

2016 钱盾安全报告（8月版）

公安部打击治理电信网络新型违法犯罪防控中心 | 出品
阿里巴巴

摘要

近年来电信诈骗案件频发，从2011年至2015年，全国电信诈骗案件数量从10万件飙升至约60万件。而在今年，电信诈骗的数量依然在上升，政府部门在各种公开场合强调必须依法严厉打击，减少其对人民群众财产安全和合法权益的损害。

电话、短信、钓鱼网址依然是电信诈骗最重要的三种方式。近85%的资金损失是通过钓鱼网址泄露支付信息造成的，而伪基站短信让钓鱼网址可信度变得更高，今年年初开始，公安部加大了伪基站的打击力度，伪基站短信诈骗案件有了显著的减少。

本年度手机病毒木马查杀量呈现上涨趋势，随着手机支付的普及，犯罪分子正在从PC转向手机设备。但近年来用户的安全意识有所提高，而且手机安全软件已经普及，手机病毒造成的资金损失案件相比去年反倒下降。钱盾数据显示，此类案件的高峰一般发生在过年前后，犯罪分子一般通过节日红包、礼包等对用户的引诱来达到目的。

近年来，阿里巴巴集团协助各地公安部门，致力于保障全国消费者的账户安全、交易安全和资金安全，钱盾APP作为公安部打击治理电信网络新型违法犯罪防控中心-阿里巴巴首推的手机安全应用。

目录

1

电信诈骗现状
及趋势

2

手机病毒木马
危害及趋势

PART 1

电信诈骗现状及趋势

黑产对个人信息的低价获取，运营商电话号码获取、群发短信的低门槛，以及伪基站的泛滥让电信诈骗有愈演愈烈之势

电信诈骗案件量一路飙升

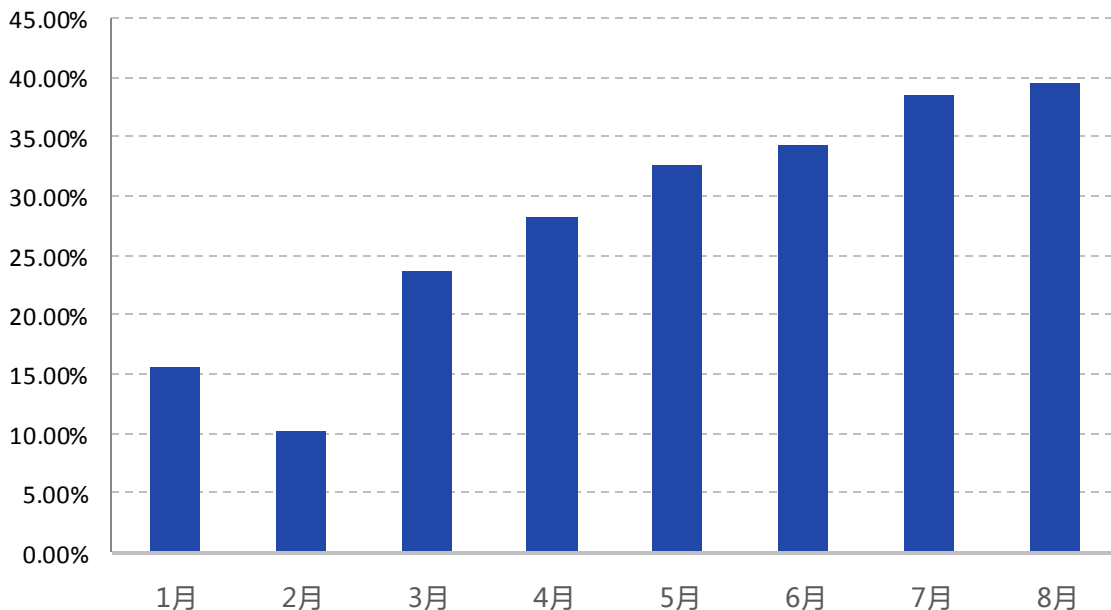
- 电信诈骗近年愈演愈烈，从2011年至2015年，全国电信诈骗案件数量从10万件飙升至约60万件。而在今年，电信诈骗的数量依然在上升
- 今年8月31日，**中共中央政治局委员、中央政法委书记孟建柱** 在上海考察反电信网络诈骗工作时**强调电信网络诈骗犯罪严重侵害人民群众财产安全和合法权益，必须依法严厉打击**。要进一步加强公安机关各警种之间以及公安机关与银行、通信等部门的协作配合，建立全国反电信网络诈骗工作平台，严厉打击泄露或非法获取公民个人信息犯罪活动，切断电信网络诈骗犯罪“黑色产业链”。深化重点地区整治，防止形成新的案件高发区和犯罪输出地。加大宣传教育力度，提升广大群众防范能力

诈骗电话呈现上涨趋势

诈骗电话逐月增加，公安部首次使用“全民受骗”概念

- 从2016年钱盾拦截提醒诈骗电话的情况来看，2月份诈骗电话较少，从3月开始诈骗电话逐月增加
- 暑期7-8月达到峰值，每月40%的钱盾用户会接到诈骗电话提醒，人均每月诈骗电话超过4次，攻势猛烈

2016年收到过诈骗电话的用户占比趋势

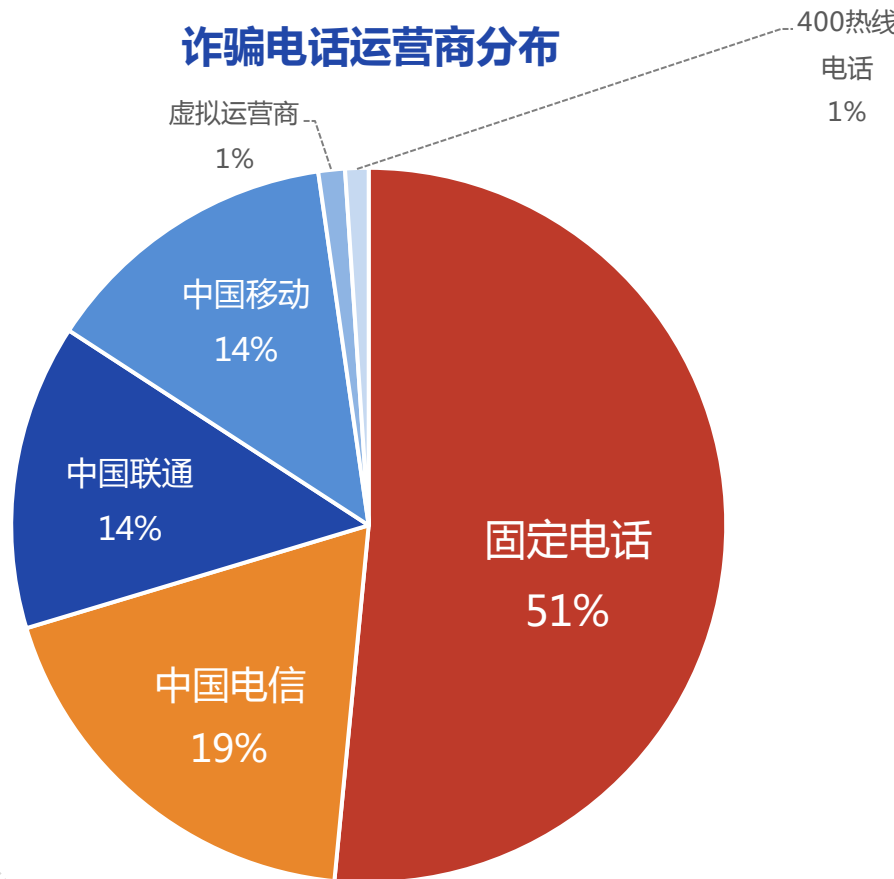


诈骗电话号源归属运营商

诈骗电话号码源固话占51%

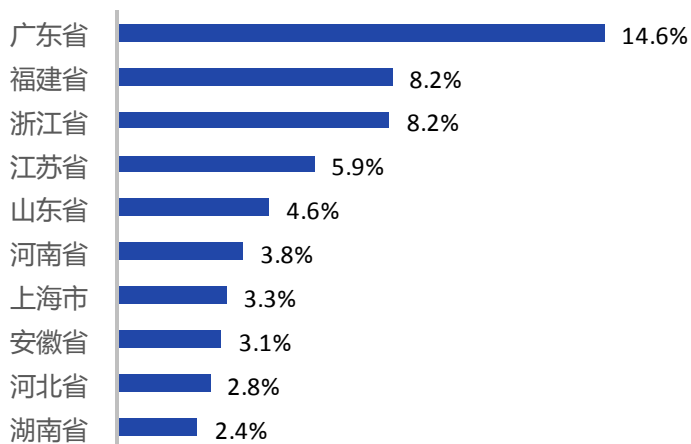
2016年1-8月，诈骗电话号源分布中，**固定电话**拨出诈骗电话最多，占比**51%**；其次为三大运营商手机拨出的电话，占比47%；虚拟运营商和400热线拨出的诈骗电话各占1%

诈骗电话运营商分布

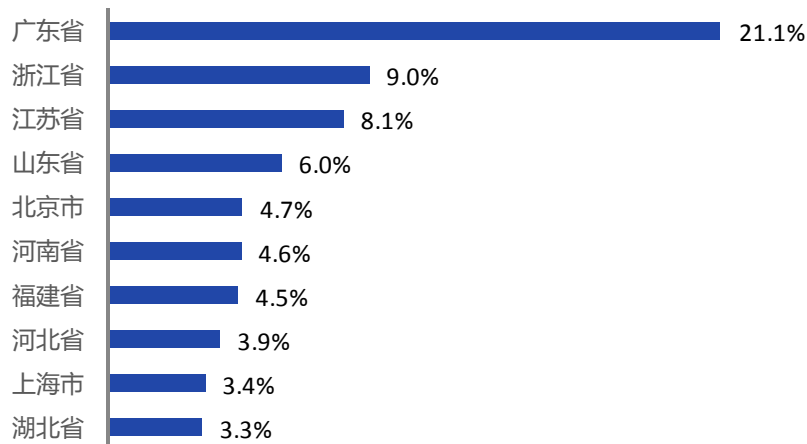


东南沿海和中部地区是诈骗电话重灾区

诈骗电话归属地最多的十大省



接到诈骗电话重灾区十大省市

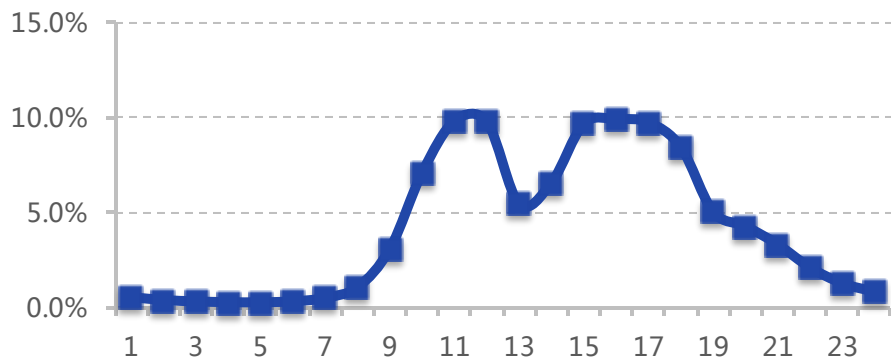


- 2016年1-8月，诈骗电话归属地**最多的是广东省，占比14.6%**，其次为福建与浙江

- 接到诈骗电话的**最多的也是广东省，占比21.1%**，其次是浙江与江苏

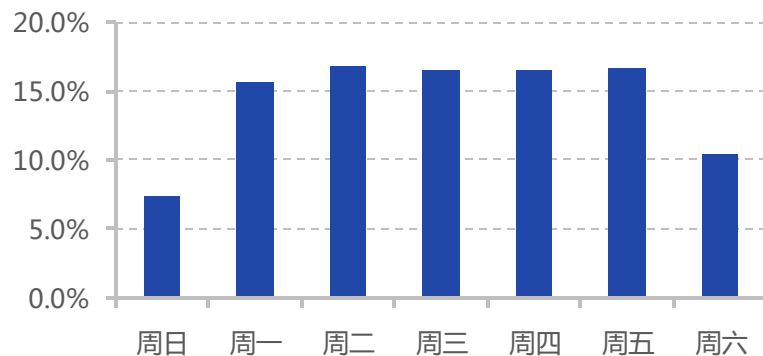
诈骗电话高峰时段

诈骗来电时间段分布



- 一天中，诈骗电话活跃高峰时间段集中在**上午11-12点**，**下午15-18点**

诈骗电话一周分布



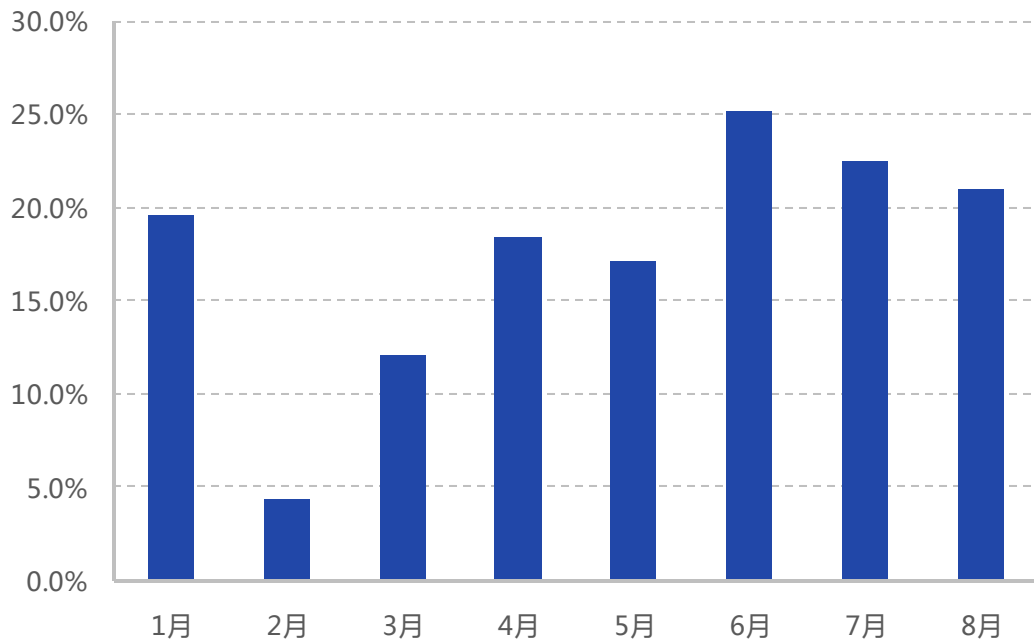
- 相较于周末，工作日骗子更为活跃，诈骗电话量是周末的**两倍**

诈骗短信屡禁不止

诈骗短信屡禁不止

- 从2016年钱盾拦截提醒诈骗短信的情况来看，除去过年期间诈骗短信明显减少外，其余月份诈骗短信占比一直处于较高水平
- **每月人均收到2条诈骗短信**；诈骗手段花样翻新让人们防不胜防

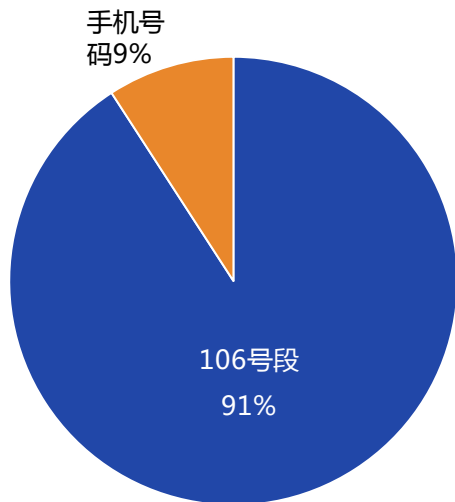
2016年收到过诈骗短信的用户占比趋势



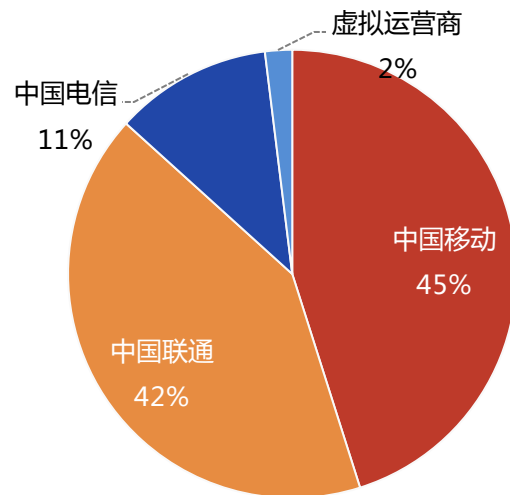
诈骗短信号码源分布

- 诈骗短信号码源中，来自于106号段最多（占比**91%**），其次为手机号码（占比9%）。手机号码中，诈骗短信分别来自中国移动（45%）、中国联通（42%）、中国电信（11%）和虚拟运营商（2%）

诈骗短信源分布

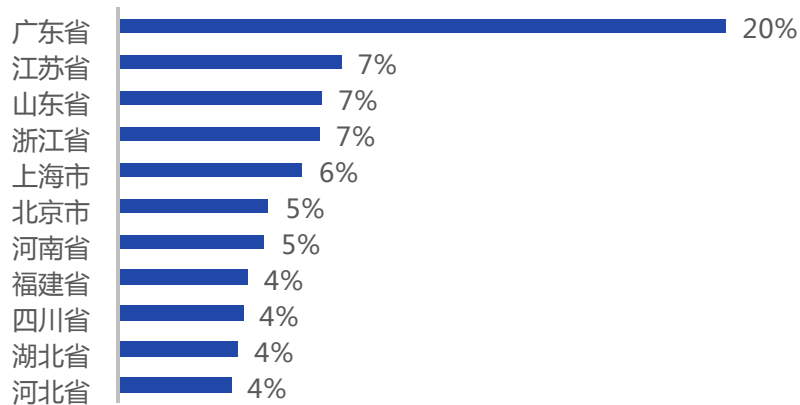


手机号码诈骗短信源分布

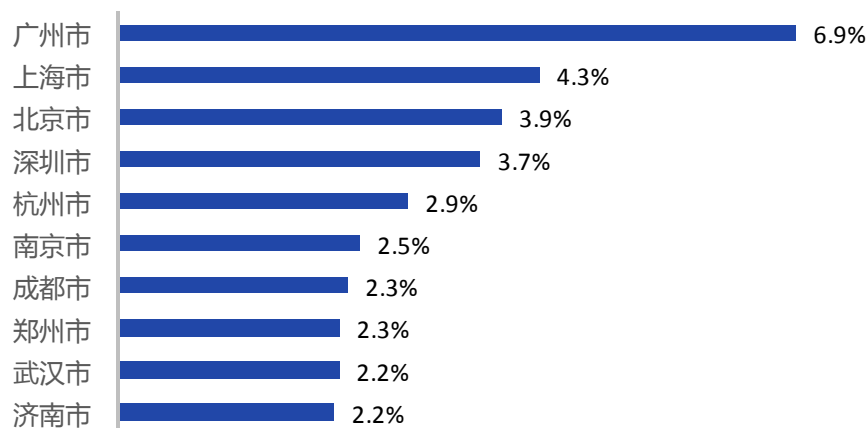


东南沿海和中部地区是诈骗短信重灾区

诈骗短信重灾区十大省



诈骗短信重灾区十大城市

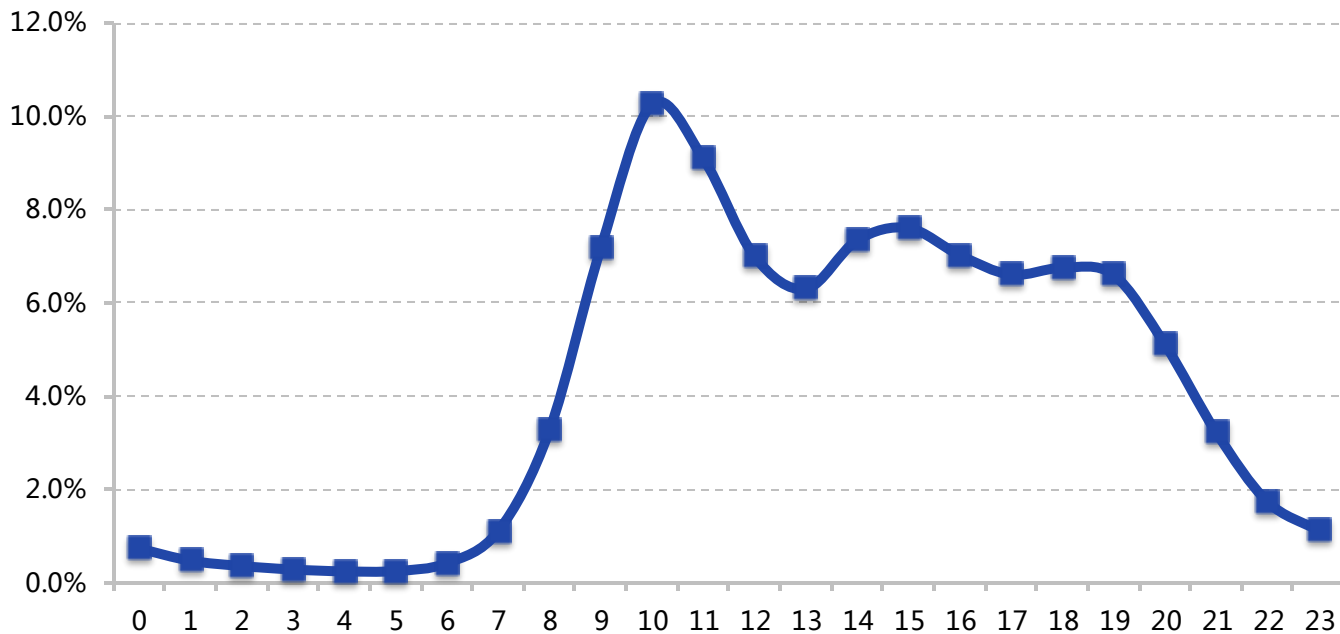


- 2016年1-8月，诈骗短信按照省份划分，重灾区依次为广东省（20%），江苏省，山东省
- 按照城市划分，重灾区依次为广州市（6.9%），上海，北京，深圳
- 东南沿海和中部区域是诈骗短信高发区域

诈骗短信活跃时间段

- 一天中，诈骗短信活跃高峰时间段集中在**上午10-下午19点**，不同于诈骗电话活跃时间，没有明显的午休时间，也比诈骗电话活跃时间更早，周期更长

诈骗短信时间段分布



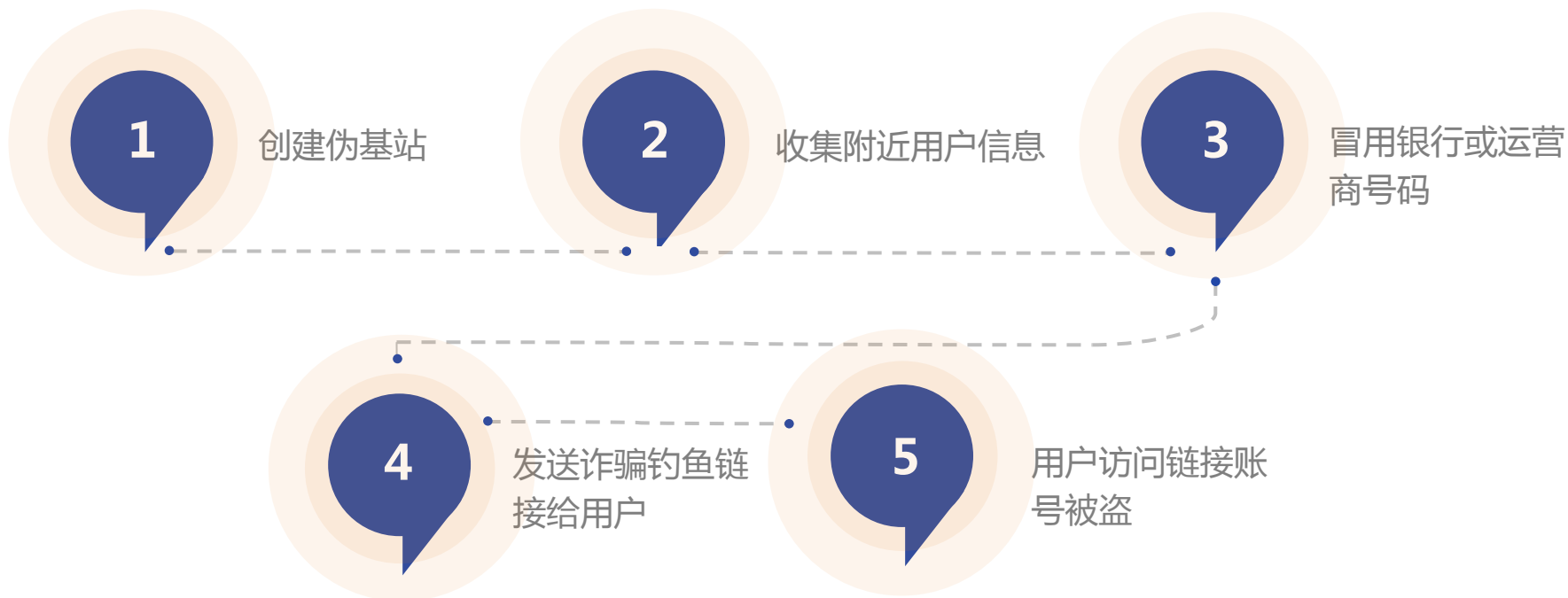
典型钓鱼类诈骗案件

伪基站+钓鱼网址让钓鱼诈骗更可信



- 浙江市民钱先生的手机不久前收到一条显示为真实运营商号码发来的信息：“你的手机积分可以换取270元钱，可以上网提现”，并附有网址链接。钱先生点进去之后觉得页面很正规，就按提示输入了姓名、电话、农业银行卡号和密码，但提交之后就再无音信了，随后去农业银行查询，发现卡里的7948元已全部被提走，损失惨重

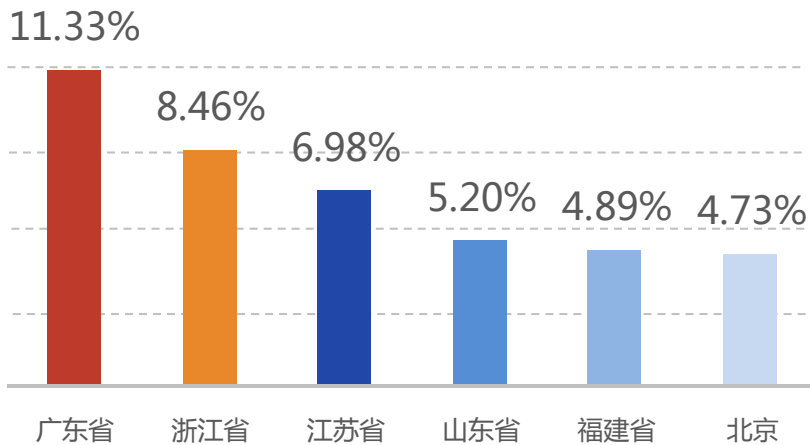
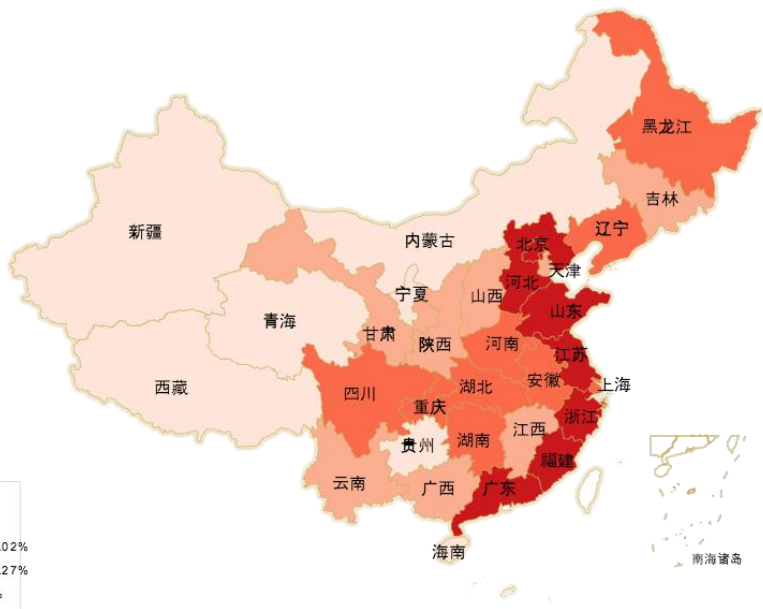
伪基站钓鱼诈骗详解



违法分子通过非法渠道购买伪基站设备，设置完毕使用电动车或者汽车等交通工具携带伪基站在人口密集处收集群众信息，然后冒用银行或者运营商号码下发诈骗或者钓鱼短信给用户，用户查看短信后，误以为是真的银行或者运营商从而被骗。

钓鱼类案件地域分析

- 被骗用户中男性多于女性，**广东省 (11%)** 钓鱼网址相关的案件最多，总体案件分布，**南方**多于北方

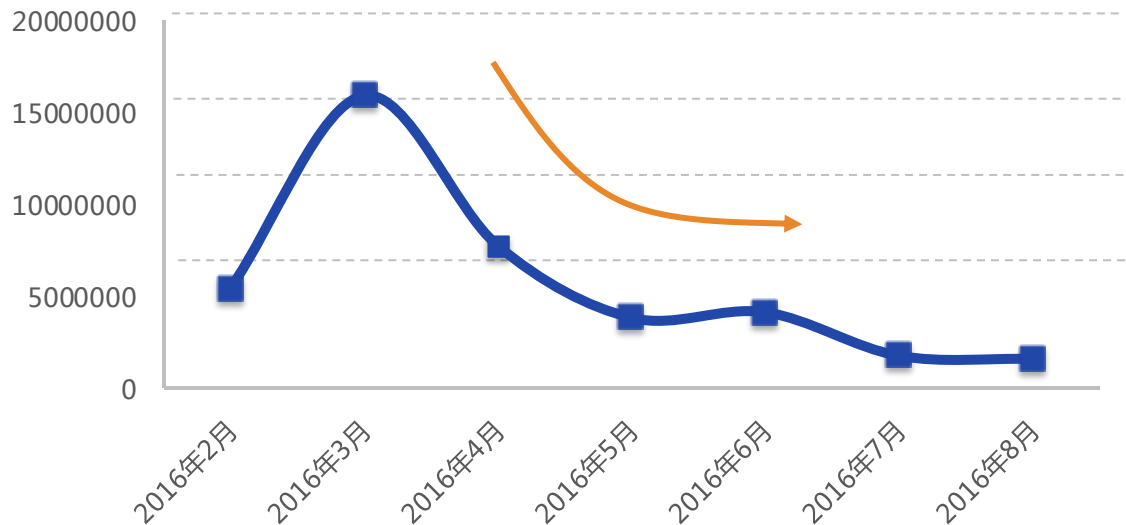


伪基站治理成果

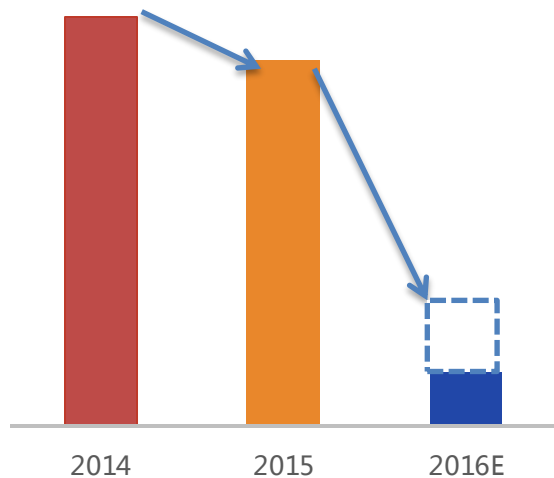
上半年伪基站的治理卓有成效

- 钱盾的数据显示，伪基站短信是钓鱼网址最重要的下发通道，经过上半年各级省市公安部门的专项整治后，钓鱼网址的感染数量从4月开始正在逐渐减少，同时钓鱼网址的案件量对比往年也有比较大的改善

钓鱼网址感染量

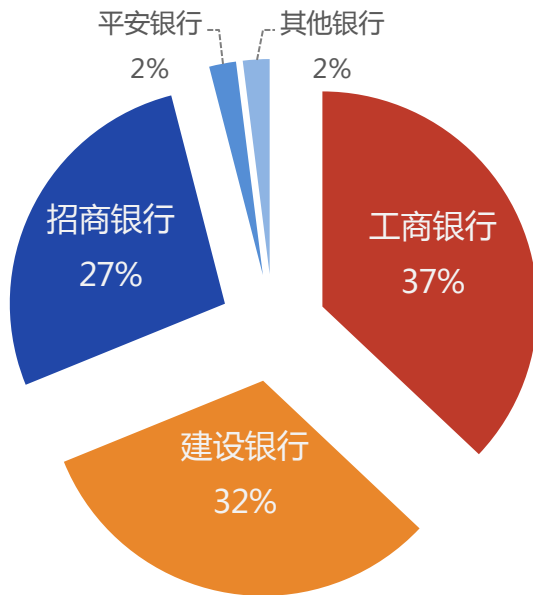
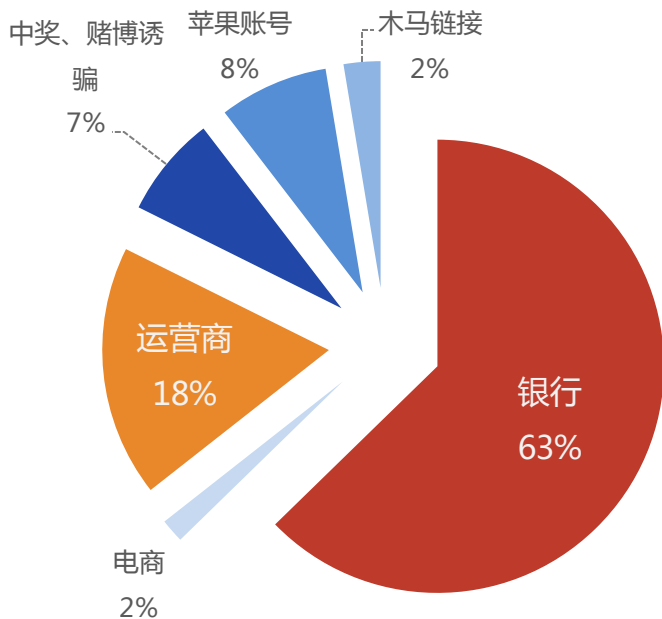


钓鱼网址案件量



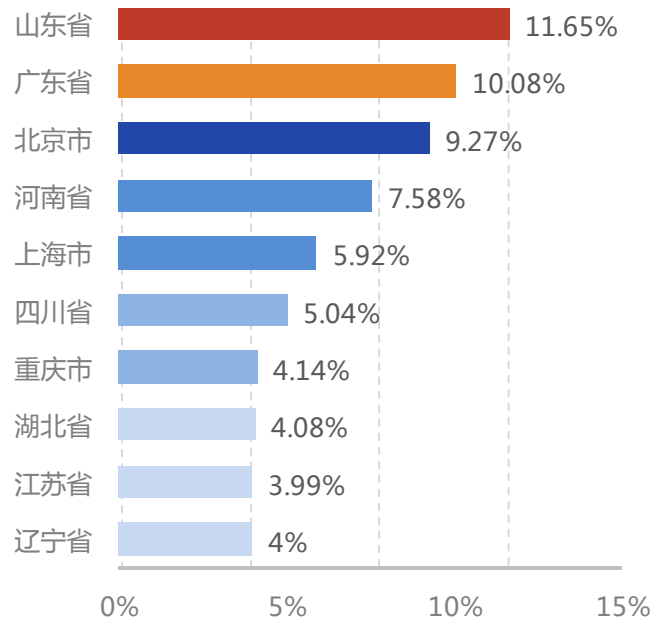
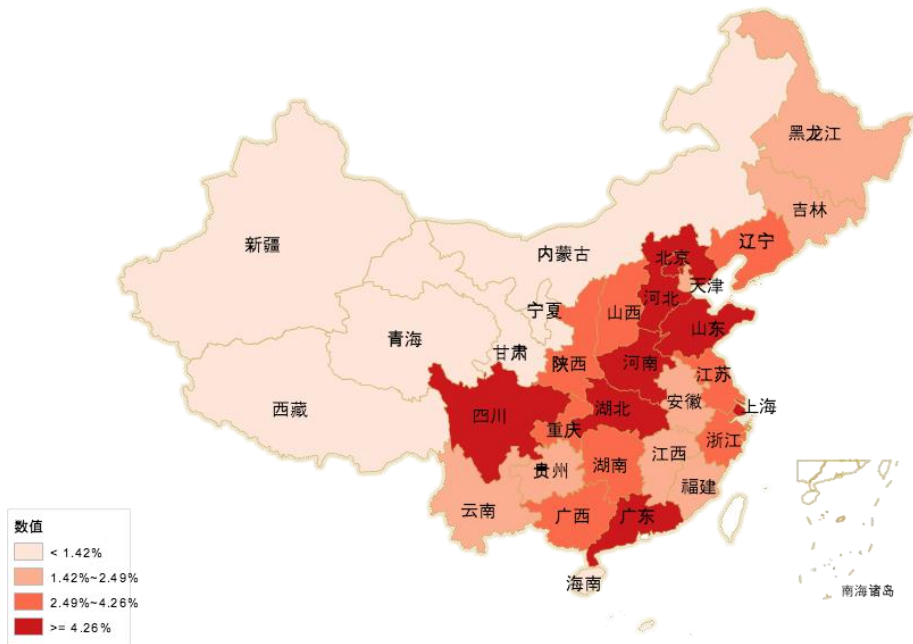
钓鱼网址类型统计

- 从钓鱼网址的类型来看，仿冒银行类比重最高为 **63%**，其他占比较高的类型包括仿冒运营商18%、仿冒苹果网站8%、中奖赌博类7%、仿冒电商 2%以及木马链接2%等类型的钓鱼网址



钓鱼网址感染量统计

- **山东(11.65%)**、广东(10.08%)、北京(9.27%)、河南(7.58%)是钓鱼网址(根据域名统计)最多的四个省或者直辖市; 伪基站是钓鱼网址发送的最主要也是危害最大的渠道, 山东省被发现的伪基站最多, 所以钓鱼网址的感染量也最多



PART 2

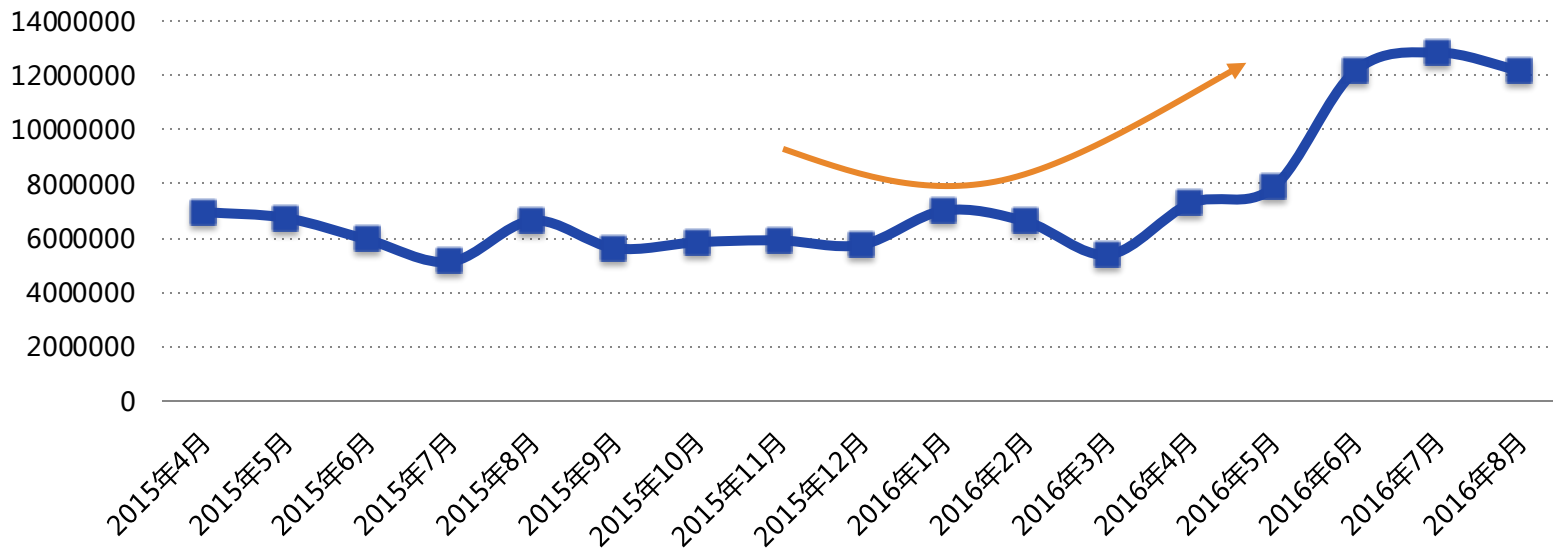
手机病毒木马危害及趋势

病毒木马作为PC 时代的黑产犯罪工具，在手机支付、移动金融逐渐覆盖的今天，成倍的向手机进行转移，造成资损难以防范

病毒木马感染移动设备概况

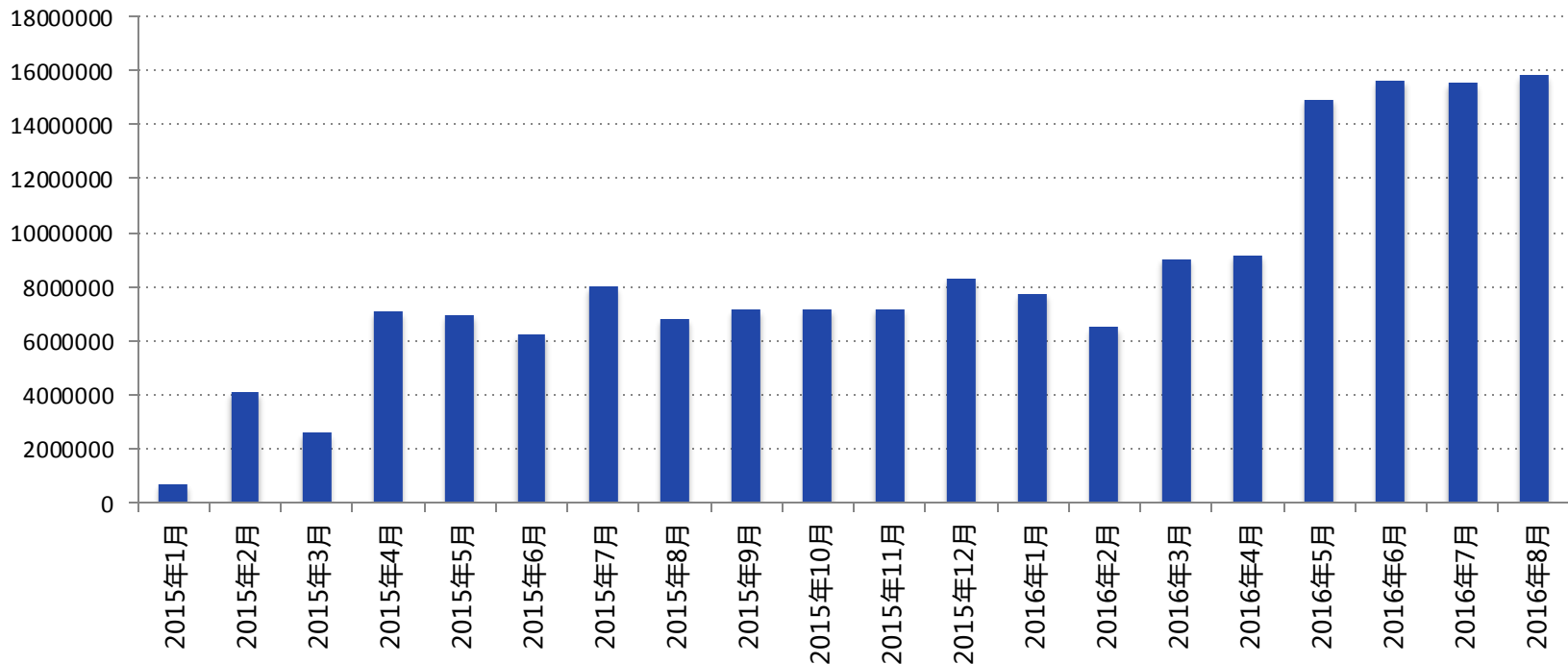
- 2016年1-8月，据钱盾统计，病毒感染移动设备量呈上涨趋势，**累计感染设备数7600万**，已接近去年全年总量。前8个月月均感染设备数955万，高于去年全年月均值45%，进入5月后数据感染设备尤为明显，用户所面临的风险加剧

感染移动设备数



病毒木马手机查杀量极速攀升

- 今年手机病毒木马查杀量呈现上涨趋势，前8个月查杀总量已突破9440万/次，超过去年全年次数近31%，月平均查杀次数1180万，与去年相比上涨近97%，特别是5月以来被查杀的病毒木马量攀升极快，**随着手机支付的普及，犯罪分子正在加快从传统PC向手机的转移**

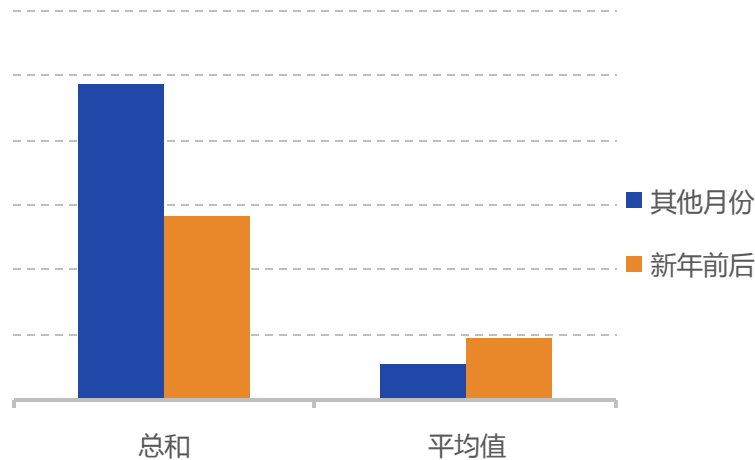
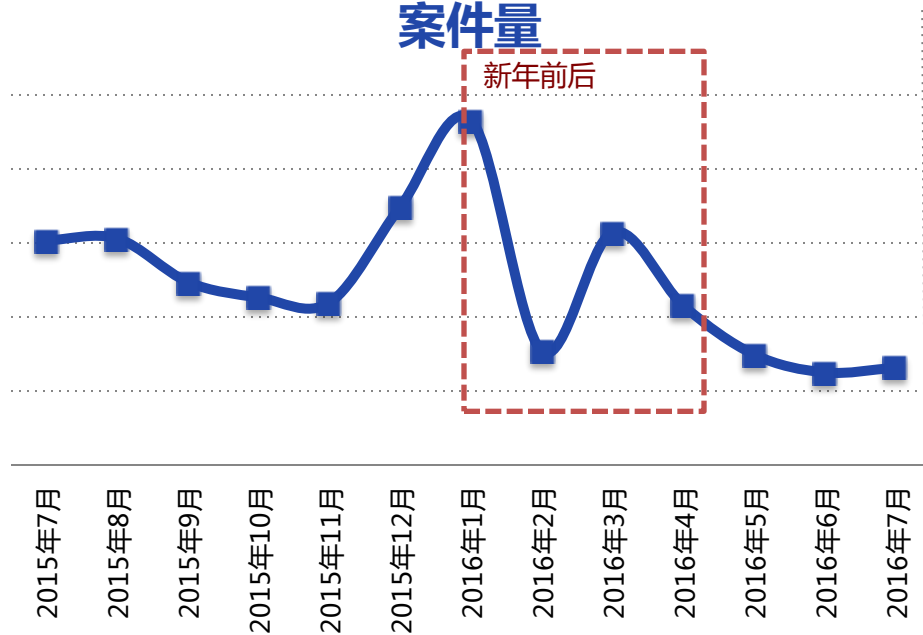


新年前后是资金案件高峰期

- 2016年上半年，随时手机安全软件的普及，因手机病毒木马造成的资金损失案件量呈下降趋势，与去年下半年相比，整体案件量下降16%，但值得关注的是年底12月、次年1月，3月是案发的高峰期，**新年前后案件量平均值超过其他月份74%**

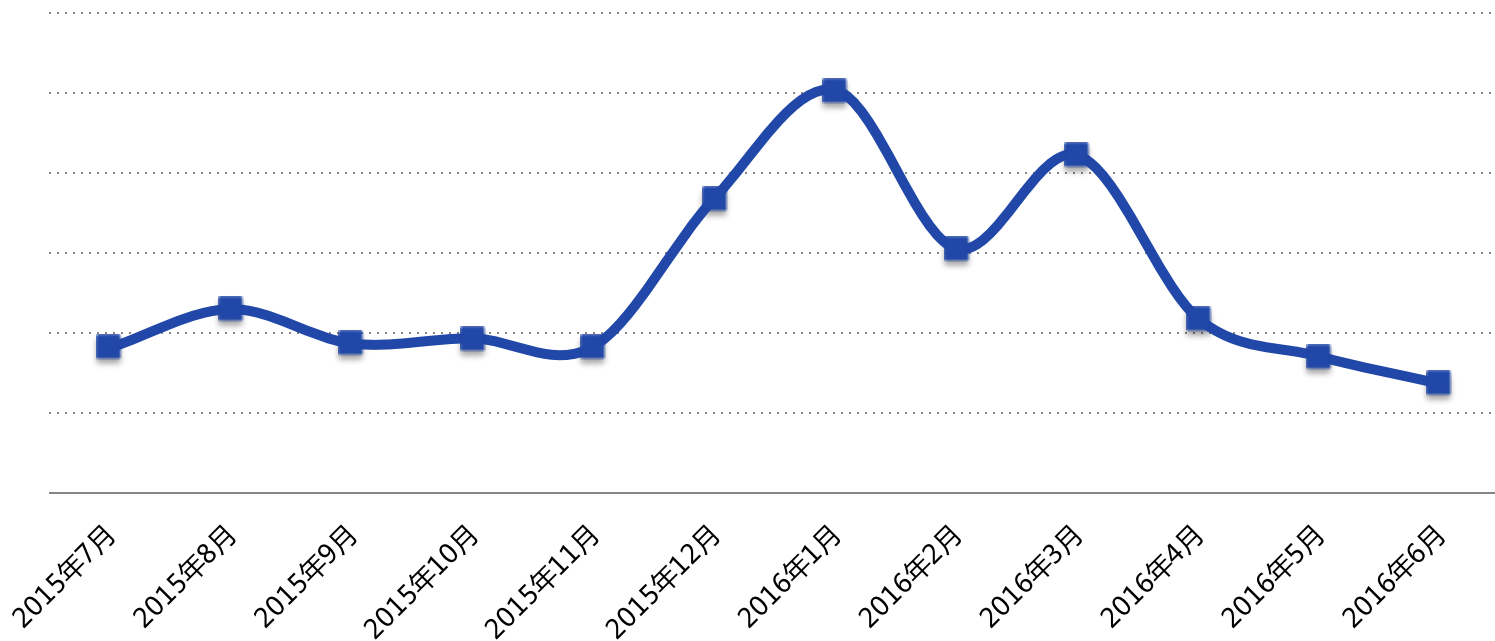
案件量

新年前后



病毒木马造成的资金损失上涨24%

- 2016年上半年，因手机病毒木马造成的资金损失额度呈上涨趋势，平均资损已经达到2051元，与去年下半年相比，平均资损上升34%，损失总金额上涨24%，**月均资损额度**上涨58%，其中1月最高，月均资损额约为2015年下半年的2.5倍，2016年上半年的1.5倍，**因木马病毒造成的资金损失在年前达到了顶峰，新年前需要特别警惕**

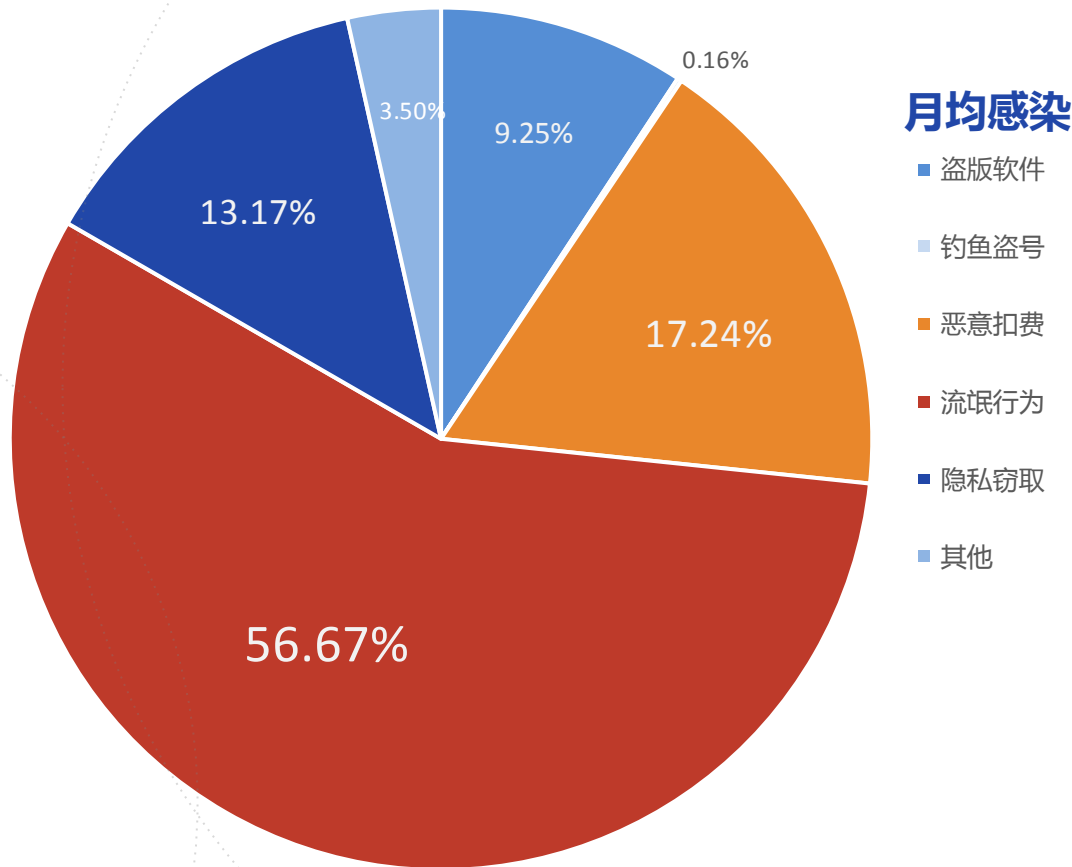


隐私窃取类病毒木马占比同比上涨

2016年1-8月发现的病毒木马感染设备中，Top5的种类行为分别为流氓行为、恶意扣费、隐私窃取、盗版软件、钓鱼盗号；

该五类占整体比例的96%，其中流氓行为占56.67%，与去年整年相比下降10%，恶意扣费占比17.24%，与去年整年相比下降2%；**隐私窃取占比**

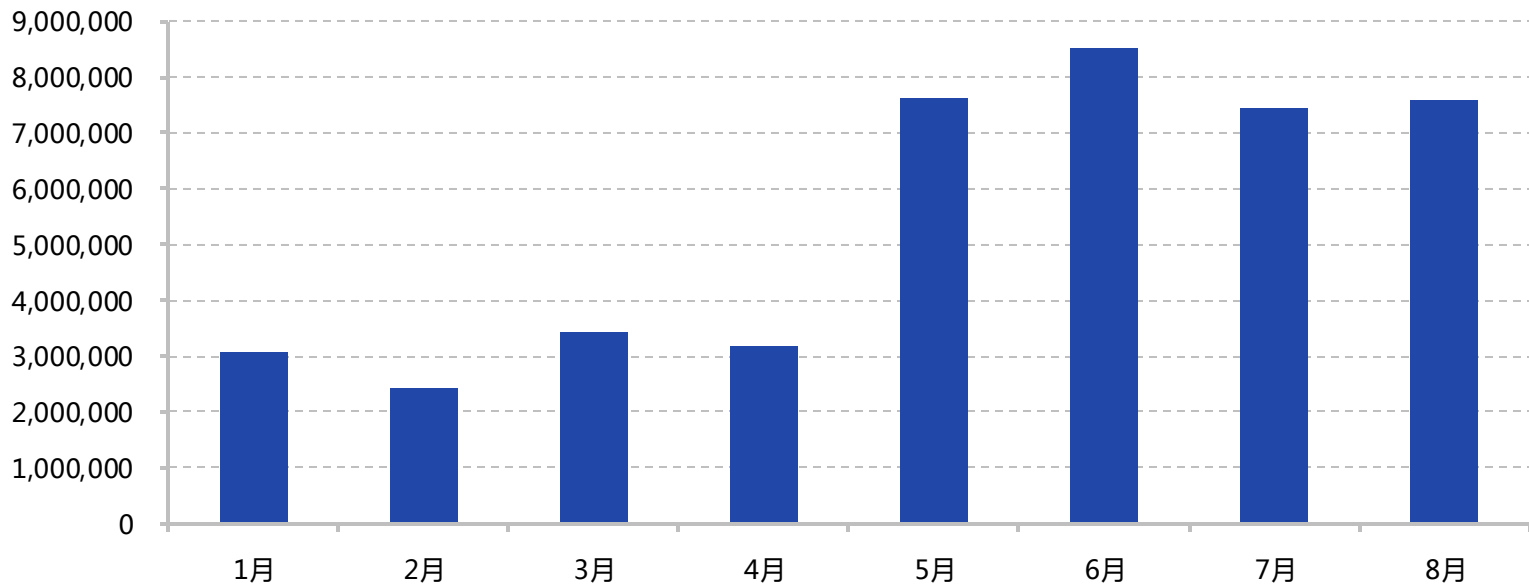
13.17%，与去年整年相比上升4%，隐私窃取等病毒容易造成用户隐私信息泄露，影响金融账户资金，对用户危害极大



具有流氓行为的病毒木马感染最多

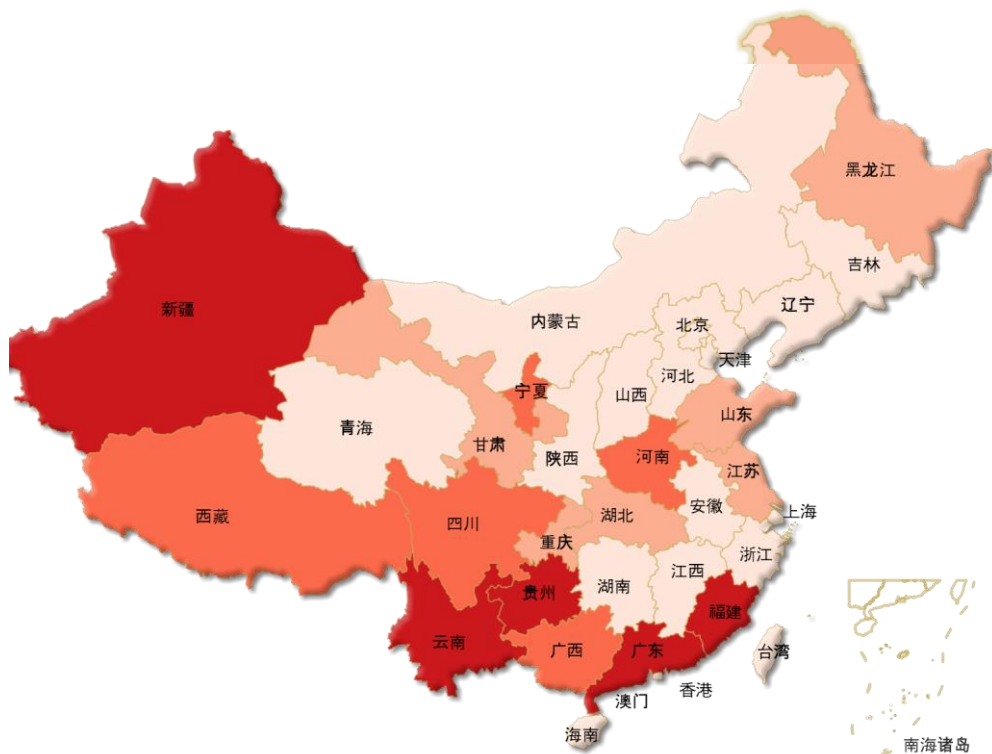
- 2016年1-8月，具有“流氓行为”的病毒木马感染用户量最多，累计感染移动设备数**4330万台**，月均感染541万台，这类病毒匿名弹窗、恶意推送广告、私自下载软件等，对用户体验和手机安全造成危害

流氓行为感染设备数



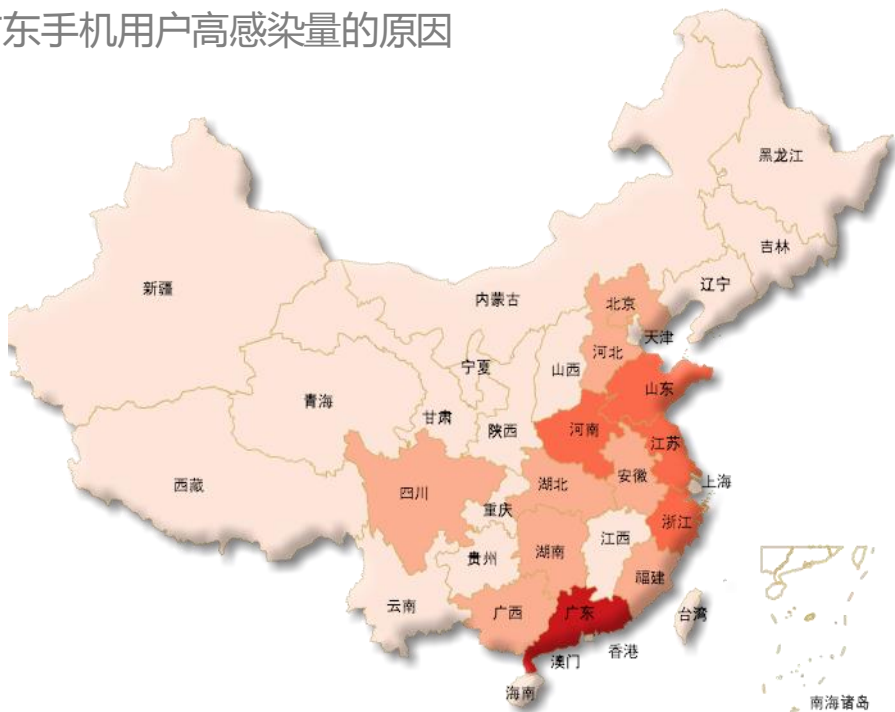
广东、福建及西部地区用户饱受危害

- 2016年，感染病毒木马设备比例最高的省份，**从去年西南地区开始向东南沿海经济发达地区蔓延**。广东、福建、贵州、云南、新疆排名前五。其中，**广东超越贵州成为最易被感染的省份**，比例达10%，比全国平均值高出比例33%



广东蝉联病毒木马感染设备量最多省份

- 继2015年统计分析之后，**广东省依然是饱受病毒木马感染设备量最多省份**，其前8个月的设备感染量约占全国总感染量的15%，较去年提升1%
- 由于广东省地处经济发达区域，外来务工人员人数居全国前列，华为、OPPO、vivo等本土手机品牌厂商崛起，带动本地市场较强消费，人均持有多台手机现象逐渐普遍，这些都是导致广东手机用户高感染量的原因



谢谢

Thank you