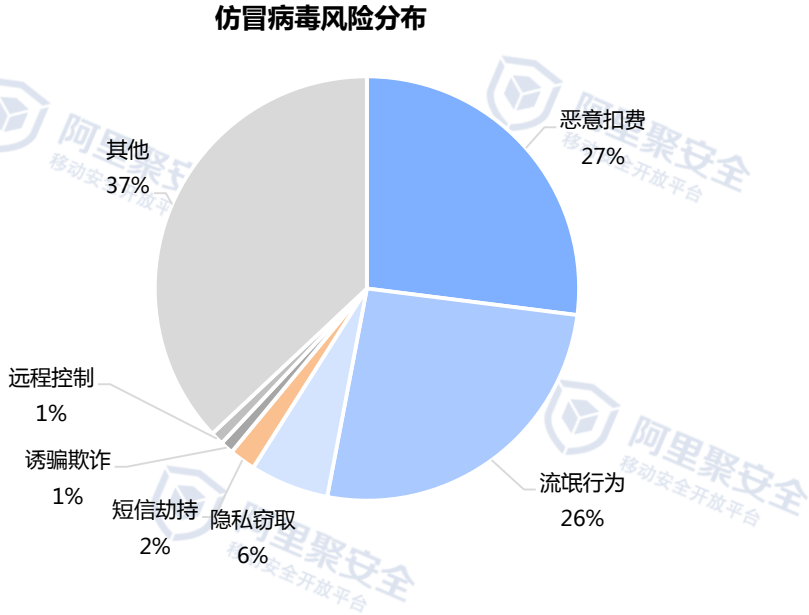


仿冒应用类别分布



3.2 仿冒风险

- Top160应用被检测出来的仿冒病毒软件中，恶意扣费是最常见的风险类型，占比高达**27%**。其次是流氓行为，占比为**26%**。



3.2 仿冒风险

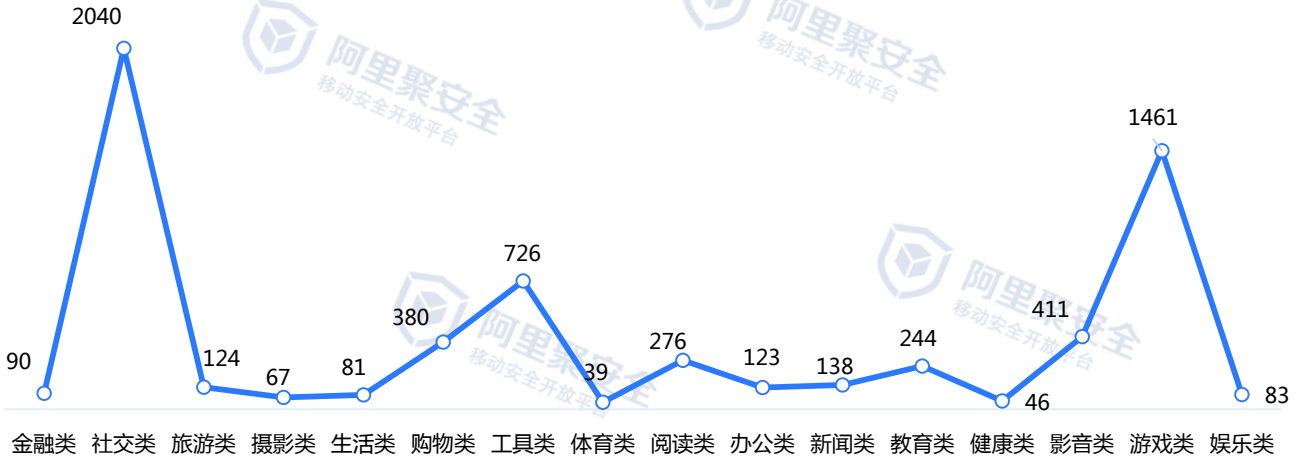
- 以下是仿冒正版软件应用名称的案例列举，包括仿冒软件的病毒类型和危害描述。
- 流氓行为和恶意扣费是仿冒重灾区，且部分仿冒应用的图标和名称与正版应用几乎一模一样，用户难以区别，建议下载【阿里钱盾】等手机安全软件进行仿冒APP查杀。

序号	仿冒应用名称	正版图标	仿冒图标	病毒类型	危害描述
1	暴风影音			恶意扣费	在未经用户允许的情况下私自发送订购收费短信，或通过第三方支付造成扣费。
2	无秘			流氓行为	影响用户体验，随意添加广告书签、广告快捷方式或影响其他软件UI等。
3	追书神器			恶意扣费	在未经用户允许的情况下私自发送订购收费短信，或通过第三方支付造成扣费。
4	百词斩			流氓行为	影响用户体验，随意添加广告书签、广告快捷方式或影响其他软件UI等。
5	PDF阅读器			流氓行为	影响用户体验，随意添加广告书签、广告快捷方式或影响其他软件UI等
6	智行火车票			恶意扣费	在未经用户允许的情况下私自发送订购收费短信，或通过第三方支付造成扣费
7	美图秀秀			恶意扣费	在未经用户允许的情况下私自发送订购收费短信，或通过第三方支付造成扣费

3.3 整体行业仿冒分析

- 分析16个行业各top10应用的仿冒情况，可以发现社交和游戏2个行业是仿冒应用的重灾区，其中社交类应用中的top10应用**100%被仿冒**，仿冒应用共计**2040个**，位居所有类别榜首。

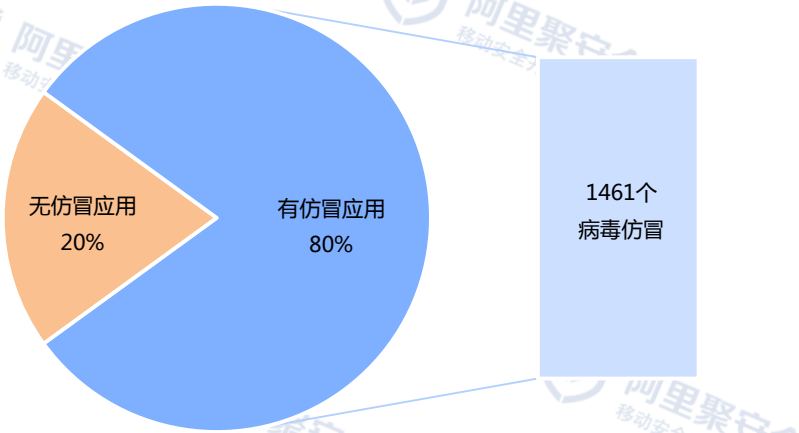
各行业top10应用的仿冒情况



3.3 整体行业仿冒分析

- Top10游戏类应用中**80%**的应用含病毒仿冒软件，仿冒总量**1464个**，平均每个应用有**183个**病毒仿冒，仿冒总量相比上一季度上涨了**82%**，游戏行业以其数量多、收益快的特性，易受不良开发者仿冒伪造，影响正版开发者和用户的权益受损，其仿冒问题之严重不容忽视。

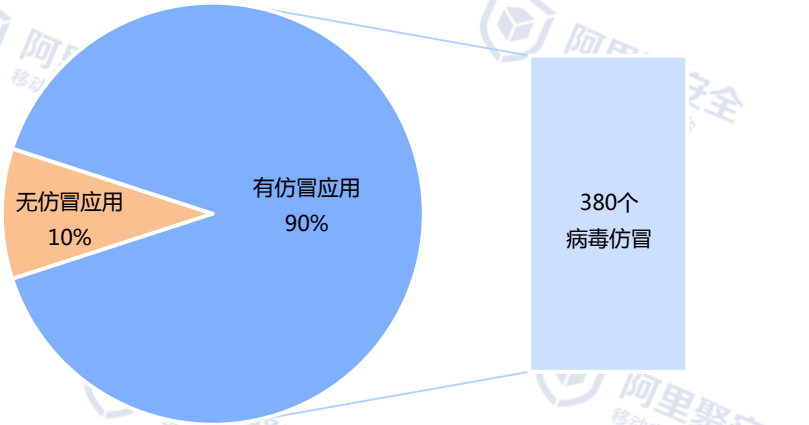
游戏行业top10应用的仿冒情况



3.3 整体行业仿冒分析

- Top10购物类应用中，**90%**的应用含病毒仿冒软件，总量**380个**，平均每个应用有**42个**病毒仿冒。网购应用仿冒比例如此之高，虽其平均仿冒量虽少于游戏行业，但因网购会涉及用户资金，仿冒软件容易导致用户财产受损。

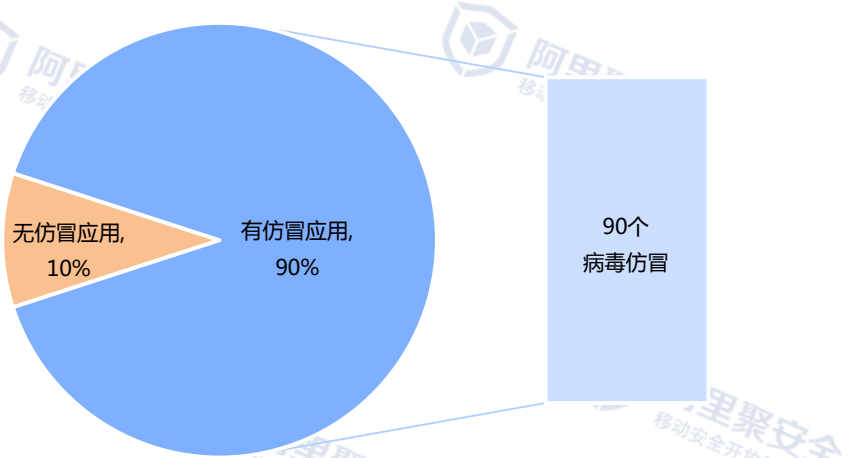
网购行业TOP10应用的仿冒情况



3.3 整体行业仿冒分析

- Top10金融类应用中，**90%**的应用含病毒仿冒软件，总量**90个**，平均每个应用有**10个**病毒仿冒。虽理财行业仿冒量相对较少，但仿冒比例依旧较高，而且其直接与资金挂钩，最容易导致较大资金资损，故其仿冒应用问题亦不容忽视。

金融行业TOP10应用的仿冒情况



安全建议

◆ 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
- 安全增强：安全组件SDK、应用加固
- 持续监控：风险数据可视化并持续监控

◆ 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