2016 中国互联网仿冒态势分析报告

阿里巴巴安全部
中国信通院

联合出品

CAICT 中国信通院

阿里聚安全
阿里安全开放平台

摘要

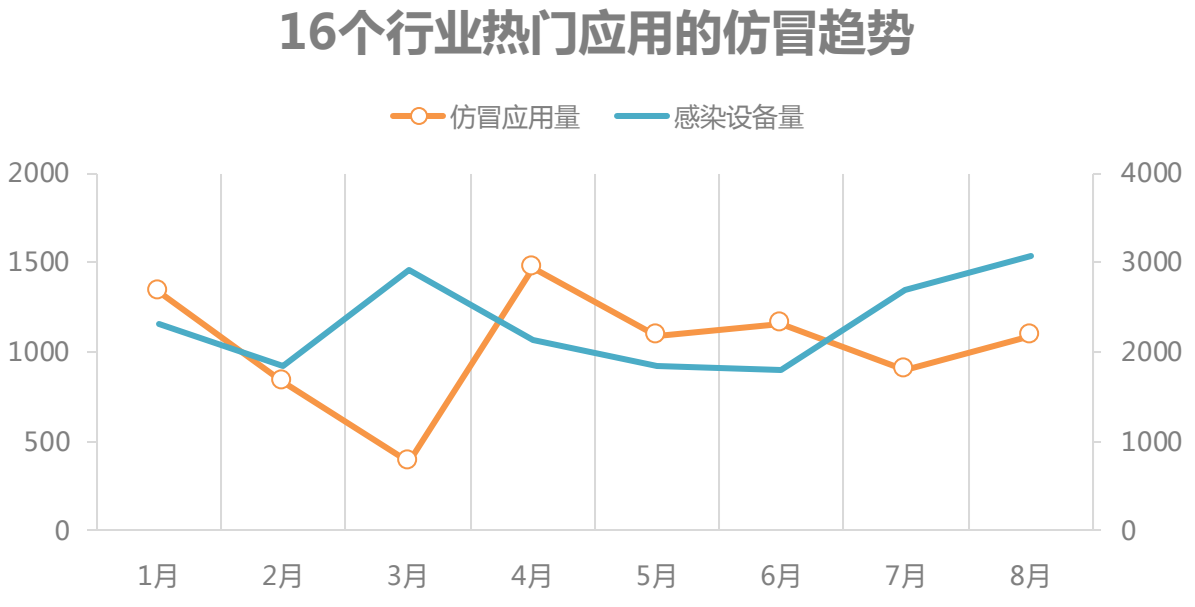
- 基于阿里聚安全在**2016年1-8月**收录的APK样本数据，从**16个行业分类**分别选取了**15个热门应用**，共**240个**应用进行仿冒分析，发现**83%**的热门应用存在仿冒，总仿冒量高达**8267个**，平均每个应用的仿冒量达**34个**，总感染设备量达**6790万台**。
- **广东省**的仿冒应用感染设备量最大，占全国的**13%**。**北京市**作为首都，仿冒应用感染量也非常大，占全国的**7%**。
- 16个行业分类中，**社交类**应用的仿冒量达**4096个**，占总仿冒量的**49.5%**，排名第一。**电信类**应用的仿冒量占**14.2%**，排名第二。
- **57%**的仿冒应用具有**流氓行为**、**恶意扣费**、**短信劫持**或**隐私窃取**等恶意行为，其中短信劫持的风险最高。
- 金融行业中，**银行类**仿冒应用占**58%**，仿冒应用以成为除仿冒网站（钓鱼链接）以外的另一大线上欺诈威胁，**伪基站**是传播银行仿冒网站与应用最重要的工具。
- 电信行业的仿冒应用绝大多数具有恶意行为，其中**短信劫持**行为占比高达**72%**。3大运营商之中，**中国移动**手机营业厅的仿冒量最大，占**84%**，其中大量通过**伪基站**传播。

仿冒应用已成为电信线上诈骗的新型手段

- **真假难辨**
  通过名称、图标等维度的伪造，或者使用重打包等手段，使得用户难以发现仿冒应用，再配合伪基站短信等传播手段，识别难度很高。
- **存活时间长**
  相对于仿冒网站，仿冒应用一旦安装以后，长期存活在用户的设备中，再利用系统漏洞提权等手法长期运行在设备后台。
- **危害程度大**
  仿冒应用不仅可以通过仿冒界面诱骗用户信息，还可以劫持短信，突破短信验证的防护；后台定制服务，恶意扣费；推广垃圾应用；甚至后台远程控制手机等设备。

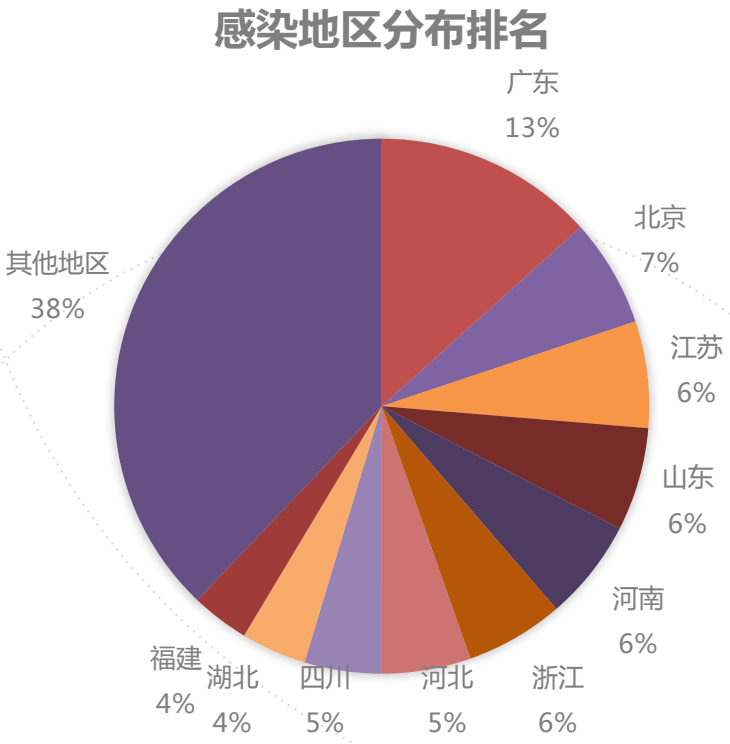
仿冒应用整体趋势

- 240个热门应用中，83%存在仿冒，总仿冒量高达8267个，平均每个应用的仿冒量达34个，感染设备量达6790万台。
- 2、3月份的仿冒应用量大幅下降，符合黑灰产在春节假期前后的活动规律。



仿冒应用地区分布

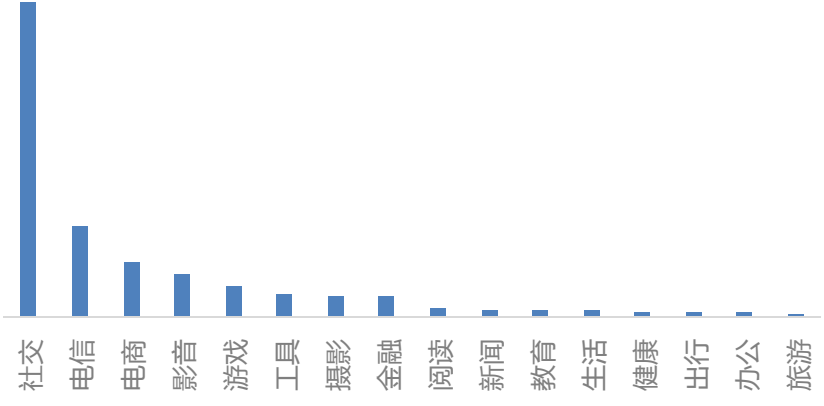
- 2016年，广东省的仿冒应用感染设备量最大，占全国的13%；北京、江苏分别是第二、三位。
- 从数据上看，仿冒应用的感染量与各地区的经济发达程度和人口密度有关，说明仿冒应用具有普遍性。



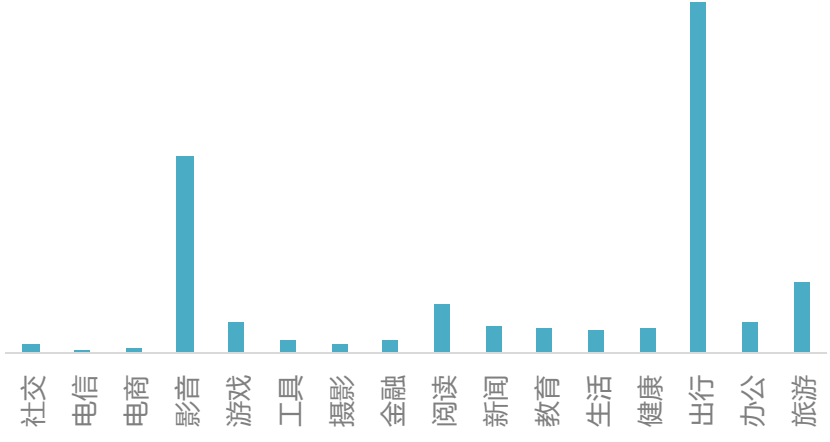
仿冒应用行业分布

- 各行业分类中，社交类应用的仿冒量达4096个，占总仿冒量的49.5%，排名第一。电信类应用的仿冒量排名第二，占总仿冒量的14.2%。电商、影音、游戏、工具、摄影和金融等6个行业分类，也是仿冒的重灾区。
- 出行和影音的仿冒应用平均感染量较大，说明这两个行业的仿冒应用传播性更强。

仿冒应用行业分布



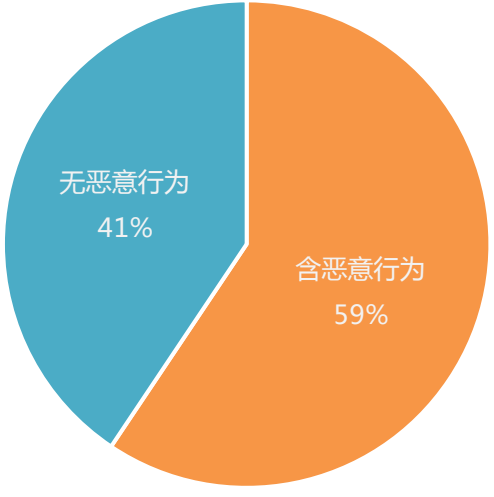
各行业仿冒应用平均感染量



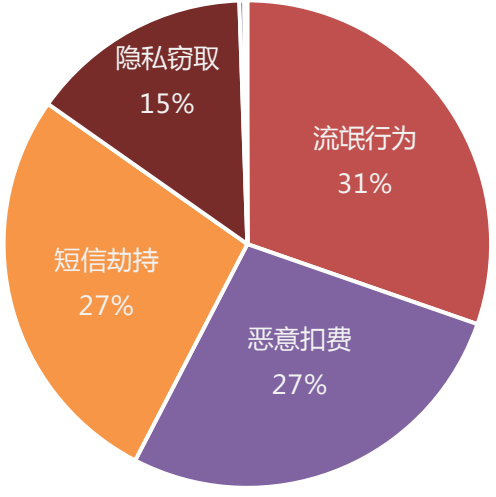
仿冒应用的恶意行为

- 在发现的仿冒应用样本中，59%具有恶意行为，对手机用户的账号、资金和隐私安全存在较大的威胁。
- 病毒仿冒应用主要具有流氓行为、恶意扣费、短信劫持或隐私窃取等恶意行为，其中短信劫持的风险最高。

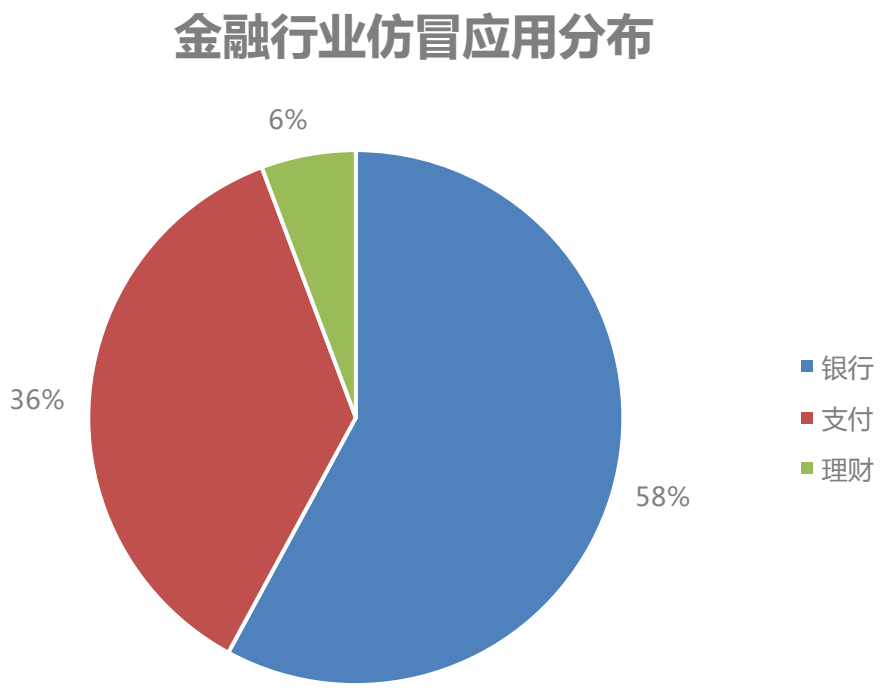
病毒仿冒应用量占比



病毒仿冒应用量风险分布



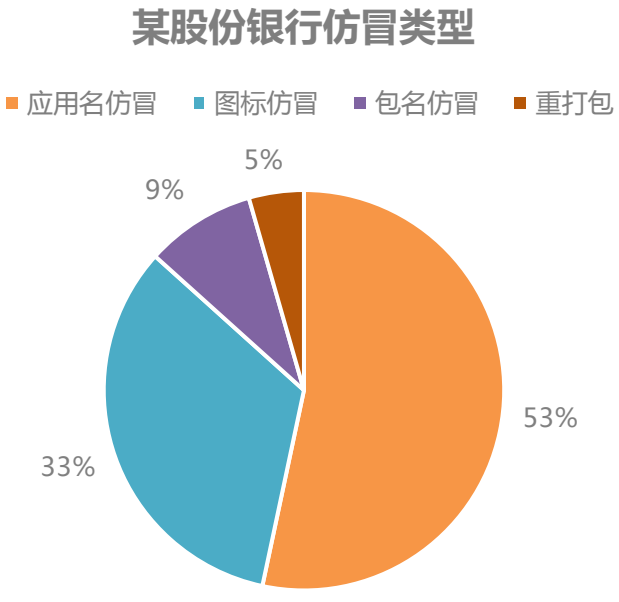
金融行业分析



- 金融行业选取银行、支付和理财3个子分类，分别选取10个热门应用进行分析，共发现仿冒应用301个。
- 银行类仿冒应用占58%，支付类仿冒应用占36%，理财类仿冒应用占6%。
- 金融类仿冒配合短信劫持，可以轻易绕过常见的短信验证机制。

金融行业分析 - 案例

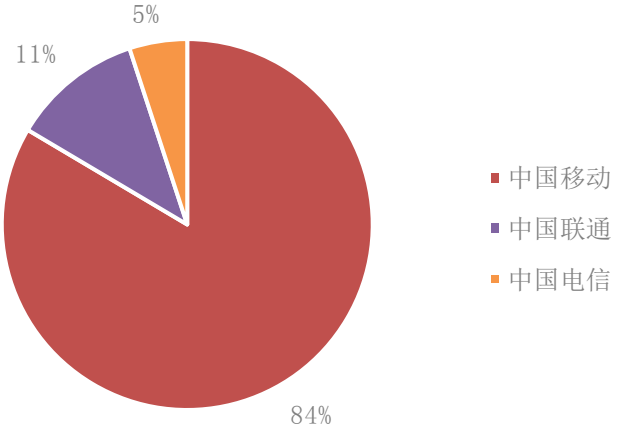
- 在本次分析中，某股份银行共发现24个仿冒应用，全部具有短信劫持行为，感染设备量为5182台，感染用户主要分布在河南、山东和江苏等省份。
- 该案例中的主要分发渠道是应用市场，网盘与伪基站短信。
- 该案例中仿冒网站（钓鱼链接）的发现量比仿冒应用更多，达到10倍以上。



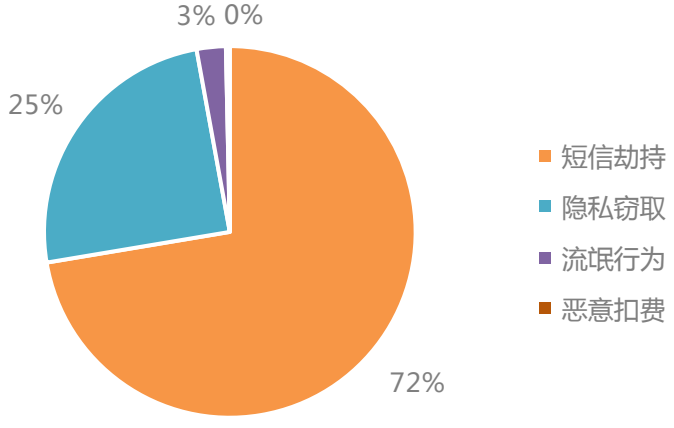
电信行业分析

- 3大运营商中，中国移动手机营业厅的仿冒量最大，占84%。这些仿冒应用主要通过伪基站传播，群发钓鱼短信。
- 电信行业的仿冒应用，绝大多数具有恶意行为，其中短信劫持行为占比高达72%，能够私自拦截和读取用户短信，截获银行交易验证码，对用户的资金安全威胁很大，需要特别注意。

电信行业仿冒应用分布



电信行业仿冒应用的恶意行为



伪基站传播分析 - 诈骗案例

- 积分兑换现金是常见的伪基站诈骗手法，其诈骗过程利用了伪基站、钓鱼短信、钓鱼网站、仿冒应用、网银、快捷支付等工具。

Step 1

伪基站群发钓鱼短信，利用人性弱点诱导用户打开短信中的钓鱼链接

Step 2

钓鱼网站仿冒掌上营业厅，利用积分兑换现金欺骗用户输入银行账户信息，诱导用户下载手机营业厅仿冒应用

Step 3

手机营业厅仿冒应用实际上是一个病毒，安装后申请设备管理器权限并隐藏应用图标，难以删除，拦截交易验证码短信并转发

Step 4

用盗取的银行账户信息，在网银或第三方支付平台完成资金盗取，病毒仿冒应用拦截转发验证码短信功不可没

伪基站传播分析

- 伪基站能够伪装成电信运营商的服务号，向手机用户群发钓鱼短信，收到的钓鱼短信跟正常短信显示在一起，真假难辨。
- 钓鱼网站的仿真度很高，并抓住了人们贪小便宜的弱点，先收集用户信息，再引导安装仿冒应用。

构建安全闭环打击各类欺诈风险

阿里聚安全

阿里安全开放平台

谢谢

Thank you