腾讯安全移动安全实验室
TENCENT SECURITY MOBILE SECURITY LAB
腾讯手机管家
有实力 无所惧

腾讯移动安全实验室

2019年上半年手机安全报告

Mobile Security Report Of First Half Year,2019

目录

腾讯移动安全实验室 2019 年上半年手机安全报告

摘要

手机病毒

2019 年上半年，Android 新增病毒包 189.87 万个，同比下降 59.49%。支付类病毒包新增 3.19 万个，同比增长了 18.30%。

2019 年上半年，Android 手机病毒感染用户 3813.70 万，同比下降了 37.55%。支付类病毒感染用户近 85.59 万，同比减少了 65.32%。

2019 年上半年，腾讯手机管家共查杀病毒 3.05 亿次，同比减少 31.16%。

2019 年上半年，手机病毒类型主要是资费消耗、恶意扣费、隐私获取和流氓行为这四种类型，占比分别为 40.30%、23.46%、17.75%和 15.10%。

2019 年上半年，手机病毒感染用户最多的省份是广东，占比为 9.55%，其次是浙江（6.55%）和山东（6.18%）。

2019 年上半年手机病毒来源渠道主要以手机资源站、电子市场和软件捆绑为主，占比分别为 23.33%，20.19%和 19.37%。

垃圾短信

2019 年上半年，腾讯手机管家用户共举报垃圾短信近 10.75 亿条，举报诈骗短信近 5425.31 万条。

2019 年上半年，垃圾短信类型中，以广告短信为主，占比 91.78%，其次是诈骗短信（5.11%）和违法短信（3.11%）。

2019 年上半年，用户举报垃圾短信和诈骗短信最多的省份是广东省，占比分别为 14.06%和 18.37%。用户举报垃圾短信最多的城市分别为北京（5.71%）、深圳（4.12%）和成都（3.80%），举报诈骗短信最多的城市是深圳（5.43%）、广州（4.81%）和北京（4.59%）。

骚扰电话

2019 年上半年，腾讯手机管家用户共举报骚扰电话 1.64 亿次，较去年同时期增长 14.83%，其中诈骗电话举报 2793.84 万，同比减少 5.95%。

2019 年上半年，iOS 用户标记骚扰电话和诈骗电话的高峰期是 4 月和 5 月，共标记骚扰电话 977.23 万次，其中诈骗电话 169.02 万次，占骚扰电话标记数的 17%。

2019 年上半年，在各类骚扰电话中，“响一声”最高占比最高，达 39.60%，诈骗电话占比 17.03%。

根据腾讯手机管家用户主动上报的恶意线索显示，常见的骚扰电话恶意线索关键词包括索要验证码、转账到安全账户和网络订单有问题，占比分别为 29.64%、23.83%和 14.33%。

2019 年上半年，用户举报骚扰电话和诈骗电话最多的省份是广东省，占比分别为 12.52%和 15.40%。举报骚扰电话和诈骗电话数最多的城市北上广深和部分新一线城市。

恶意网址

2019 年上半年，腾讯安全实验室检测到恶意网址 1.04 亿次，拦截恶意网址 3010.05 亿次。

2019 年上半年，在拦截的各类恶意网址中，色情网站排名第一，占比 56.91%，博彩网站和信息诈骗紧随其后，占比分别为 34.78%和 6.86%。

风险 WiFi

根据腾讯 WiFi 管家数据显示，2019 年上半年，截至 6 月，已发现的公共 WiFi 总数近 9.14 亿。连接公共 WiFi 的人群以 30 岁以下用户为主，占比 60.79%，男性用户略多于女性。

2019 年上半年，在公共 WiFi 中，未发现风险 WiFi 占比为 61.00%，风险 WiFi 占比 39.00%，其中高风险 WiFi 占比 19.19%，低风险 WiFi 为 19.81%。

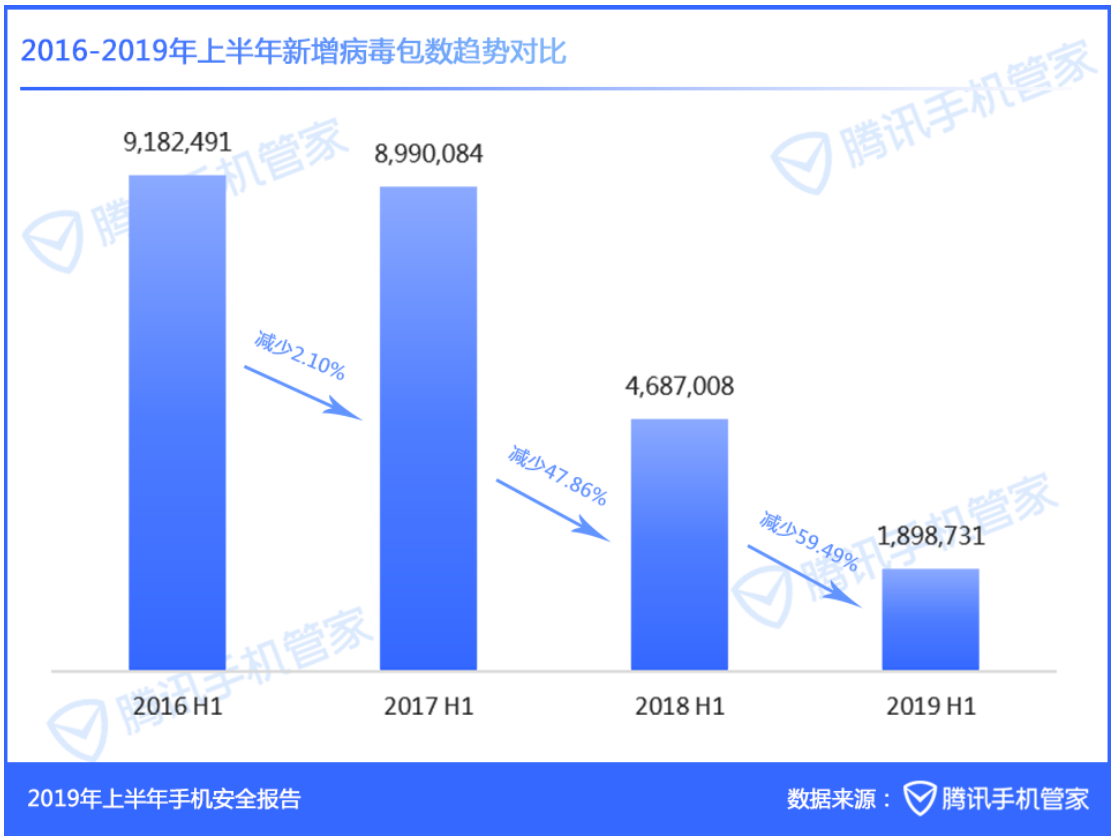
2019 年上半年，高风险 WiFi 攻击行为以 ARP 攻击为主，占比高达 99.33%，其次是虚假 WiFi 和虚假 DNS，占比分别为 0.59%和 0.08%。

2019 年上半年，高风险 WiFi 主要分布在广东、山东和江苏等省份，占比分别为 11.10%、7.06%和 6.47%。在城市方面，高风险 WiFi 在各个城市之间的分布较均匀，主要分布在上海（2.25%）、重庆（2.23%）和北京（2.05%）。

第一章 2019 年上半年手机病毒现状分析

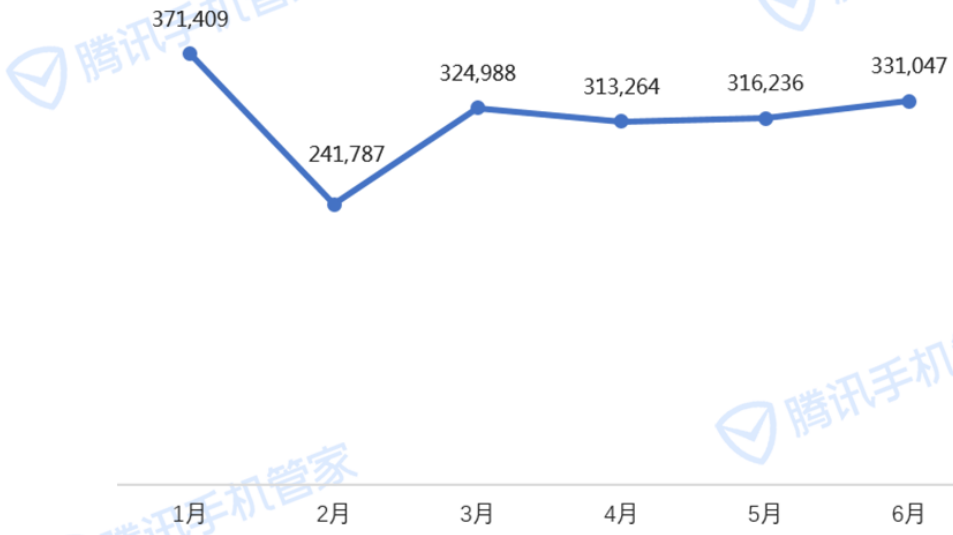
随着移动设备的数据价值越来越大，恶意程序、资费消耗、数据泄露等移动端应用安全威胁与日俱增，Android 应用端的安全防护引起全行业重视。2019 年上半年，在对移动应用的数据安全与隐私保护日益重视的背景下，基于腾讯移动安全实验室新增病毒包数、手机病毒感染用户数、病毒查杀次数、感染地域分布等数据进行统计分析发现，Android 平台的安全风险状况依然严峻，出现了新的挑战，但同时也有所好转。

1.1 2019 年上半年手机病毒包增长趋势进一步减缓



根据腾讯手机管家数据显示，2019 年上半年手机病毒包新增 189.87 万个，较去年同期减少 59.49%，为近年来最低。从去年开始，工信部联合多企业、多单位开展移动恶意程序专项治理工作，整治恶意应用的违法违规行为，维护用户的合法权益。

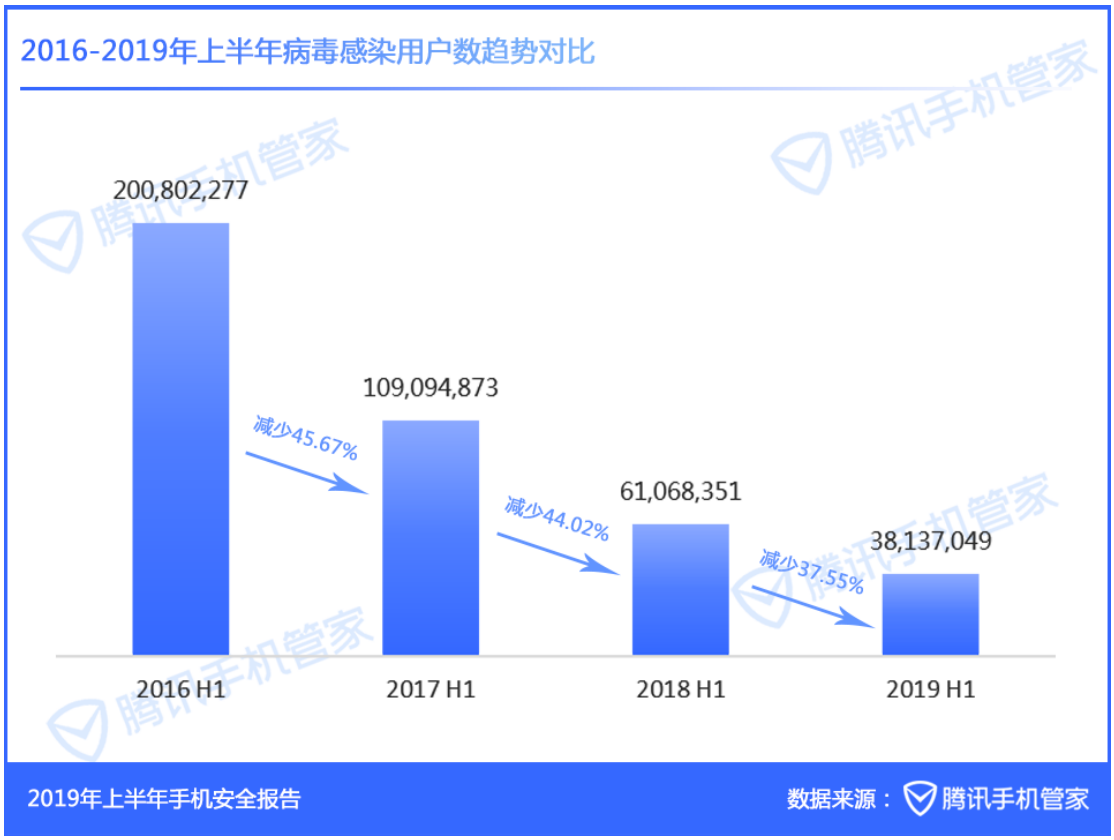
2019年上半年新增病毒包数变化趋势



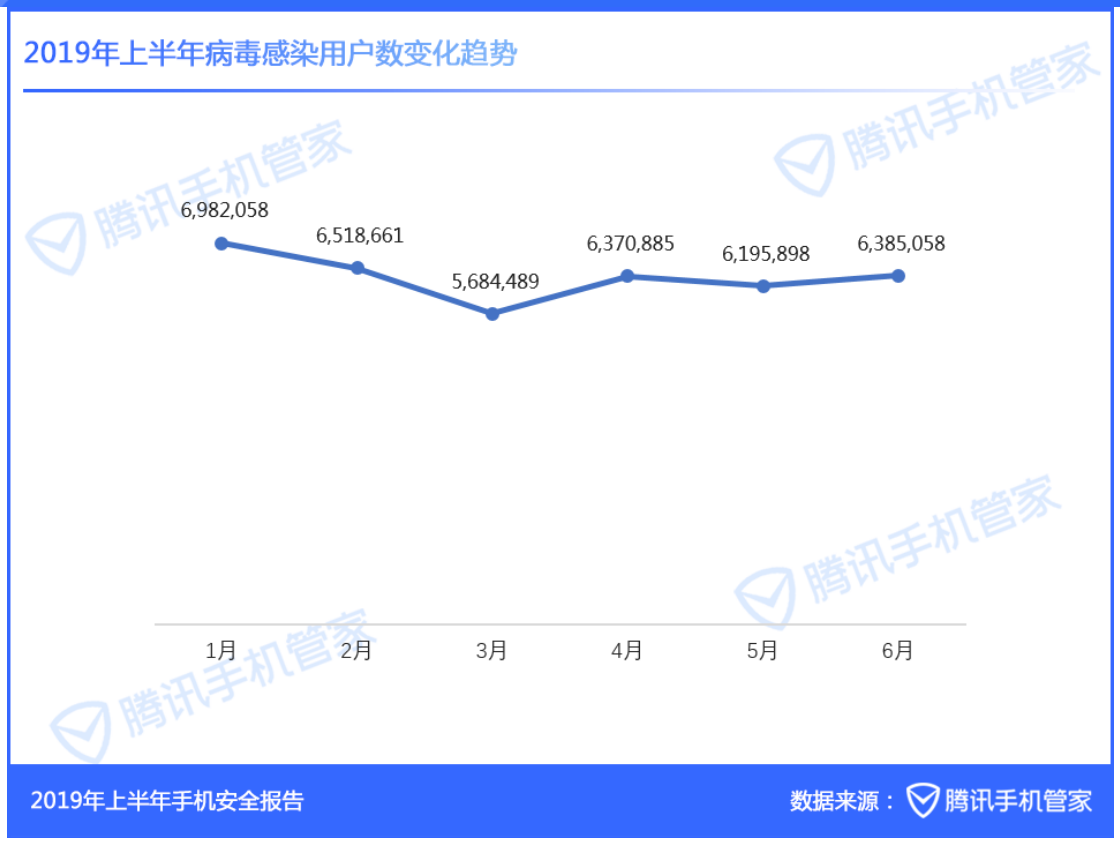
2019年上半年手机安全报告 数据来源：腾讯手机管家

2019 年上半年平均每月新增 31.65 万个病毒包，1 月份新增病毒包最多，达 37.14 万个。这些病毒包通常都会伪装成各类打色情擦边球的应用、游戏破解类应用、聊天交友应用等诱导用户下载安装。

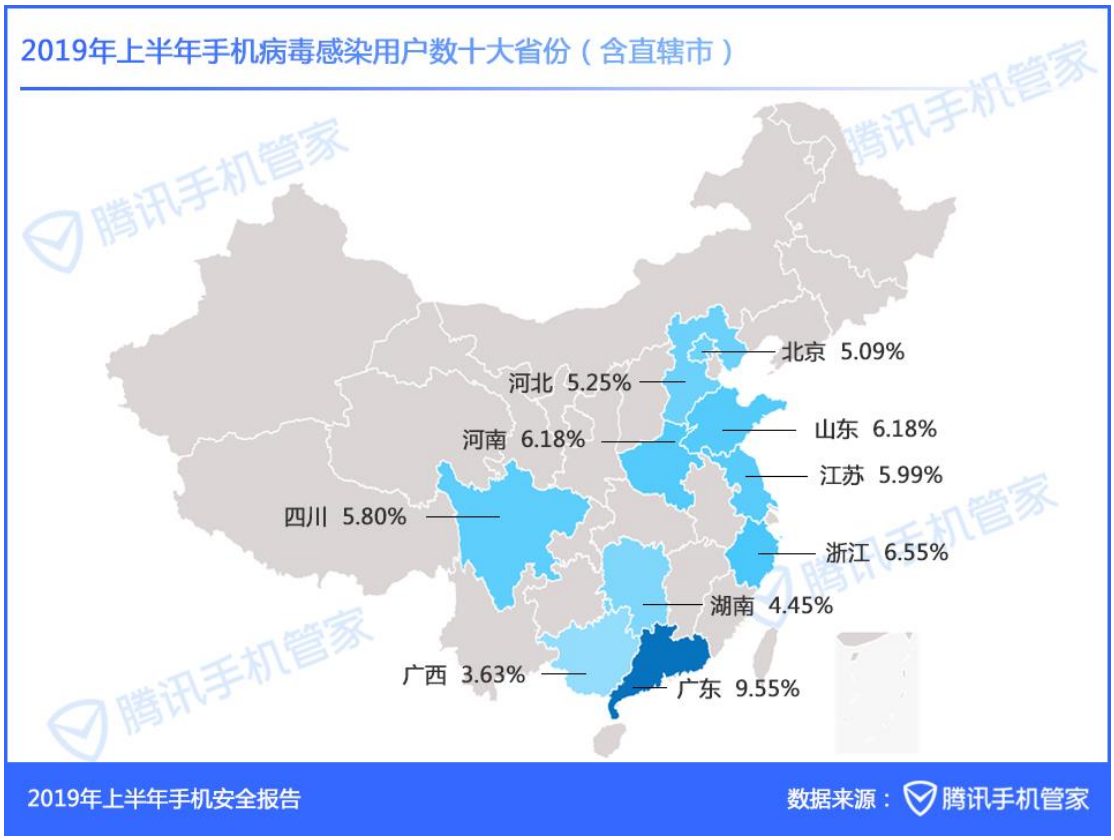
1.2 2019 年上半年感染病毒用户 3813.70 万



2019 年上半年病毒感染用户数达 3813.70 万，同比下降了 37.55%。有关部门对病毒 APP 和风险 APP 的预警和公示，以及安全防护软件对病毒的查杀，有效降低病毒感染人数。

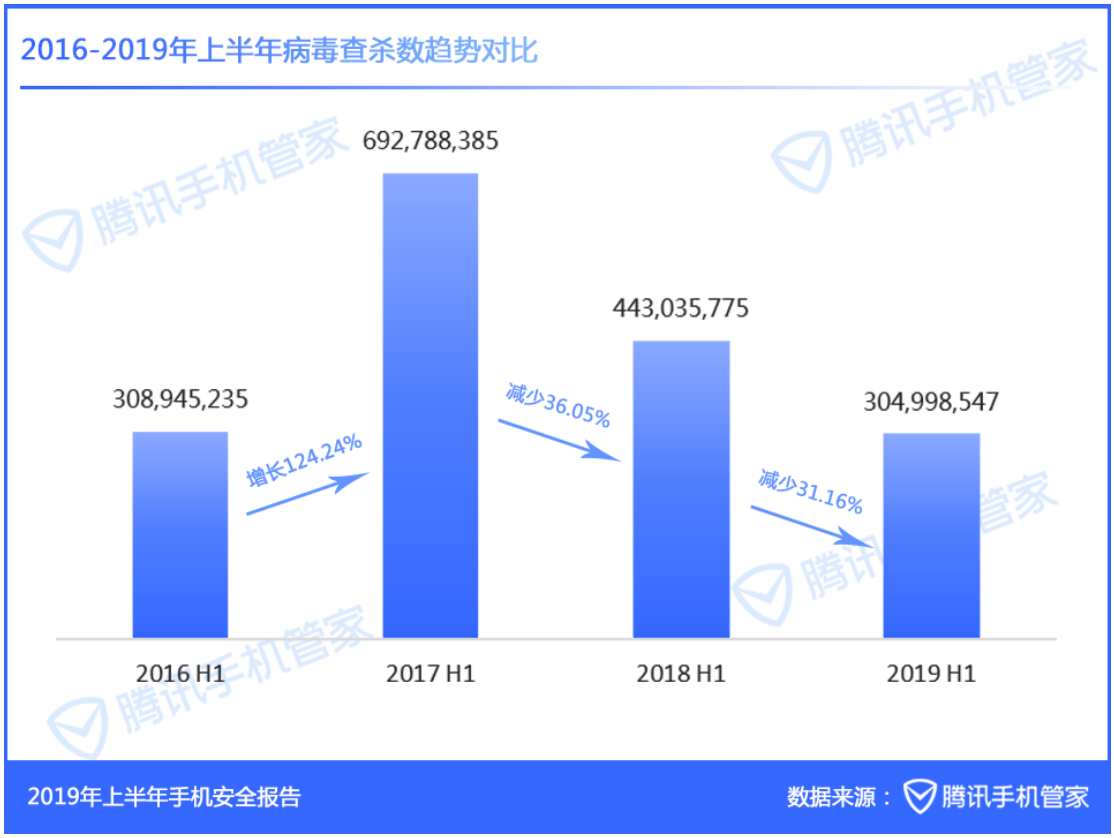


2019 年上半年平均每月感染 635.62 万用户，各月之间相差不大，最高是 1 月份，近 698.21 万。

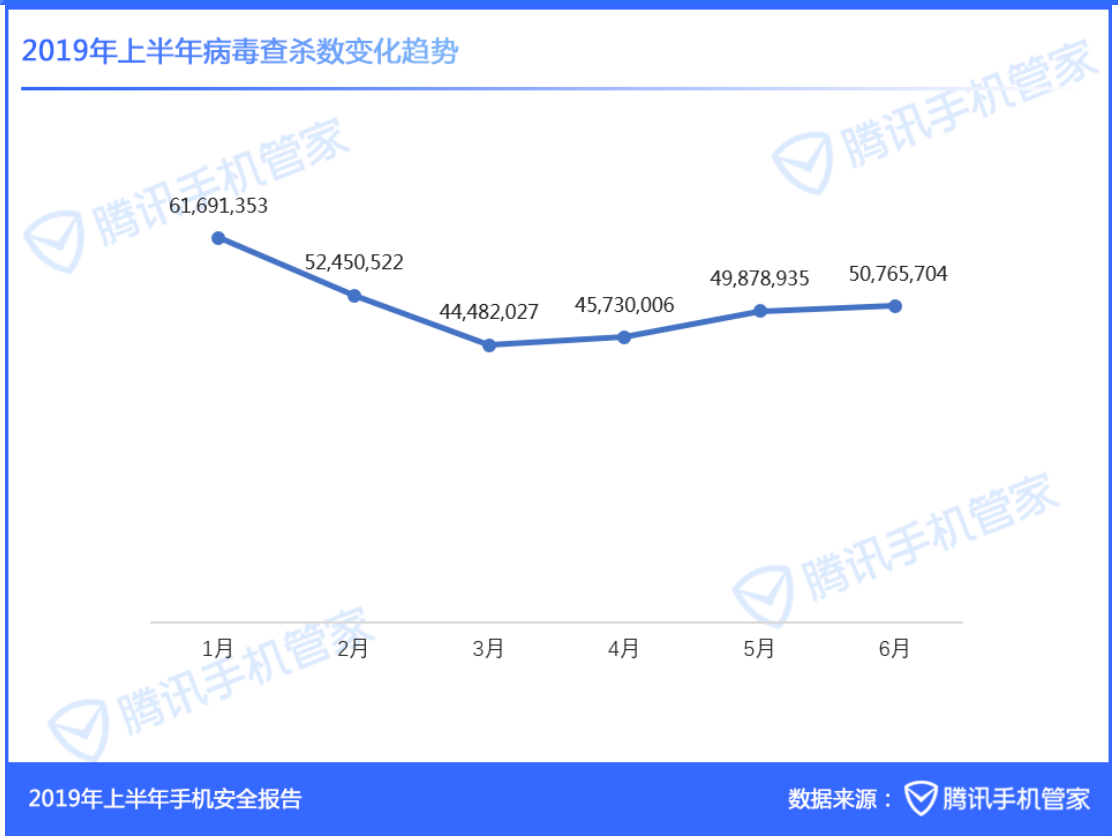


病毒感染的地域分布上，2019 年上半年病毒感染用户最多的省份仍然是广东（9.55%），浙江（6.55%）和山东（6.18%）。

1.3 2019 年上半年腾讯手机管家共查杀安卓病毒 3.05 亿次

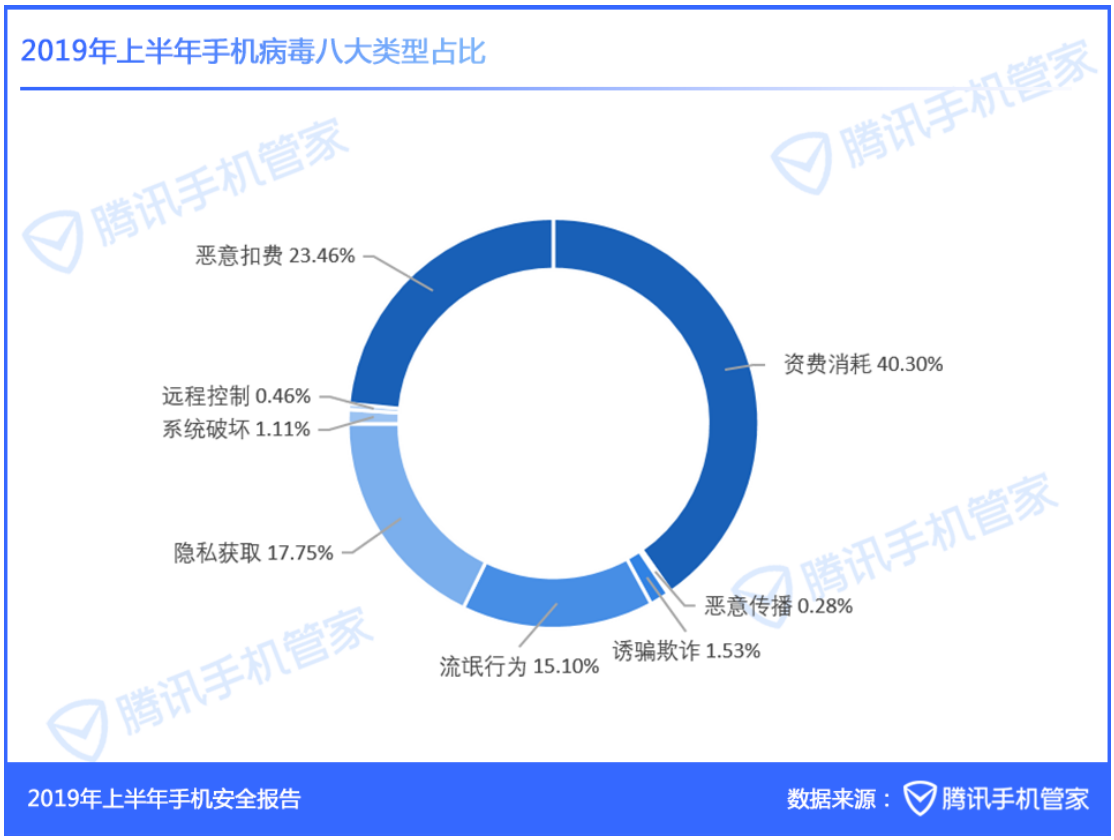


2019 年上半年腾讯手机管家共查杀病毒 3.05 亿次，同比下降 31.16%。作为移动端的第一道安全防线，腾讯手机管家不断升级安全能力，探索不同场景下用户的安全需求并给出解决方案，帮助用户屏蔽木马病毒、骚扰诈骗电话和短信、欺诈网址等风险，全方位保护用户手机安全。国际知名第三方网络安全测评认证机构——赛可达实验室发布 2019 年 5 月份全球手机安全软件(中文版)病毒防护能力横评报告，腾讯手机管家以 99.84%的查杀率占据榜首，在众多手机安全软件中脱颖而出，持续领跑安全行业。



2019 年上半年腾讯手机管家平均每月查杀病毒 5083.31 万次，1 月份是查杀高峰期近 6169.14 万次，3 月查杀病毒数最少 4448.20 万次。

1.4 2019 年上半年手机病毒类型：以资费消耗和恶意扣费为主



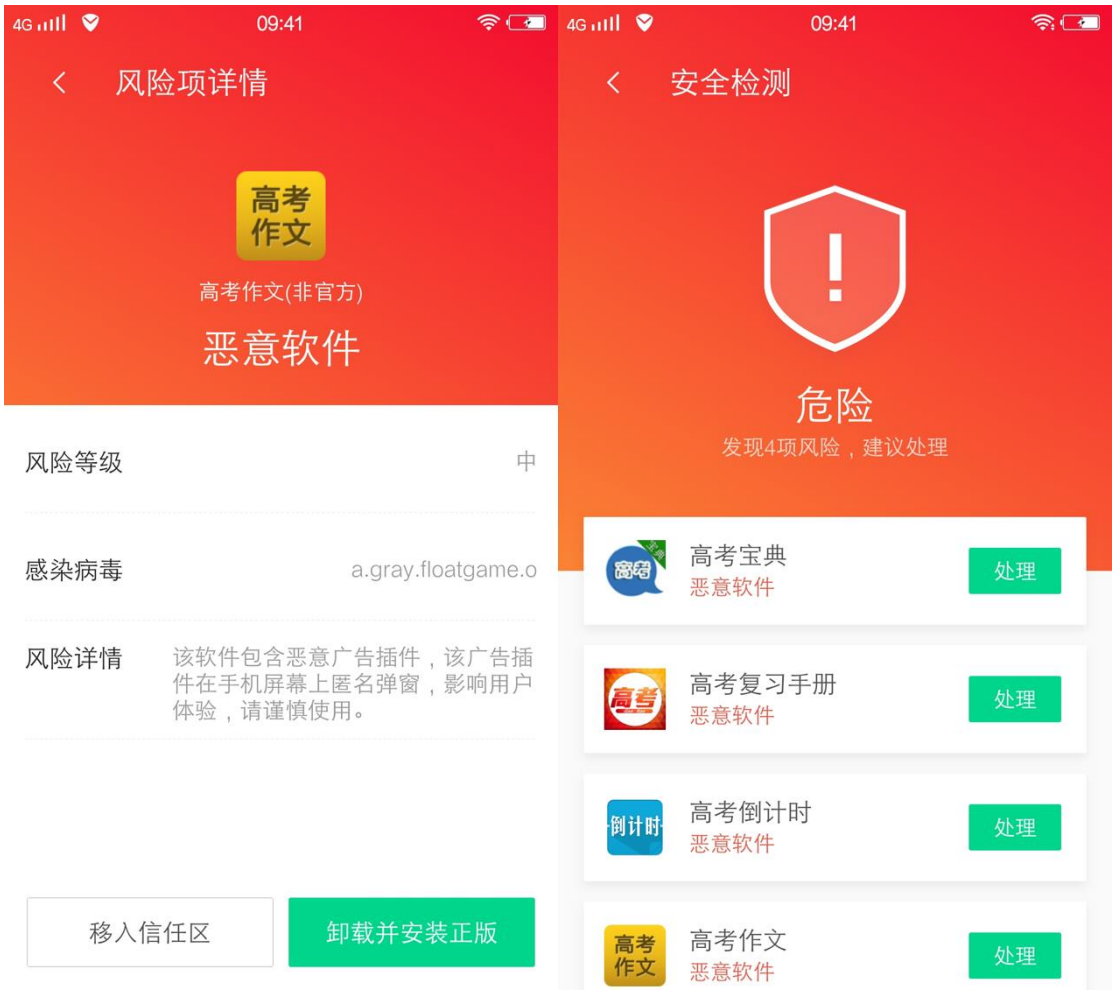
2019 年上半年，手机病毒以资费消耗、恶意扣费、隐私获取和流氓行为这四种类型为主，占比分别为 40.30%、23.46%、17.75%和 15.10%。

资费消耗型病毒通常在用户不知情或未授权的情况下，通过自动拨打电话，发送短信、彩信、邮件，频繁连接网络等方式，导致用户资费损失。

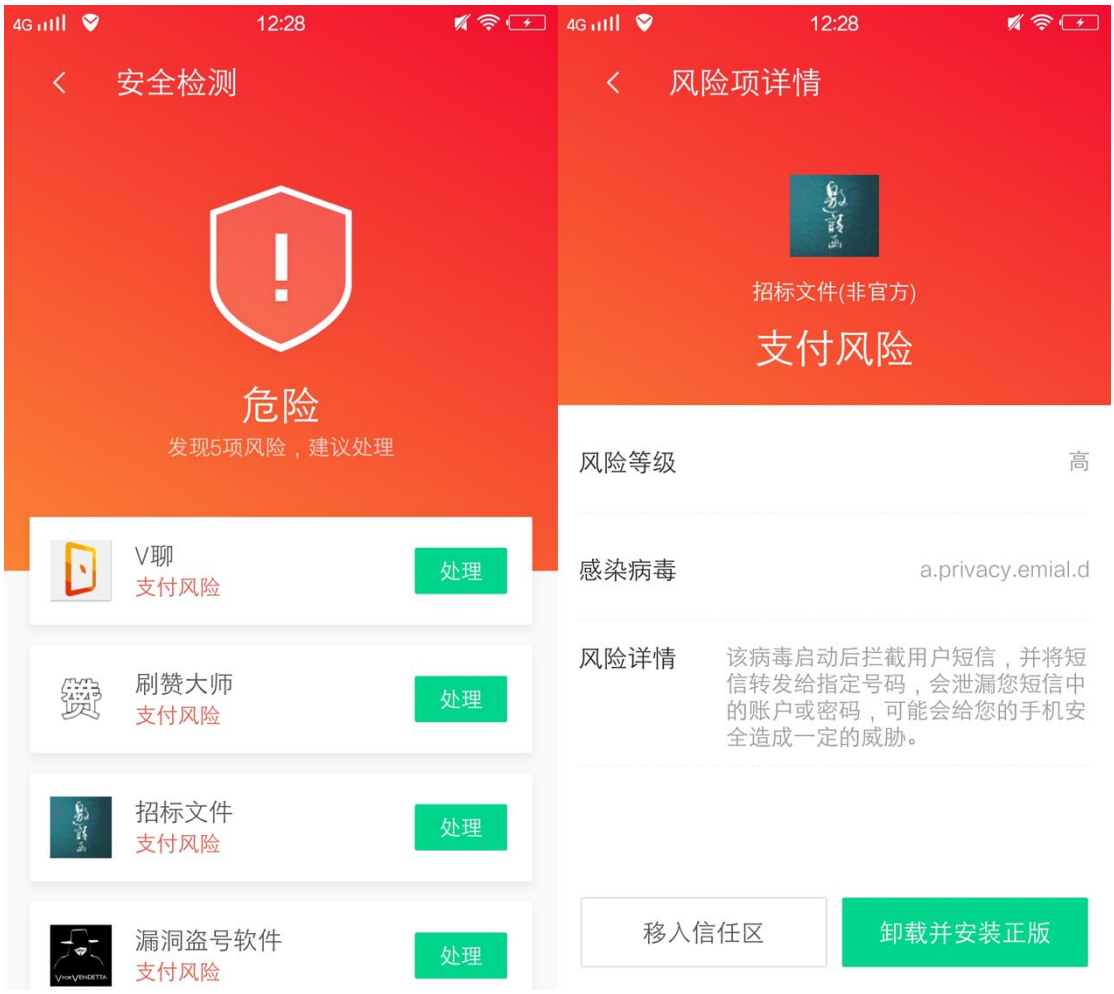
恶意扣费类病毒通常会在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务或使用移动终端支付，导致用户经济损失。国家计算机病毒应急处理中心在“净网 2019”专项行动中，通过互联网监测发现《小历》（版本 1.0）、《头像吧》（版本 1.0）、《Pictu》（版本 2.9.1）这三款移动应用在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务，导致用户经济损失，具有恶意扣费属性。

隐私获取型病毒在用户不知情或未授权的情况下，获取涉及用户个人信息，具有隐私窃

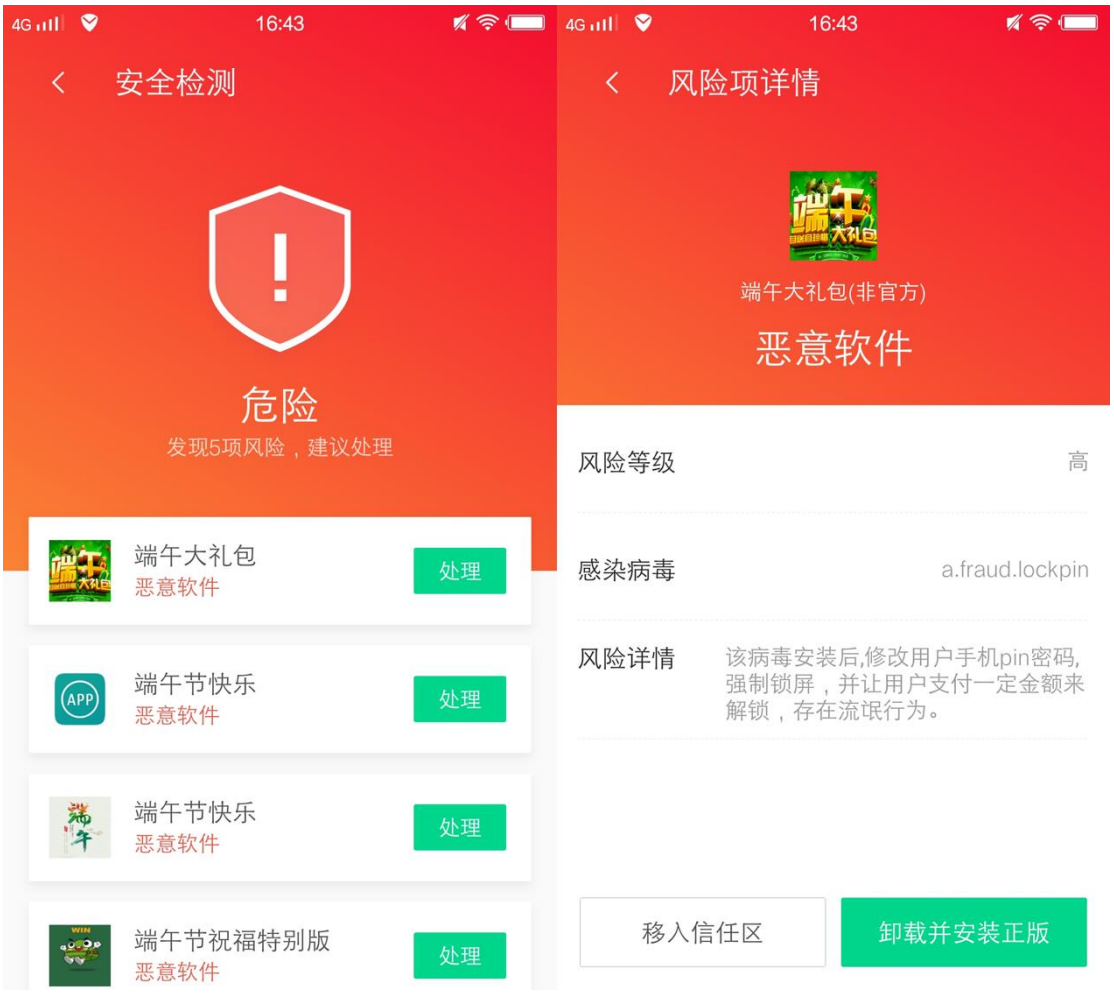
取属性。国家互联网应急中心通过自主监测和样本交换形式，多次发现窃取用户个人信息的恶意程序变种。66 款恶意 AP 被发现窃取用户信息，包括 V 聊、盗号神器、漏洞盗号软件、刷赞大师等 APP，不仅会私自窃取用户的短信和通讯录，还会将用户接收到的新短信转发至指定的手机号，同时在收件箱中删除该短信。



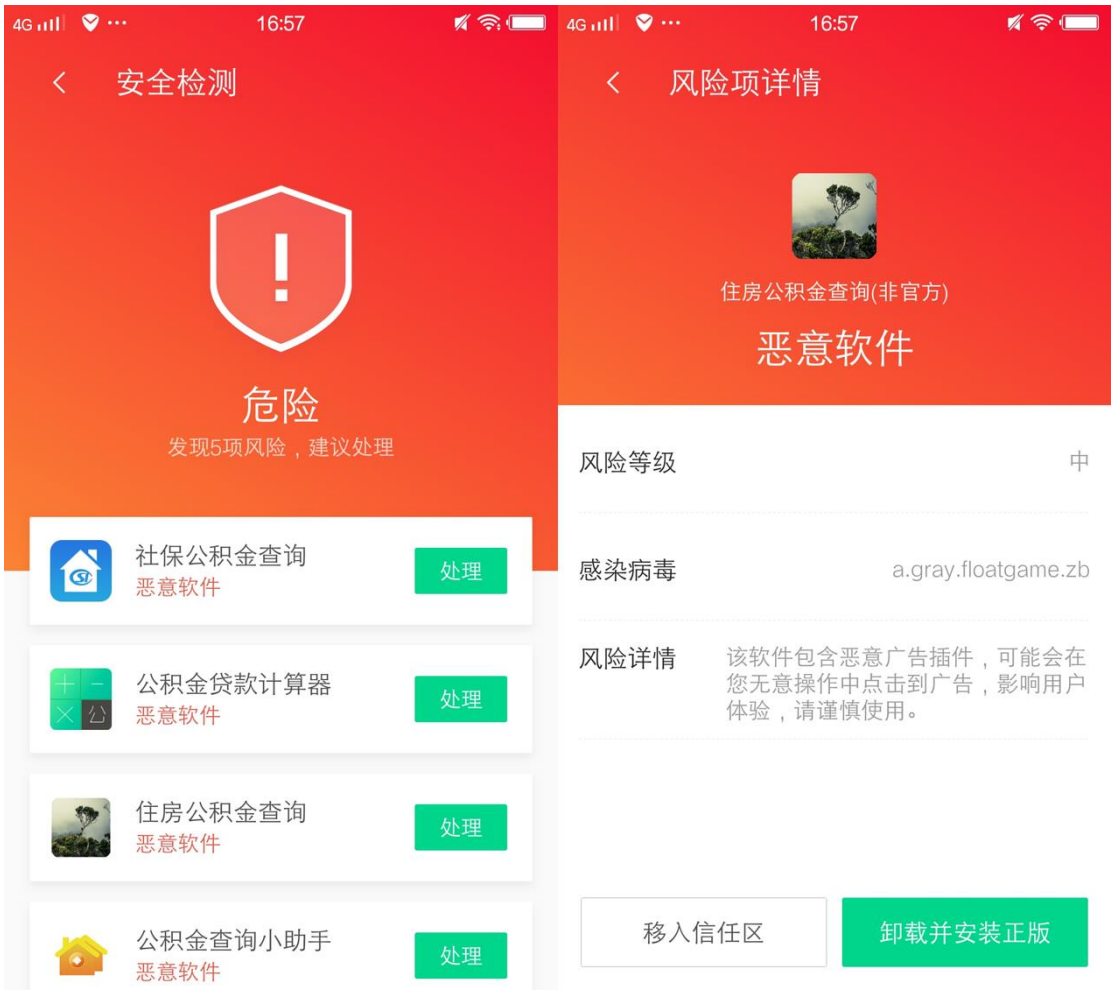
6 月前后是高考季，与高考先关的病毒软件也相当活跃。腾讯手机管家对“高考作文”“高考宝典”、“高考复习手册”、“高考倒计时”等多款与高考相关软件病毒 APP 进行了精准查杀。“高考作文”软件携带一种名为“a.gray.floatgame.o”的病毒，用户在下载安装后会启动恶意广告插件，在用户手机屏幕上匿名弹窗，影响手机正常使用。



2019 年 5 月，国家互联网应急中心通过自主监测和样本交换形式，发现 66 款窃取个人信息恶意程序，通过短信进行传播，私自窃取用户短信和通讯录，对用户信息安全造成严重安全威胁。根据腾讯手机管家病毒查杀记录显示，“招标文件”软件包含名为“a.privacy.emial.d”病毒，该病毒启动后会拦截用户短信，并将短信转发给指定号码，泄漏用户短信中的账户或密码，可能给用户的手机安全造成一定的威胁。

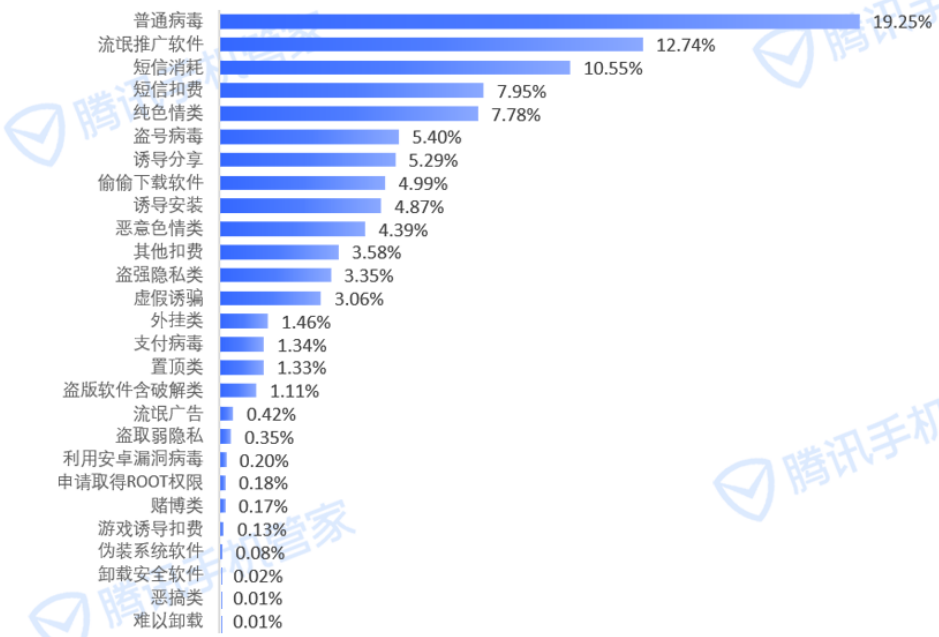


腾讯手机管家对“端午节大礼包”、“端午节龙舟视频 APP”、“端午节快乐”、“端午节祝福特别版”等 5 款病毒软件进行了精准查杀。“端午大礼包”是一款恶意软件，含有名为“a.fraud.lockpin”的病毒，该病毒在安装后会修改用户手机 pin 密码，强制锁屏，用户需要根据提示支付一定金额才能够解锁手机，存在流氓行为，看似是恶作剧，实则是强制用户付费，侵犯了用户的手机、财产安全。



6 月和 7 月前后，全国各地会调整住房公积金的缴存基数、缴存比例和月缴存限额，很多查询公积金的软件在网络上扩散，一些木马病毒 APP 也混杂其中，致使用户中招。腾讯手机管家依托腾讯自研 AI 反病毒引擎 TRP-AI 和自研杀毒引擎 TAV，对“公积金贷款计算器”、“住房公积金查询”、“公积金查询”、“社保公积金查询”以及“公积金查询小助手”等多款病毒软件实现精准查杀。其中，“住房公积金查询” APP 非官方版本，潜藏名为“a.gray.floatgame.zb”的木马病毒，其病毒行为在于流氓推广，通过恶意广告插件，让用户无意操作中点击到广告，进而影响使用体验。

2019年上半年手机病毒细分类型占比



2019年上半年手机安全报告　　数据来源：腾讯手机管家

从细分类型来看，流氓推广软件（12.74%）、短信消耗（10.55%）、短信扣费（7.95%）、纯色情（7.78%）和盗号病毒（5.40%）等等，依然是手机病毒常见的类型。

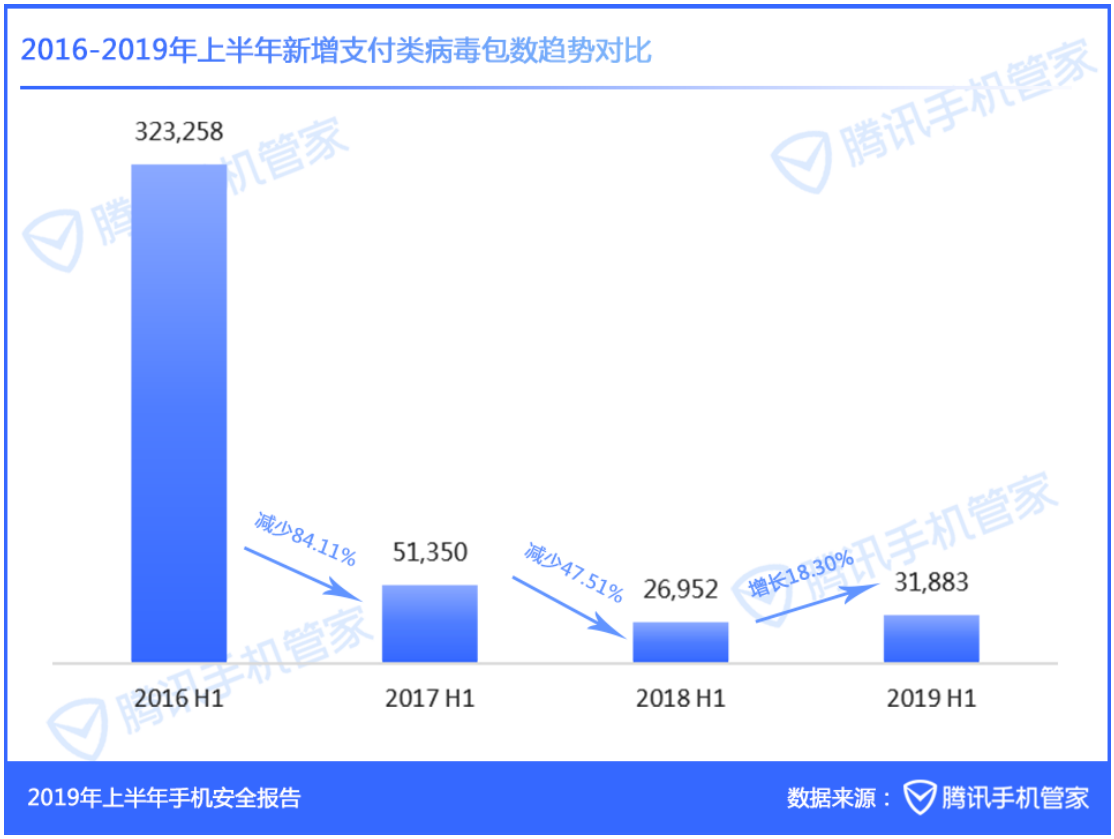
流氓推广软件作为一条成熟的黑色产业链，因其数量惊人已经成为黑色暴利产业，在腾讯手机管家查杀的众多病毒中，很多都属于此类型，也是用户最常见和饱受困扰的病毒类型之一。一些渠道代理商通过恶意软件联网自动下载、强行刷机内置的流氓推广的方式来强推应用，然后根据安装量领取相应的报酬结算分成，从中牟利。

扣费类病毒以游戏类手机应用为主，私自扣费、推送广告弹窗，对用户的手机使用造成了严重的威胁。常见的恶意扣费形式主要分为明扣和暗扣两种，与明扣相比，暗扣的方式更为隐蔽，用户难以察觉，并且主要通过三种形式进行：其一，软件后台私自向固定号码发送扣费短信；其二，后台私自上传用户的手机号码等信息到服务器，获取指定短信内容后，发送订阅短信订购收费业务；其三，拦截或屏蔽运营商的回执短信，自动回复并确认订购短信，随后删除该订阅信息。

纯色情类病毒往往藏匿于用户浏览的网页、视频中，通过诱导、伪装的方式，吸引用户点击下载安装。

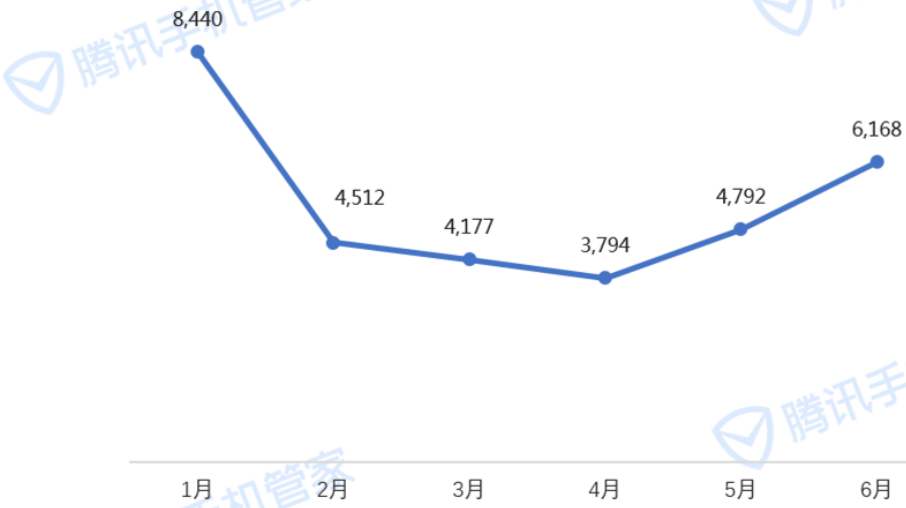
此外，诱导分享、偷偷下载软件、诱导安装等也是常见的病毒风险类型，破坏用户的手机使用体验，威胁用户的信息安全与财产安全。

1.5 2019 年上半年手机支付类病毒新增 3.19 万个



2019 年上半年支付类病毒包新增 3.19 万个，占新增病毒包总数的 1.68%，与去年同期相比增长了 18.30%。移动支付广泛应用于日常生活，移动支付的安全问题日益重要，而金融移动 APP 安全是用户账户、资金安全的基础。央行 146 号文《关于开展支付安全风险专项排查工作的通知》，要求金融机构支付 APP 进行全面检测与排查，排查内容包括移动客户端应用软件的敏感信息保护、安全漏洞防护、信息传输安全等方面存在的隐患。

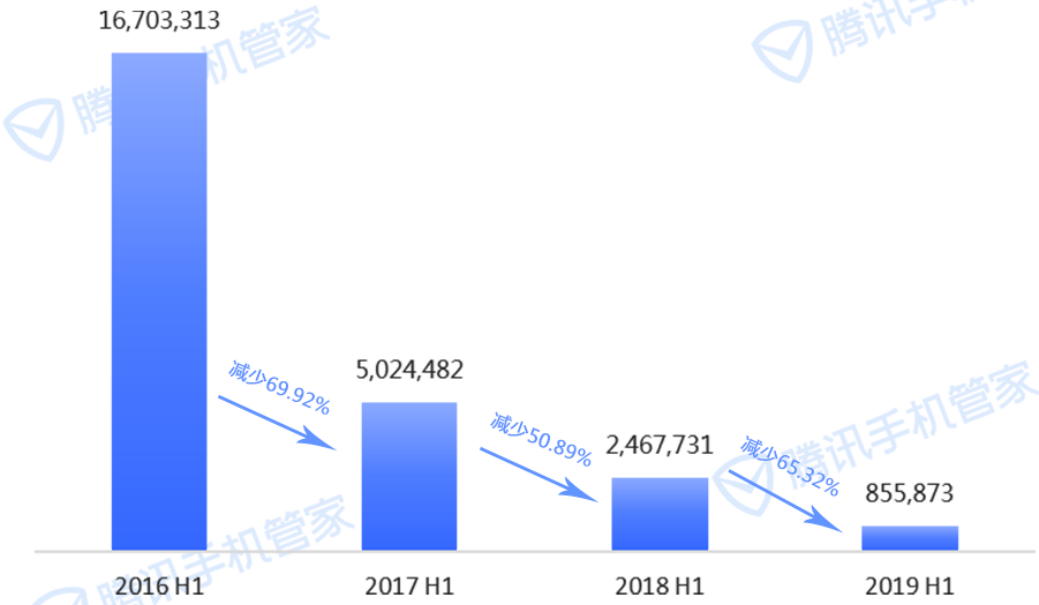
2019年上半年新增支付类病毒包数变化趋势



2019年上半年手机安全报告 数据来源：腾讯手机管家

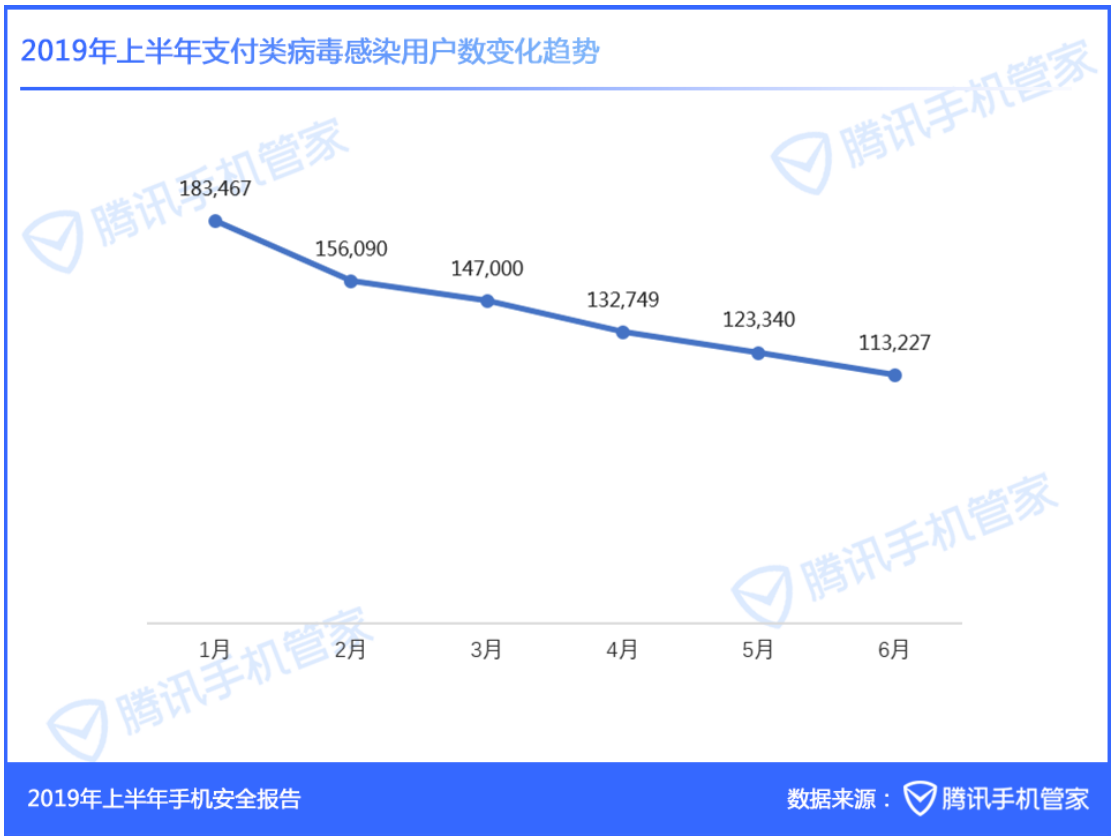
2019 年上半年，1 月份新增支付类病毒包最多，8840 个，2 月、3 月和 4 月逐月下降，5 月和 6 月又回升至 6168 个。

2016-2019年上半年支付类病毒感染用户数趋势对比

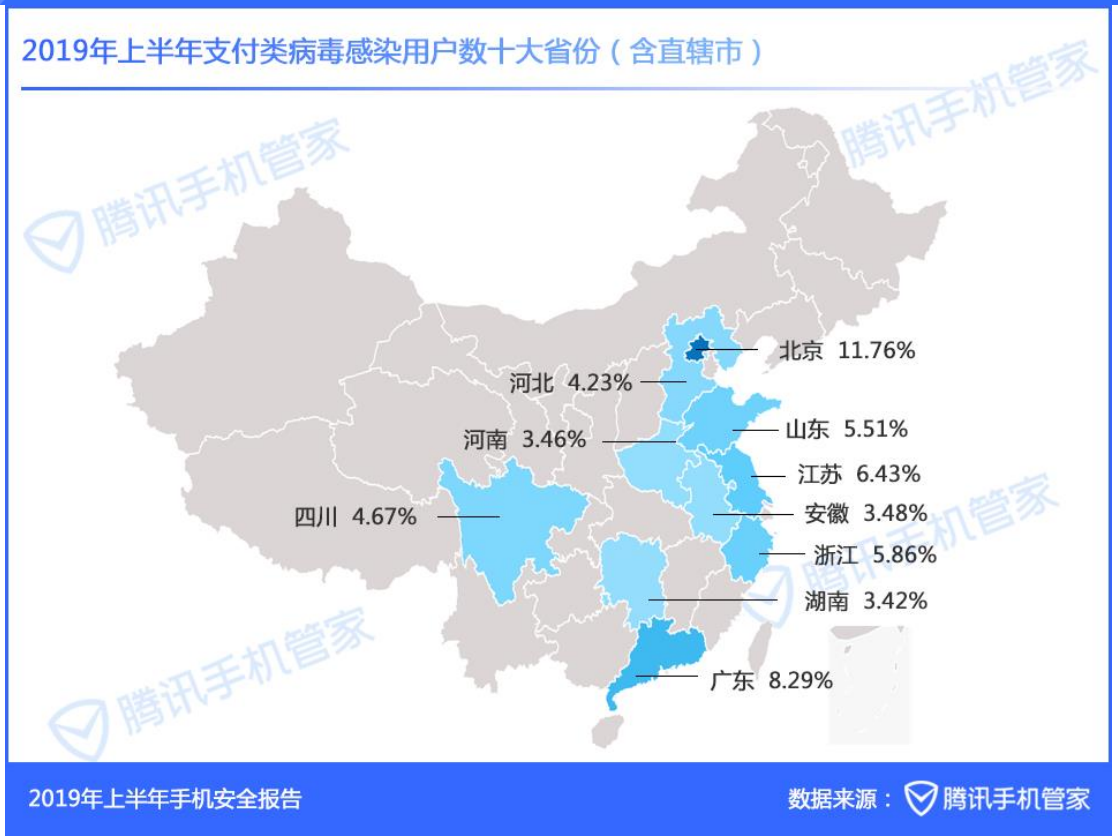


2019年上半年手机安全报告 数据来源：腾讯手机管家

根据腾讯手机管家数据显示，2019 年上半年支付类病毒感染用户近 85.59 万，较去年同期减少 65.32%，占手机病毒感染总人数的 2.24%。

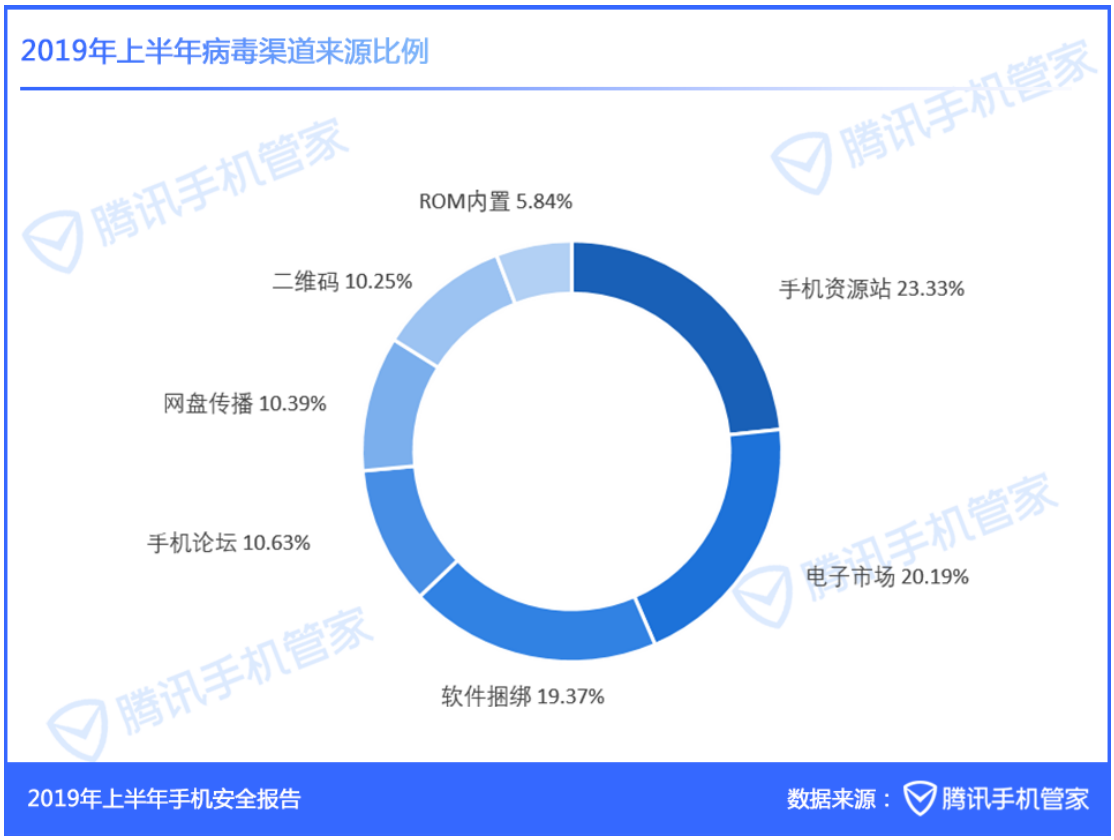


2019 年上半年支付类病毒感染情况呈现好转趋势，1 月份感染人数最多，近 18.35 万，随后逐月降低。



支付类病毒感染地区严重的地区多为经济大省或人口大省，其中最严重的省份是北京、广东和江苏，占比分别是 11.76%、8.29%和 6.43%。

1.6 2019 年上半年安卓手机病毒渠道来源持续多样化



手机病毒包传播渠道多样化，常见的手机病毒传播七大渠道有手机资源站、电子市场、软件捆绑、二维码、网盘传播、ROM 内置和手机论坛。

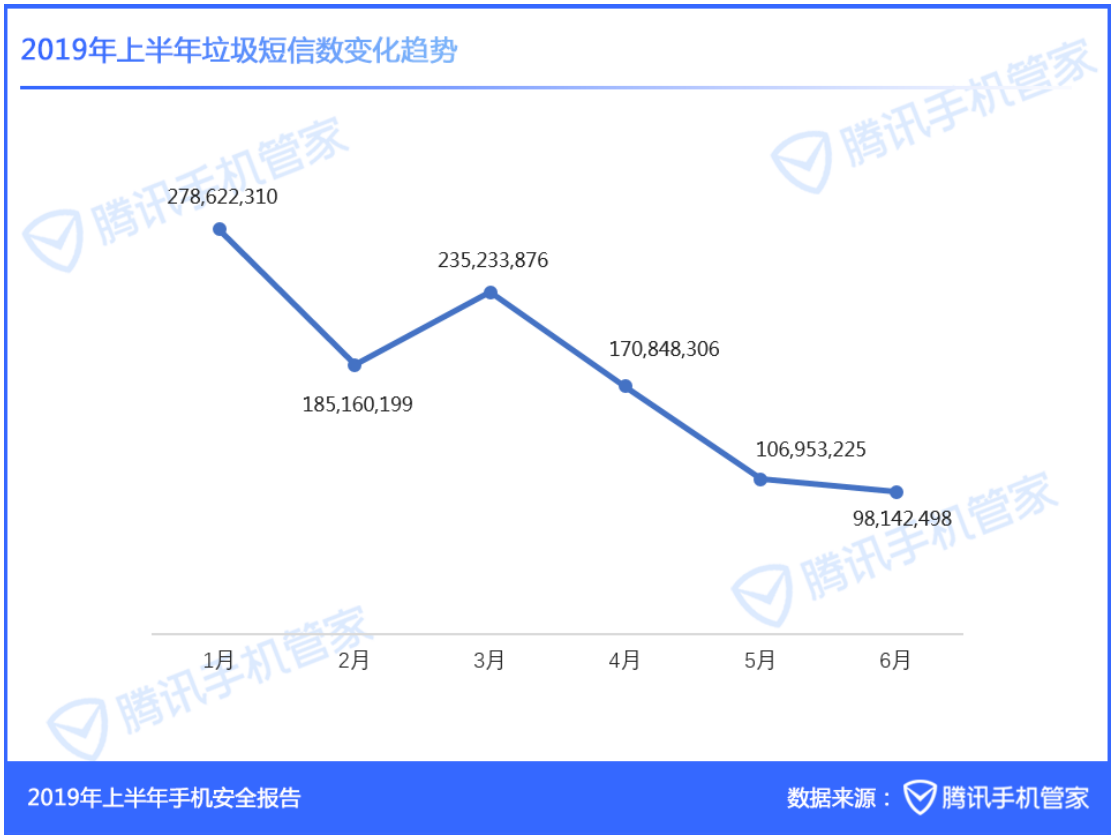
目前手机资源站仍有很多尚未建立完善的安全审查机制，恶意程序监管鉴别机制缺失，是病毒传播的主要渠道之一，占比 23.33%。

20.19%病毒包通过电子市场传播。应用商店落实 APP 运营者真实身份信息验证、应用程序安全检测、违法违规 APP 下架等责任，切实规范用户个人信息的收集使用行为。

软件捆绑传播病毒的方式排名第一，占比 19.37%。不法分子常在游戏类、工具类应用植入恶意代码、二次打包篡改软件版本，伪装成正常软件，用户将其安装到手机后，私自下载安装其他恶意软件，给用户造成资费消耗、隐私泄露等后果。

第二章 2019 年上半年垃圾短信现状分析

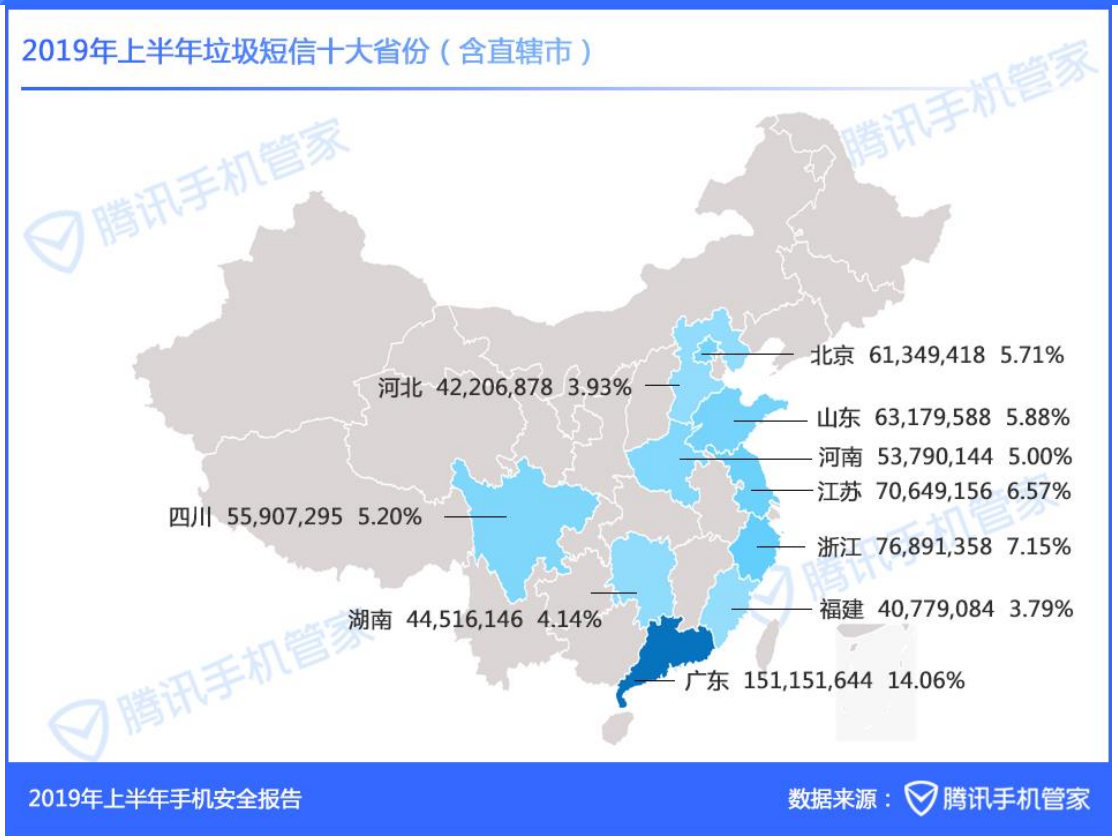
2.1 2019 年上半年用户举报垃圾短信近 10.75 亿



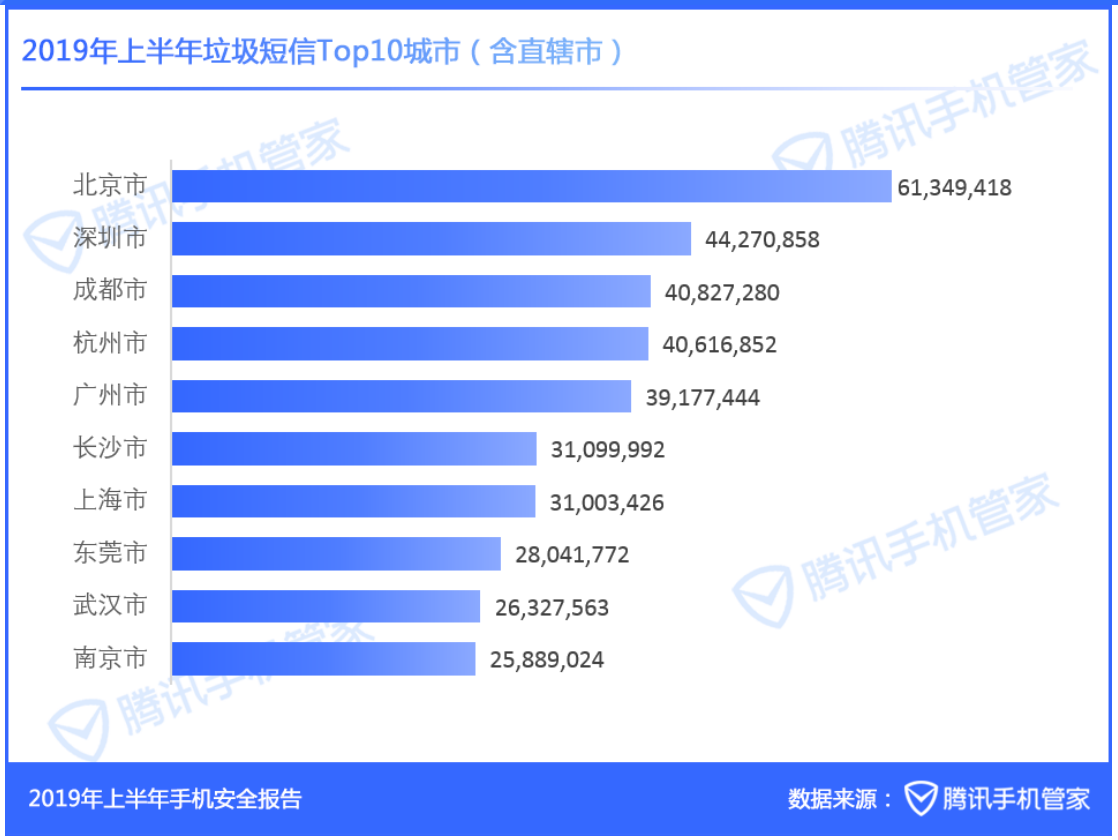
根据腾讯移动安全实验室数据显示，2019 年上半年腾讯手机管家用户举报垃圾短信近 10.75 亿条，其中 1 月份举报最多，近 2.79 亿条，随后基本逐月下降，6 月份举报 9814.25 条。

随着有关部门对垃圾短信监管力度不断加大，手机号码实名制认证举措不断推进，从源头打击了垃圾短信的进一步扩张，垃圾短信泛滥的问题有所好转。

工信部对于违规发送垃圾短信的手机号码运营商将采取停机(停止通信服务)、列入垃圾短信黑名单(不能发短信)、停短信功能(不能收发短信)等处置方式，对于违规发送垃圾短信的端口，将关闭端口、为用户屏蔽或业务整改等。

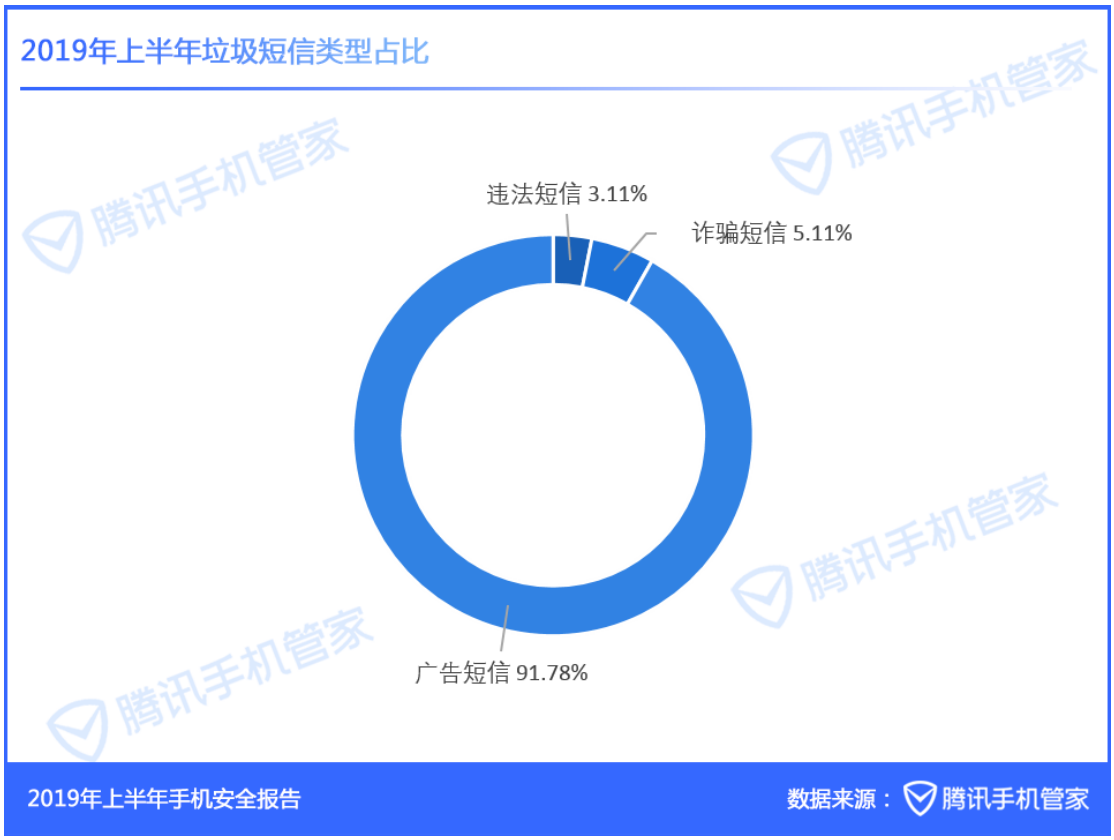


从地域分布上看，垃圾短信举报量最大的前十个省份， 分别为广东（14.06%）、浙江（7.15%）、江苏（6.57%）、山东（5.88%）和北京（5.71%）等。61%被举报的垃圾短信都集中在这十大省份里。



北京和深圳的垃圾短信最多，分别为 6134.94 万和 4427.09 万。成都、杭州、广州和长沙等经济发达、人口众多的城市也是垃圾短信的泛滥区。

2.2 2019 年上半年垃圾短信类型：广告类占比 92%

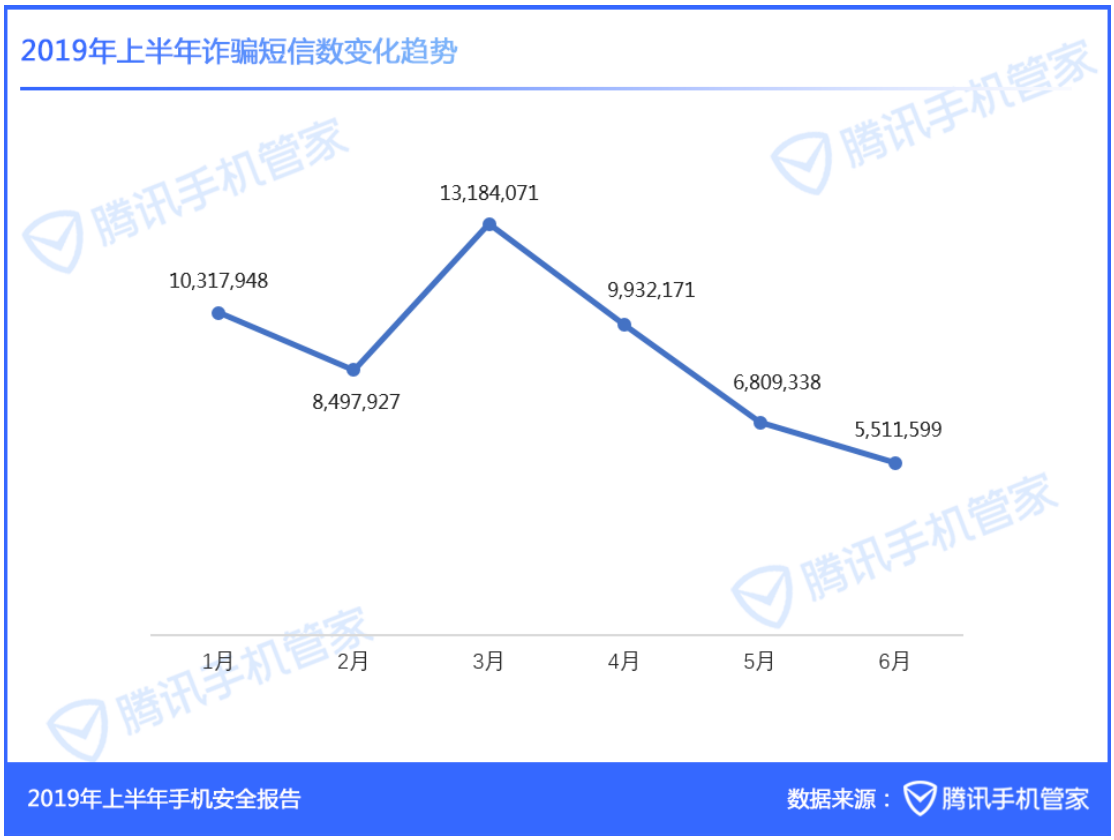


从 2019 年上半年垃圾短信的类型的占比可以看出，广告短信是垃圾短信最主要的组成部分，占比 91.78%，广告推销仍是垃圾短信的主要传播目的。

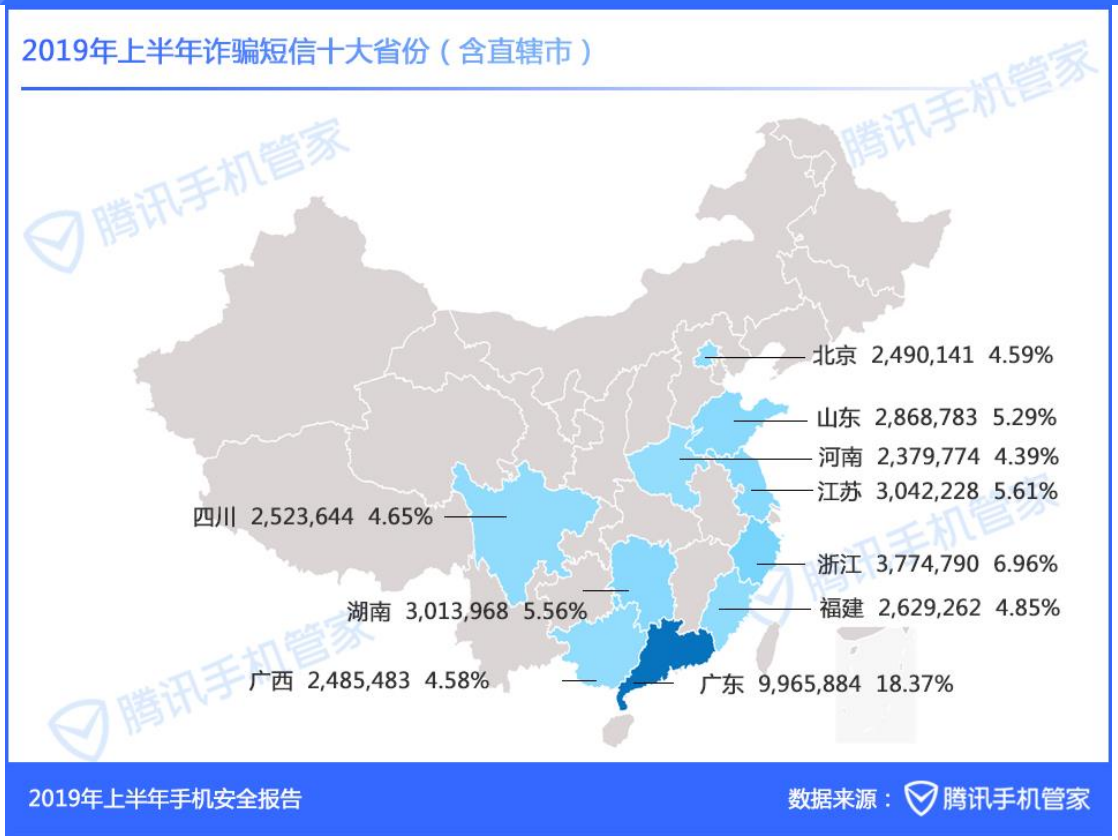
根据法规，未经用户同意或者请求，广告主不得向其发送商业性短信息，但在巨大的利益链条的推动下，广告主不断升级技术，钻空子，以应对运营商及安全防护软件的拦截。

诈骗短信占比分别为 5.11%，其类型多样，以非法贷款、高薪招聘和病毒软件、恶意网址为主。违法短信占比 3.11%，主要是假证件、发票买卖、色情广告和枪支弹药等违法违规的内容。

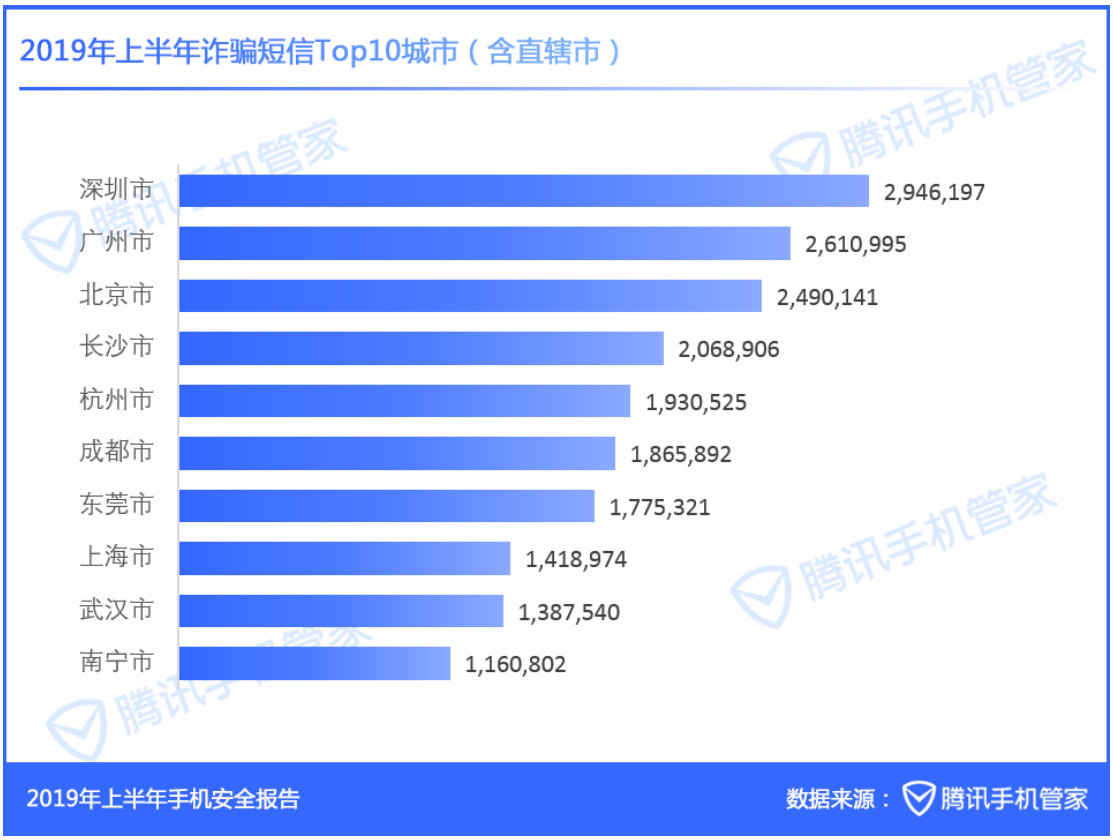
2.3 2019 年上半年用户举报诈骗短信近 5425.31 万条



2019 年上半年，腾讯手机管家收到用户举报诈骗短信近 5425.31 万条，平均每月举报 904.22 万条。3 月份举报量最大，近 1318.41 万条。

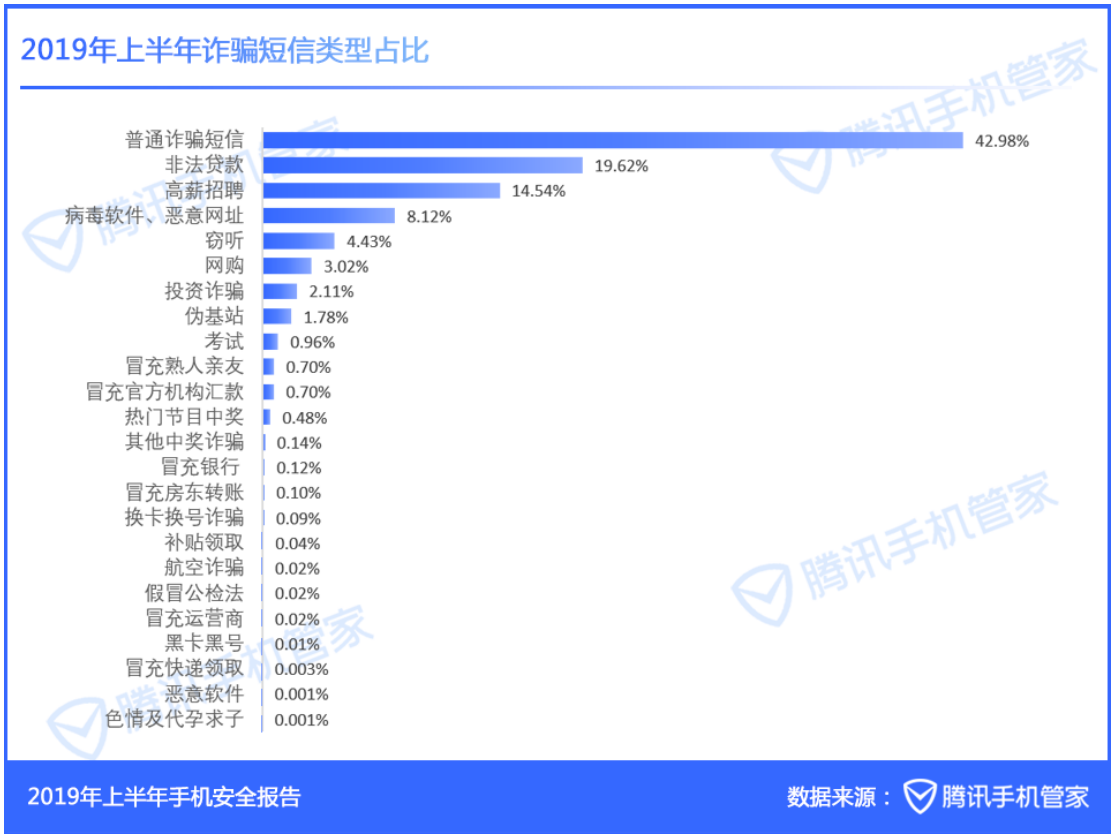


广东的诈骗短信举报最多 近 996.59 万条 ,占比 18.37%。浙江（ 6.96% ）、江苏（ 5.61% ）、湖南（ 5.56% ）和山东（ 5.29% ）等省，诈骗短信的举报量在全国范围内也比较高。



具体到城市，用户举报诈骗短信数最多的城市是深圳、广州和北京，占比分别为 5.43%、4.81%和 4.59%。长沙、杭州、成都和东莞等也是诈骗短信重灾区。

2.4 2019 年上半年常见的诈骗短信类型



根据腾讯手机管家的数据显示，2019 年上半年最常见的诈骗短信类型多样，多达二十几种，其中案发量大且较有欺骗性的当属非法贷款、高薪招聘和病毒软件&恶意网址这三类。

从上图可以看出，非法贷款类短信占比达 19.62%。不法分子先通过短信触达受害人，以收取“保证金、好处费、保险费、解冻费”等费用为由，先榨取其第一笔钱款，然后利用受害人不愿放弃沉没成本的心理，继续要求缴纳各种费用。为增强说服力，诈骗分子会借助图片，将事先伪造好的清除贷款记录、现金支票、银行交易流水图片发给受害人。

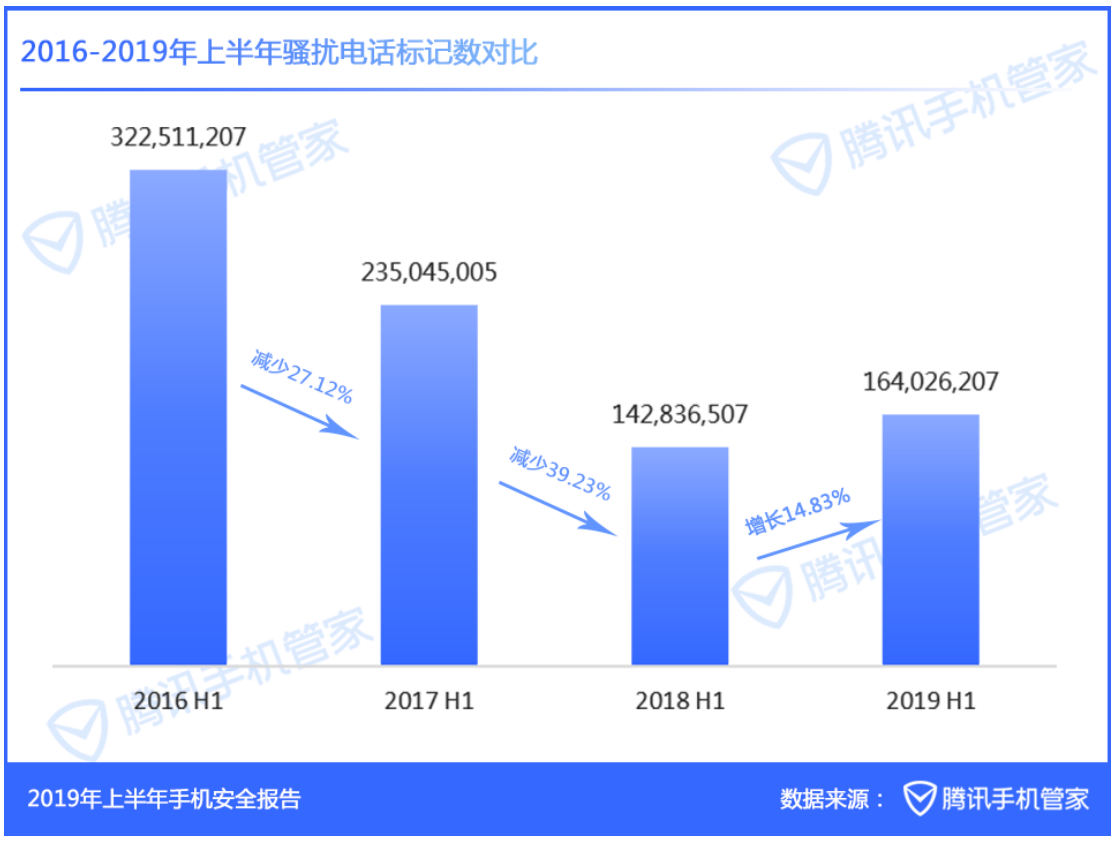
金三银四加上毕业季，上半年正好处于招聘找工作的高峰期，与招聘相关的诈骗短信占比 14.54%。不法分子以高薪或工作简单轻松等吸引用户联系所谓的“客服人员”，然后以交纳保证金、会员费、充值等为由要求用户转账，甚至“招转培”，诱导受害人在贷款软件

上办理贷款，支付培训费用。

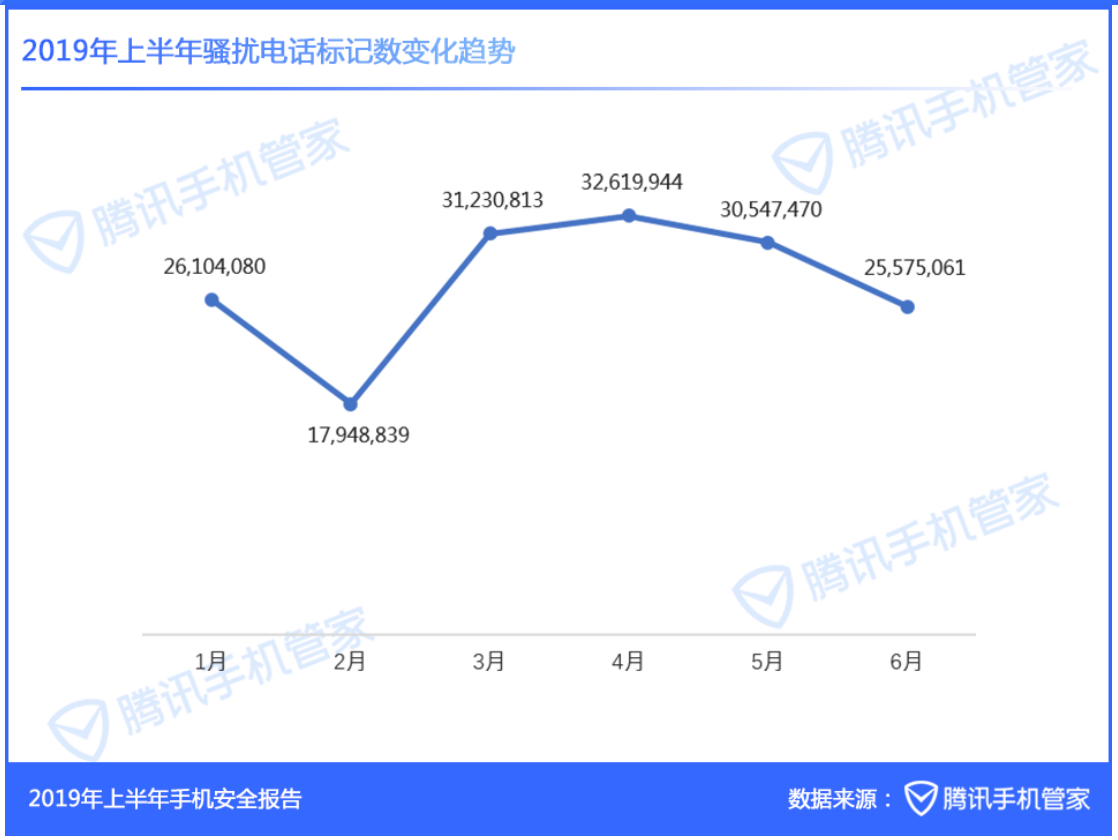
数量大且危害性强的诈骗短信还有病毒软件&恶意网址类，占比 8.12%。近年来木马病毒单独作案的几率降低，多通过诈骗短信联合作案，其危害性和隐蔽性大大增强，网上打着破解、盗号名义的软件多为不规范应用，潜藏病毒的可能性更高。

第三章 2019 年上半年骚扰电话现状分析

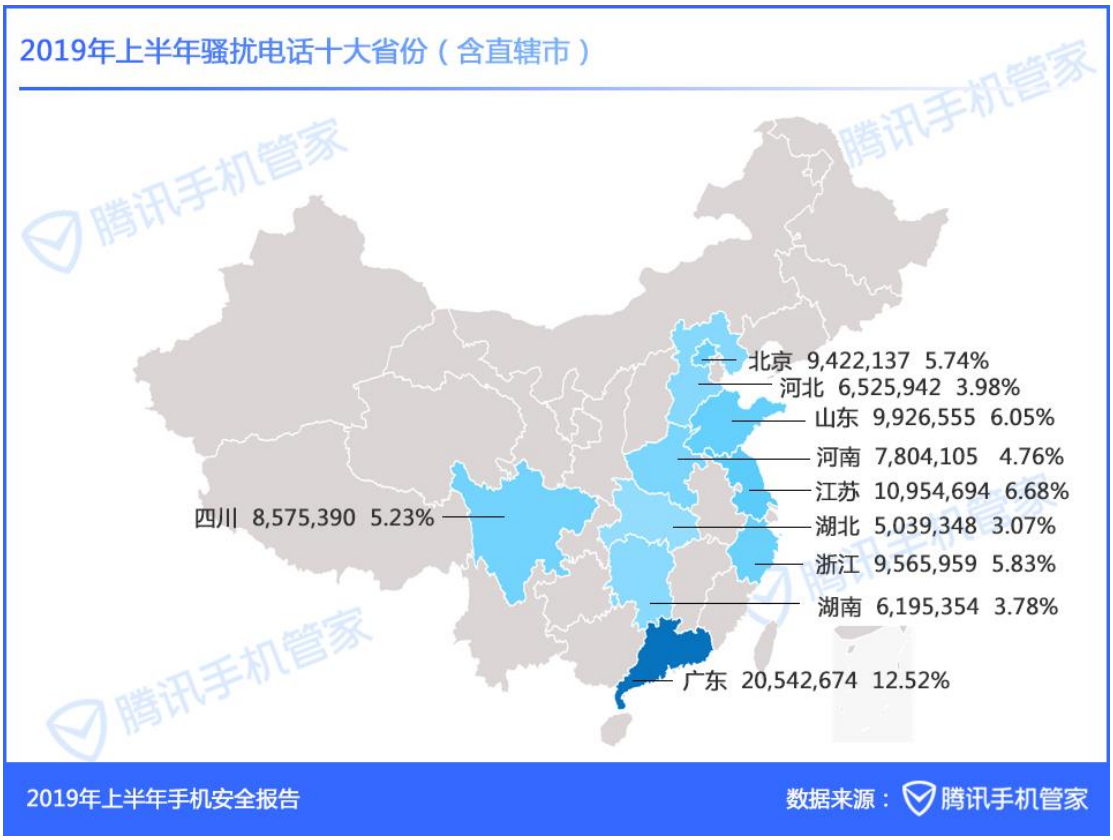
3.1 2019 年上半年骚扰电话标记数达 1.64 亿个



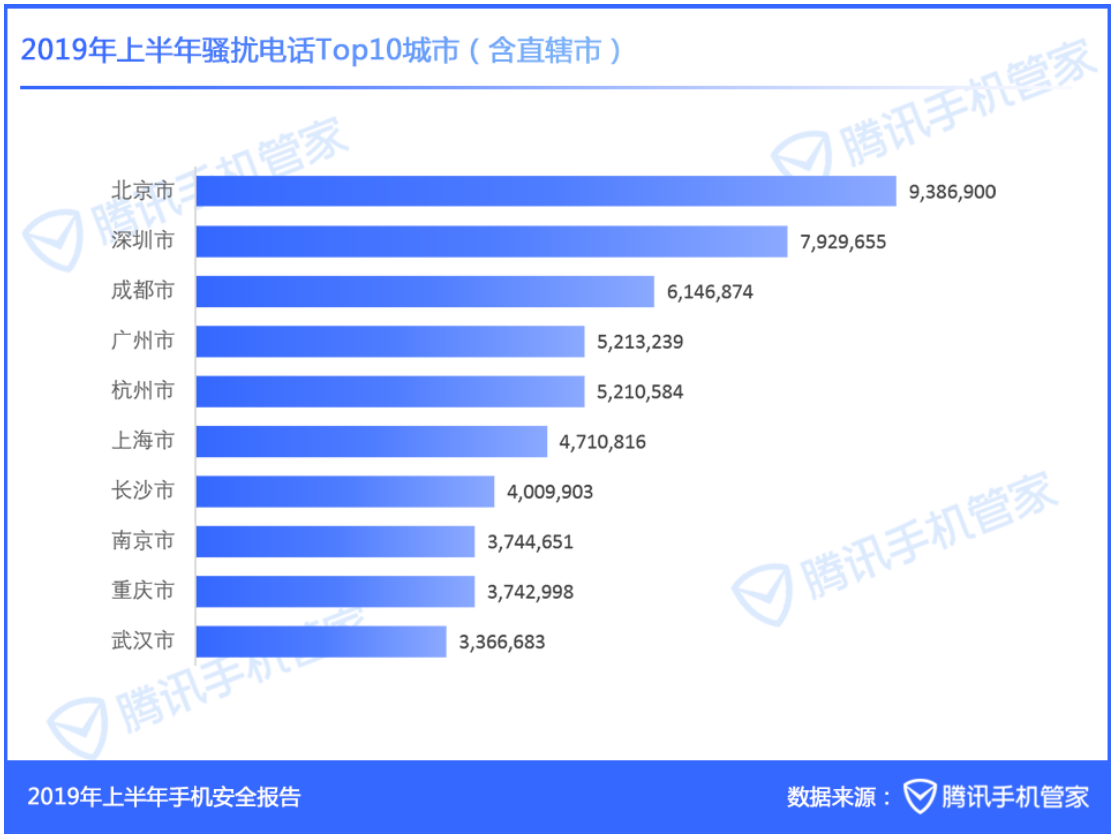
根据腾讯移动安全实验室数据显示，2019 年上半年腾讯手机管家用户共标记骚扰电话达 1.64 亿个。随着人工智能技术的快速发展，AI 电话机器人被应用于在金融、地产、教育等多个领域，在有关部门大力整治的形势下，骚扰电话仍较去年同时期增长 14.83%。



2019 年上半年，腾讯手机管家用户平均每天标记骚扰电话 2733.77 万个，4 月份标记最多，达 3261.99 万个。

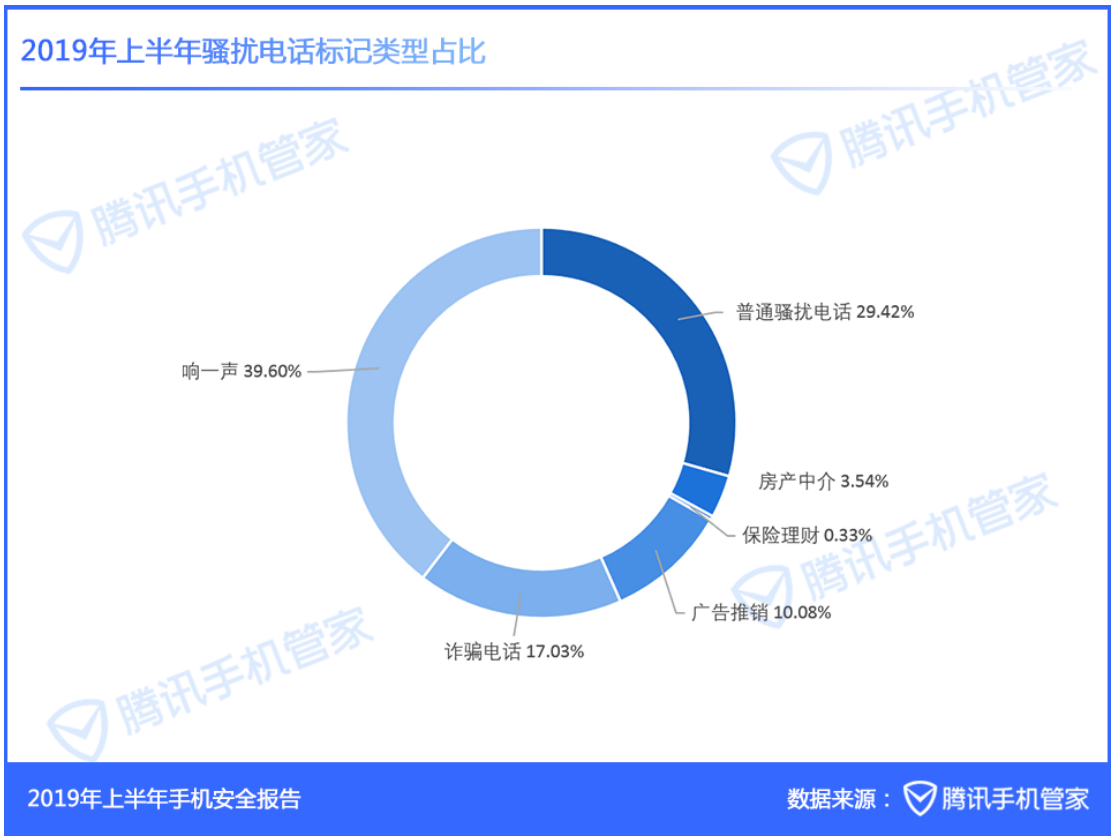


广东、江苏和山东是骚扰电话标记数最多的三个省份，分别为 2054.27 万（12.52%）、1095.47 万（6.68%）和 992.66 万（6.05%），其次是浙江、北京、四川、河南、河北、湖南和湖北。



城市方面，北上广深和部分新一线城市如杭州、长沙、南京和重庆等，骚扰电话标记量最高，其中北京、深圳和成都的标记量排名前第三。骚扰电话举报量 Top10 的城市，用户一共举报了 5346.23 万个骚扰电话。

3.2 2019 年上半年骚扰电话类型



2019 年上半年，骚扰电话主要分为以下类型：响一声（39.60%）、普通骚扰电话（29.42%）、诈骗电话（17.03%）、广告推销（10.08%）、房产中介（3.54%）和保险理财（0.33%）。

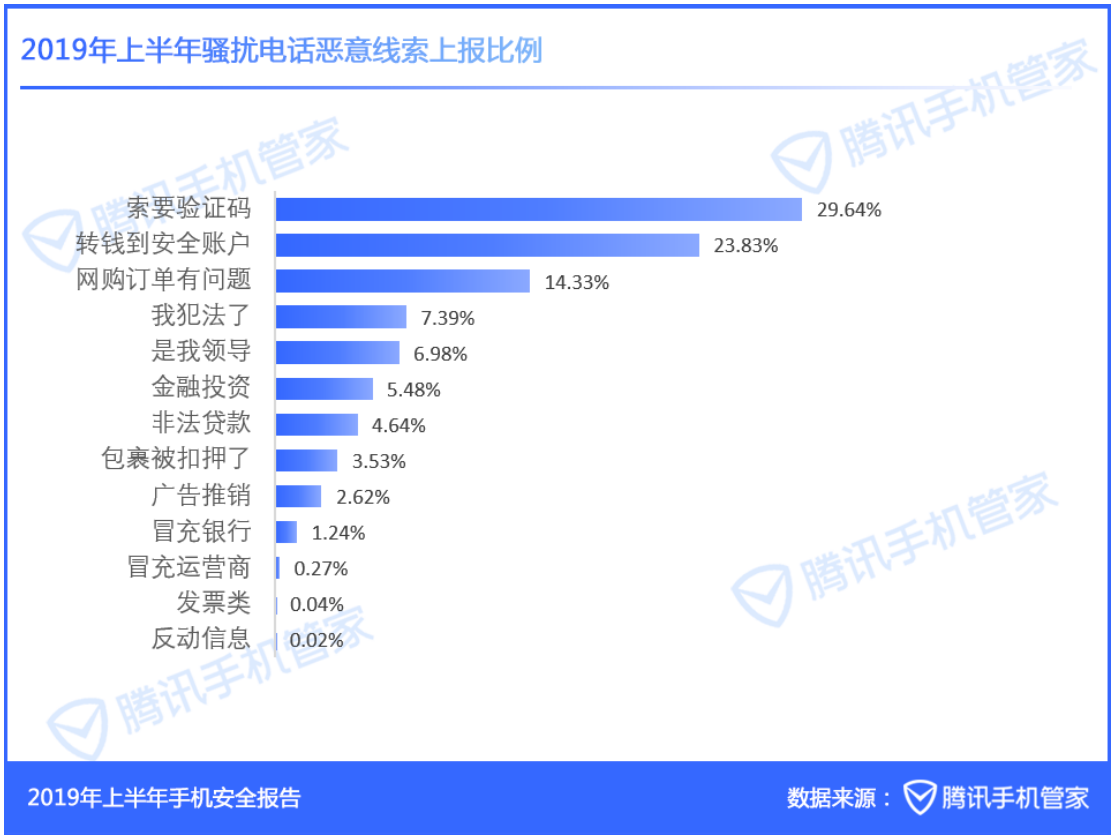
占比最高，用户深恶痛觉的“响一声”电话，运营商方面加强了监测管理。中国移动在全国范围内建立了骚扰电话集中监测系统，针对“响一声”“语音群呼”“呼死你”等骚扰电话集中监测，主动发现且核实后将实施号码关停或加入呼叫黑名单等处理。

从 2018 年 7 月开始，工信部等十三部门联合整治骚扰电话，重点对商业营销类、恶意骚扰类和违法犯罪类骚扰电话进行整治，并多次约谈运营商，表明了治理骚扰电话的态度与决心。今年，三大运营商整治骚扰电话也纷纷出新招：推出“防骚扰电话神器”，采用云端拦截技术等。

但是，各类骚扰电话在各方利益的驱动下，已经形成产业链条，借助高科技手段推广实

施。“95”、“400”、“800”开头的电话是骚扰电话的重灾区，据悉，“95”号码的语音机器人，一天能拨打 800 至 1000 个电话。很多企业或个人常常利用这些电话来推销。

针对骚扰电话整治领域出现的新问题，当前的法律法规和治理手段尚未同步更新，AI 电话机器人的生产、购买和使用等环节的监管有待进一步规范。



根据腾讯手机管家用户主动上报的恶意线索数据显示，2019 年上半年常见的骚扰电话恶意线索关键词是索要验证码、转账到安全账户、网络订单有问题和我犯法了等，不仅常见，并且受害人数众多。

提供验证码可以解冻账户、提供验证码可以开通超出流量叠加套餐、提供验证码可提升信用卡额度……验证码作为身份验证的最后一道防线，是骗子实施诈骗行为成功与否的关键，骗子以各种理由索要验证码，导致索要验证码类的恶意线索关键词占比高达 29.64%。

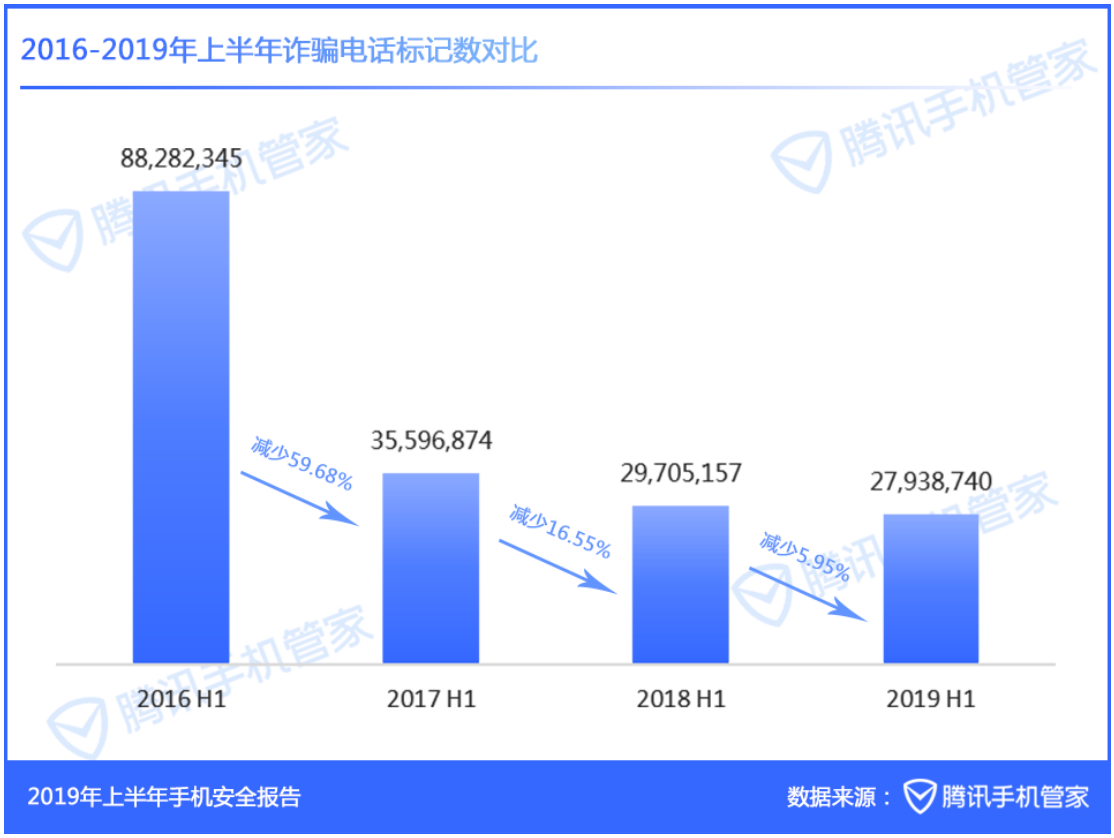
转账到安全账户类恶意线索关键词占比 23.83%，骗子假冒公安、检察院或者法官等，以电话卡发送异常信息、快递包裹有问题等各种违法行为为由，要求受害人提供账户核查资

金或将资金转入“安全账户”。此类诈骗电话多以中老年人为主要目标，但近来上当受骗的群体逐渐年轻化。

“网购订单有问题”恶意线索举报量占比 14.33%。在警方侦破的此类案件中，可以看到，犯罪团伙通过多种途径获取受害人的订单信息，实施诈骗：应聘客服，卧底在各大电商平台内的网店，然后植入恶意木马，盗取用户和订单信息；通过黑客技术攻击小型电商平台或快递公司网站。

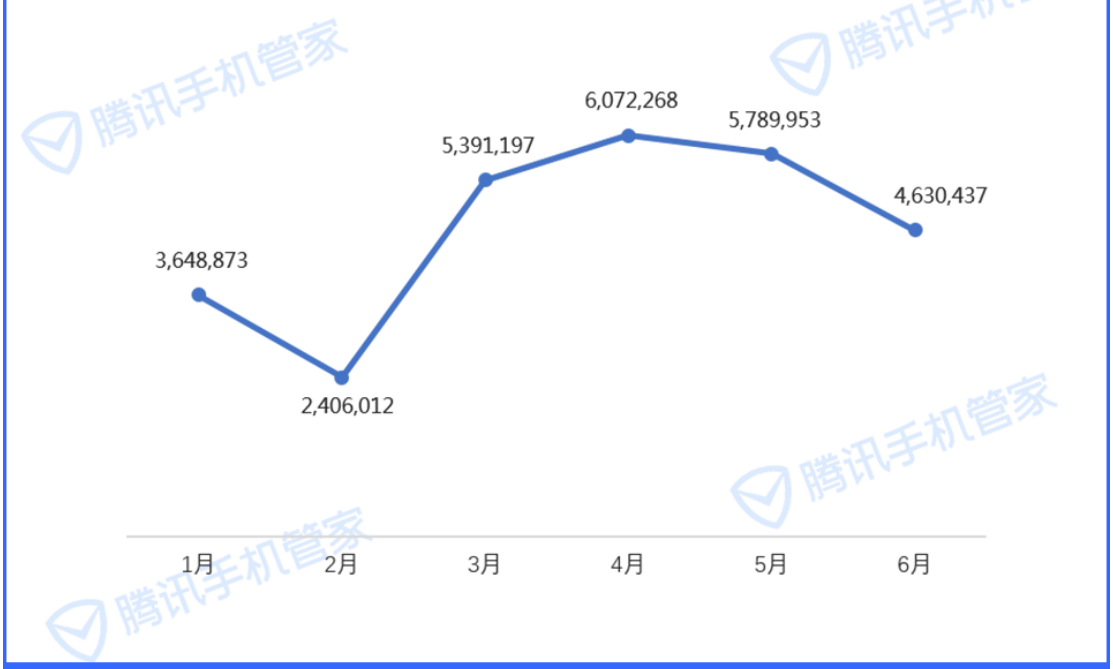
在电话诈骗中，不法分子在作案时常结合“改号软件”等新技术手段，不用出面接触受害人，只需躲在幕后远程操控即可，具有手段隐蔽、跨区域、流动性强等特点。

3.3 2019 年上半年用户标记诈骗电话达 2793.87 万个



基于腾讯手机管家用户标记诈骗电话的相关数据显示，2019 年上半年用户标记诈骗电话达 2793.87 万个，同比减少 5.95%。

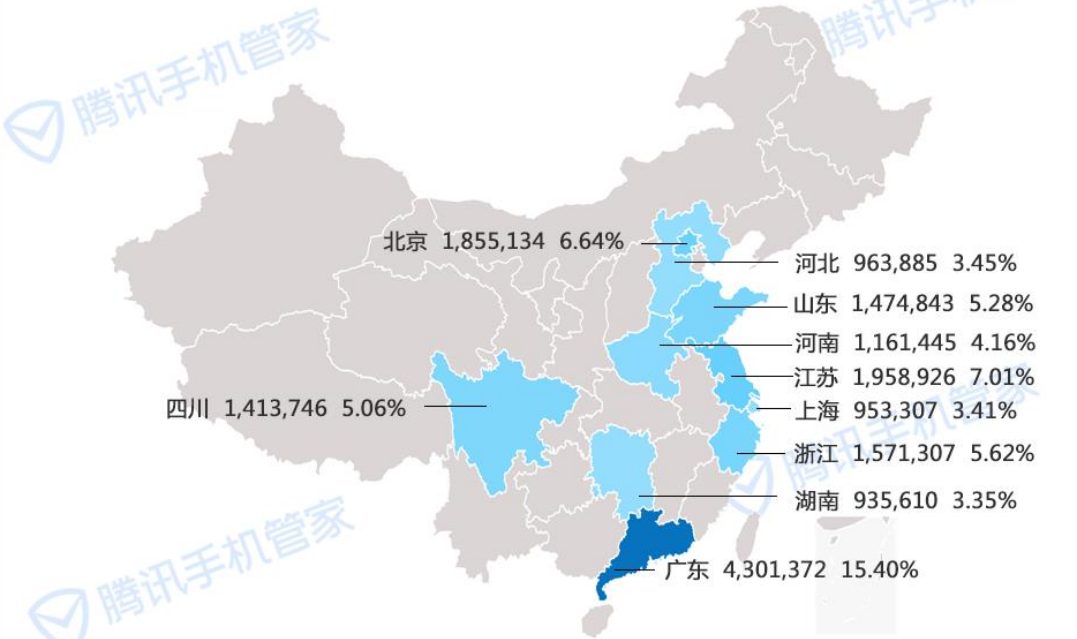
2019年上半年诈骗电话标记数变化趋势



2019年上半年手机安全报告　　数据来源：腾讯手机管家

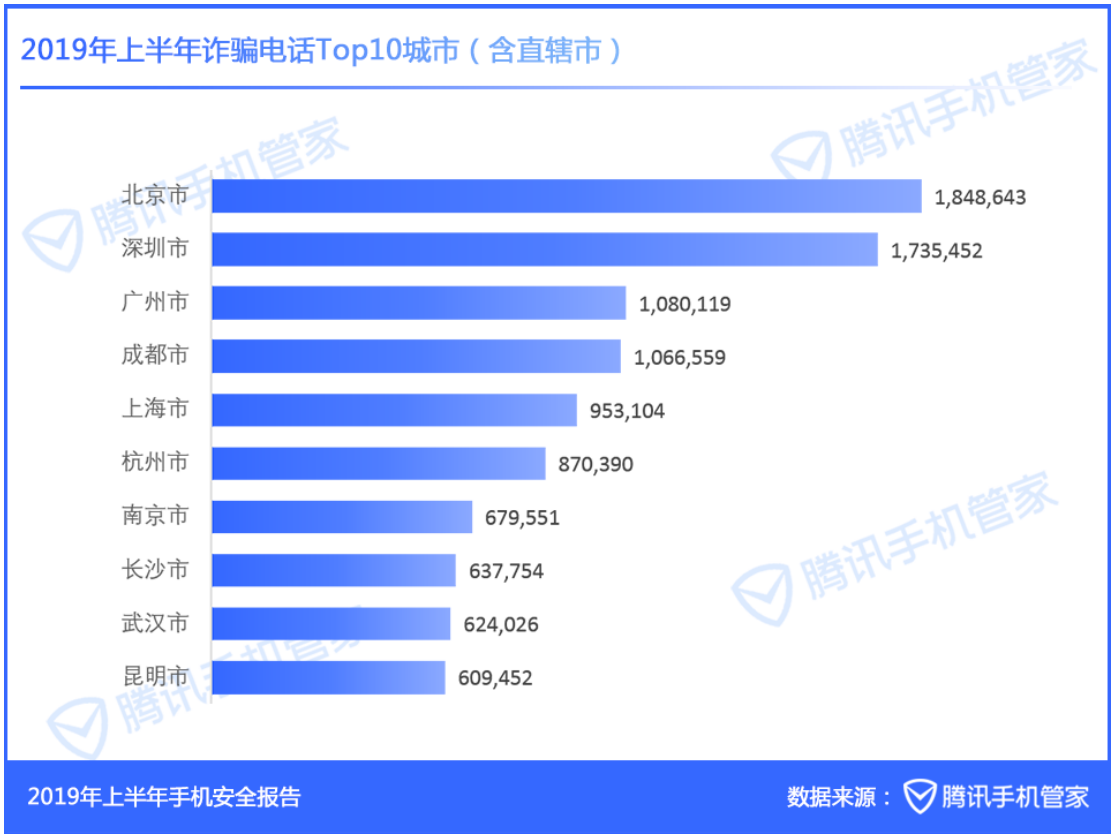
2019 年上半年，腾讯手机管家用户平均每月标记诈骗电话 465.65 万个，在 4 月份标记了近 607.23 万个诈骗电话，为上半年最高。

2019年上半年诈骗电话十大省份（含直辖市）



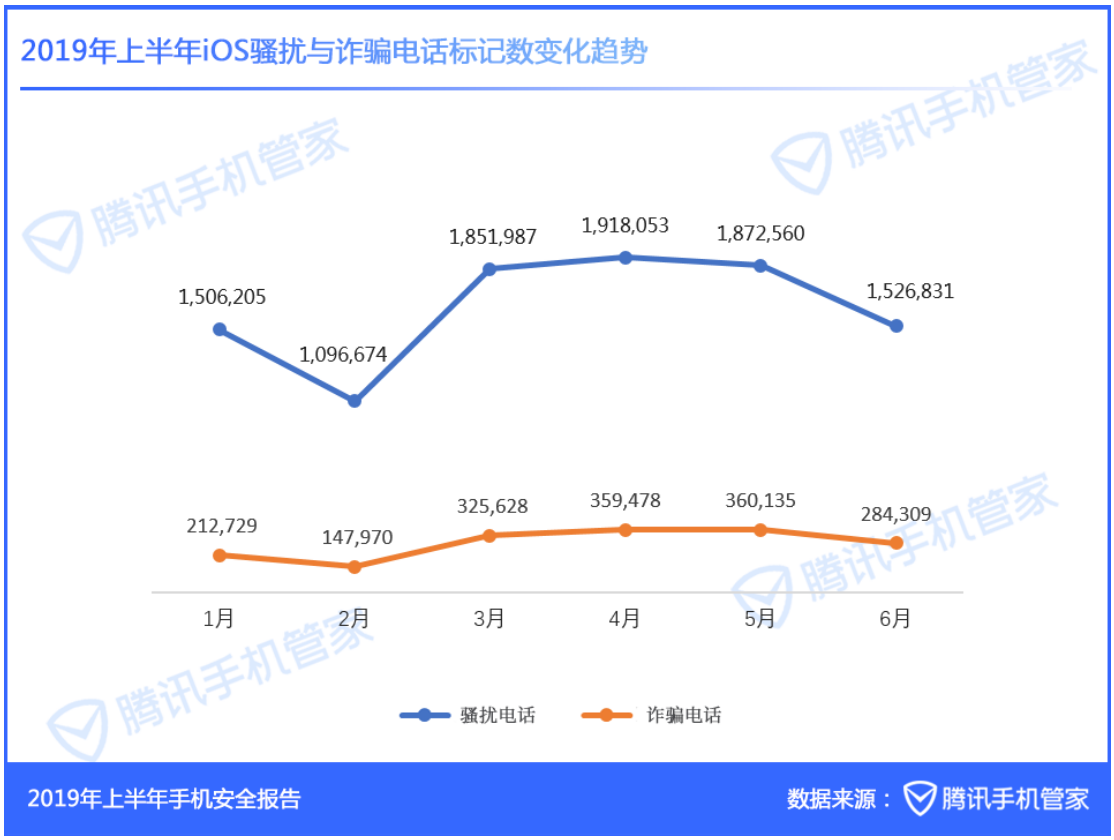
2019年上半年手机安全报告　　数据来源：腾讯手机管家

诈骗电话十大省份的地域分布与骚扰电话相类似，总数近 1658.96 万个，占诈骗电话总和的 59%，诈骗电话的分布总体比较集中。排名前三的省份是广东、江苏和北京，总数分别为 430.14 万（15.40%）、195.89 万（7.01%）和 185.51 万（6.64%）。浙江、山东、四川、河南、河北、上海和湖南电话诈骗情况也较为严重。



北上广深和部分新一线城市，不仅骚扰电话多，诈骗电话也多。骚扰电话标记数前十的城市，基本上诈骗电话也比较多。诈骗电话标记数排名十名的城市分别为北京、深圳、广州成都和上海等，总和达到 1010.51 万。

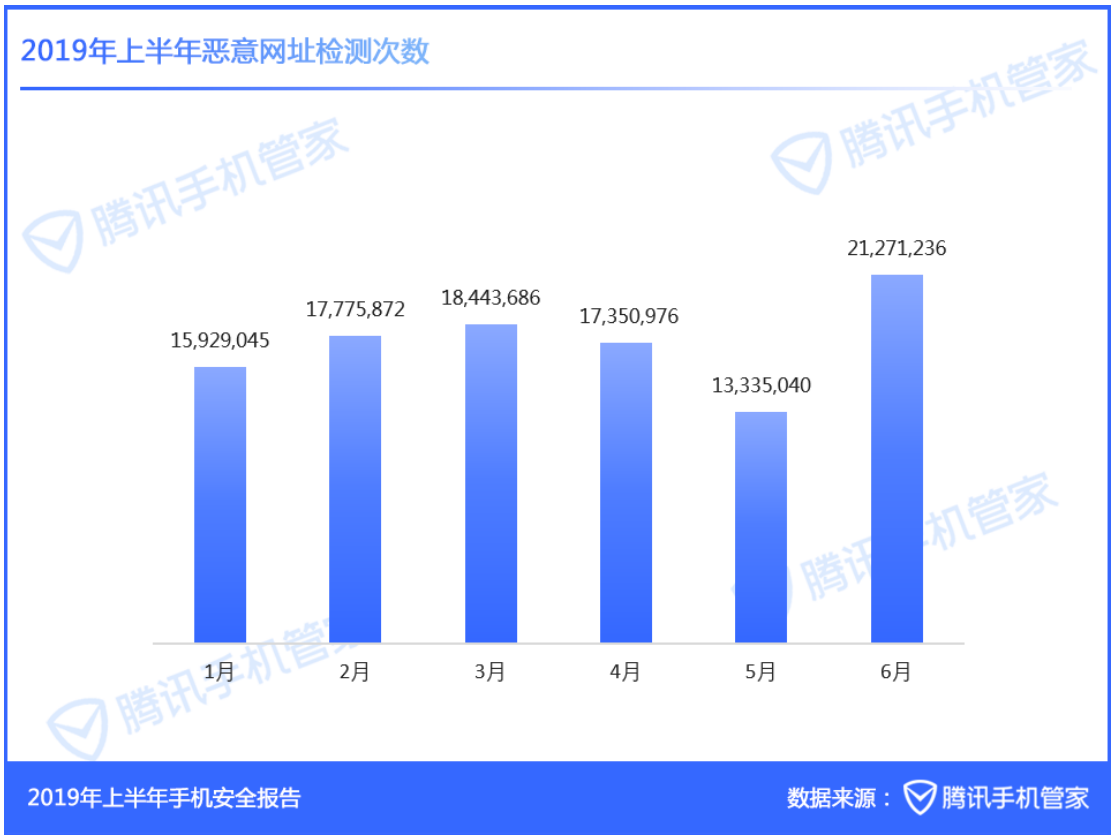
3.4 2019 年上半年 iOS 骚扰及诈骗电话现状



2019 年上半年，iOS 的骚扰电话、诈骗电话总标记数分别为 977.23 万和 169.02 万，高峰 4 月和 5 月。

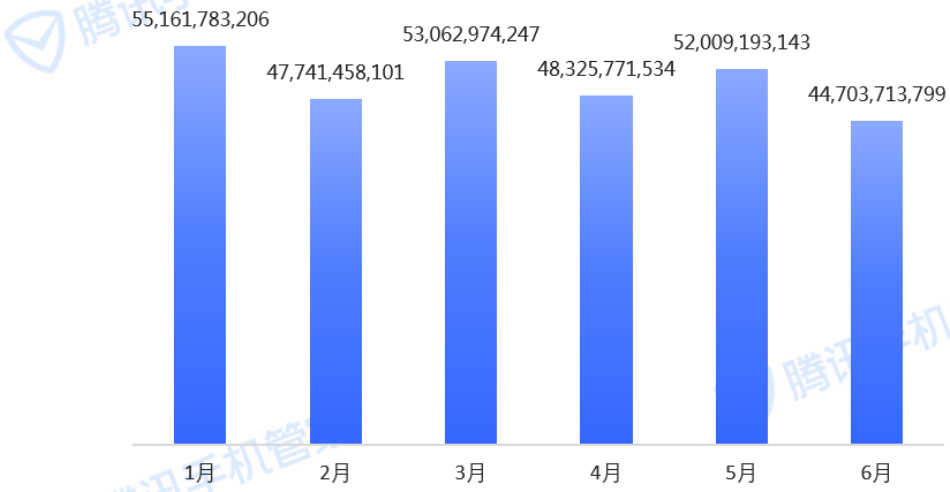
第四章 2019 年上半年恶意网址现状分析

4.1 2019 年上半年恶意网址拦截次数近 3010.05 亿次



2019 年上半年，腾讯安全实验室共计检测恶意网址 1.04 亿次，6 月份检测到的恶意网址最多，近 2127.12 万次。基于腾讯安全云智能过滤技术及千万级恶意网址特征，腾讯安全实验室精准过滤各类网址。

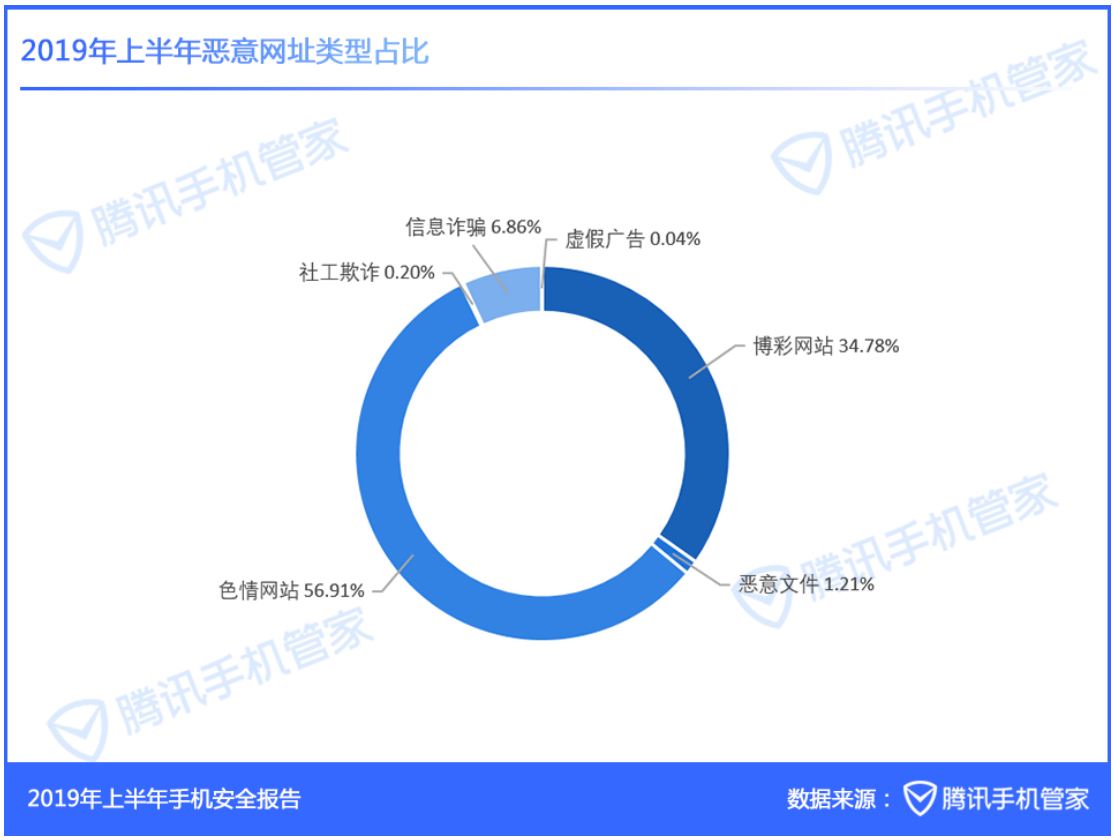
2019年上半年恶意网址拦截次数



2019年上半年手机安全报告　　数据来源：腾讯手机管家

2019 年上半年，腾讯安全实验室拦截恶意网址近 3010.05 亿次。1 月份拦截恶意网址最多，近 551.62 亿次。腾讯安全实验室基于海量数据处理能力，海量社交用户举报数据，结合全面的互联网产品接入，实现秒级识别恶意网址。

4.2 2019 年上半年恶意网址类型：色情网站最多



恶意网址的类型多样，根据腾讯安全实验室拦截的恶意网址数据，色情网站和博彩网站是最常见的恶意网址类型，占比分别达 56.91%和 34.78%。

跟据拦截规则，色情内容类的网站指包含大量的色情的内容或者提供色情服务的平台，提供色情内容展示以及提供情色交友等服务，例如色情视频播放、色情视频种子下载、色情小说、色情交流论坛、裸聊平台等。

博彩网站指包含大量的赌博推广的内容，或站点提供赌博交易平台，由于此类网站的资金安全无法保证，会造成财产的损失，依据国家相关的法律，这类网站也在拦截的范围之内。

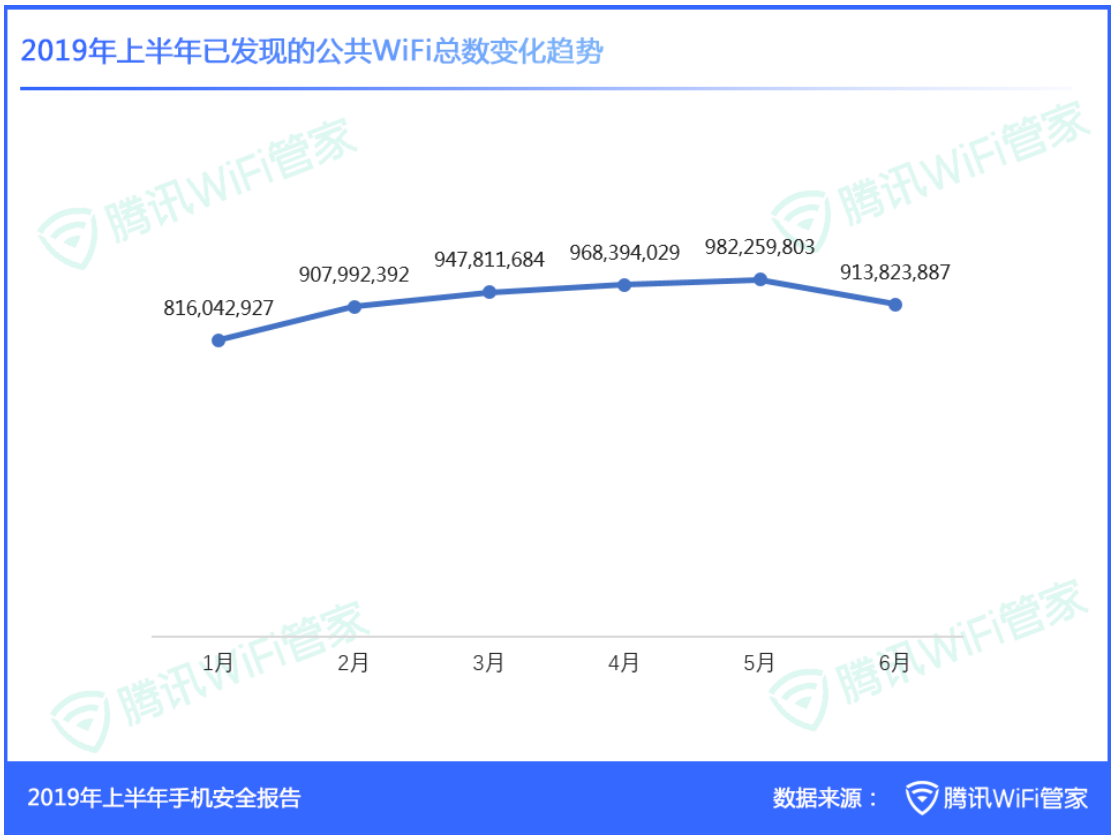
近年来，国内的非法博彩公司将博彩网站将服务器转移到境外，从事赌博活动。为了获取流量，这些网站疯狂做流量劫持和关键词劫持，以及群发垃圾短信。除此之外，这些博彩公司还用所谓的“高薪”将国人欺骗过去当推广、客服。

恶意网址威胁已经发展成为受经济利益驱使的商业活动，势力强大，而反恶意软件厂商

由于受到各种因素的制约，应对和反击措施相对被动，并且前者在暗处，后者在明处，形式对反恶意软件的开发者不利，但两种力量的斗争将持续下去。

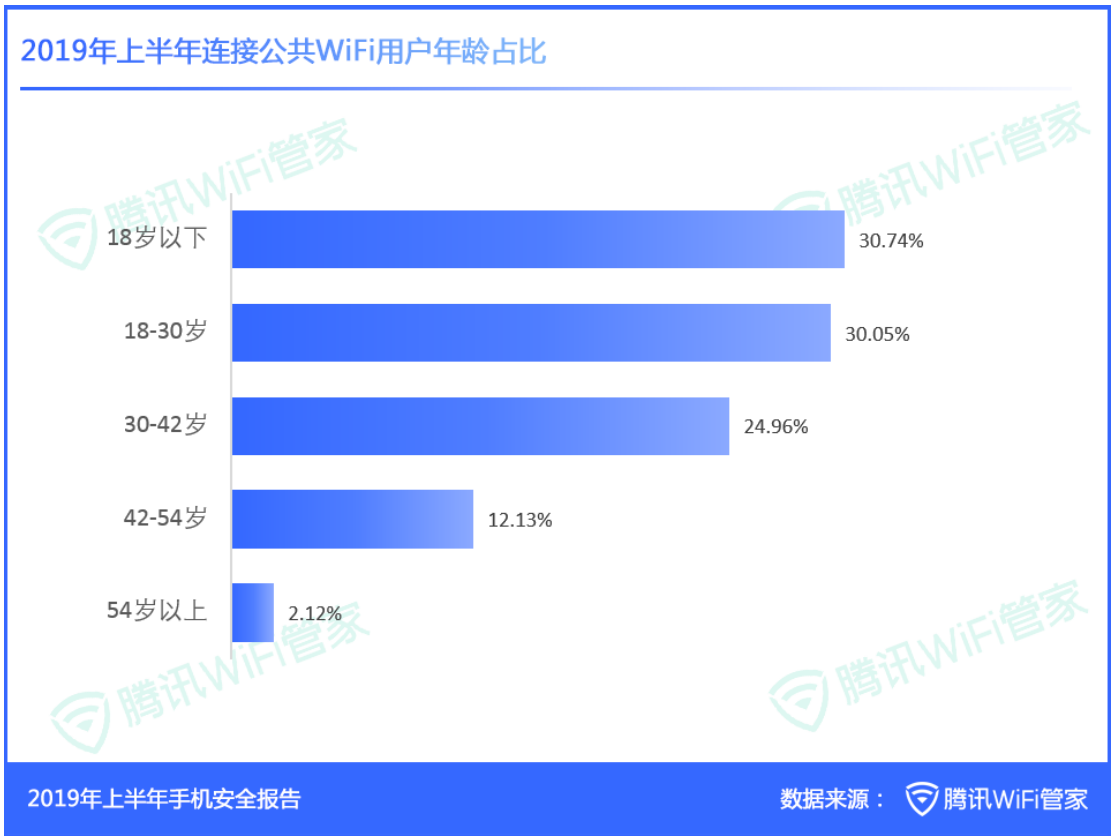
第五章 2019 年上半年风险 WiFi 现状分析

5.1 2019 年上半年已发现的公共 WiFi 数量近 9.14 亿

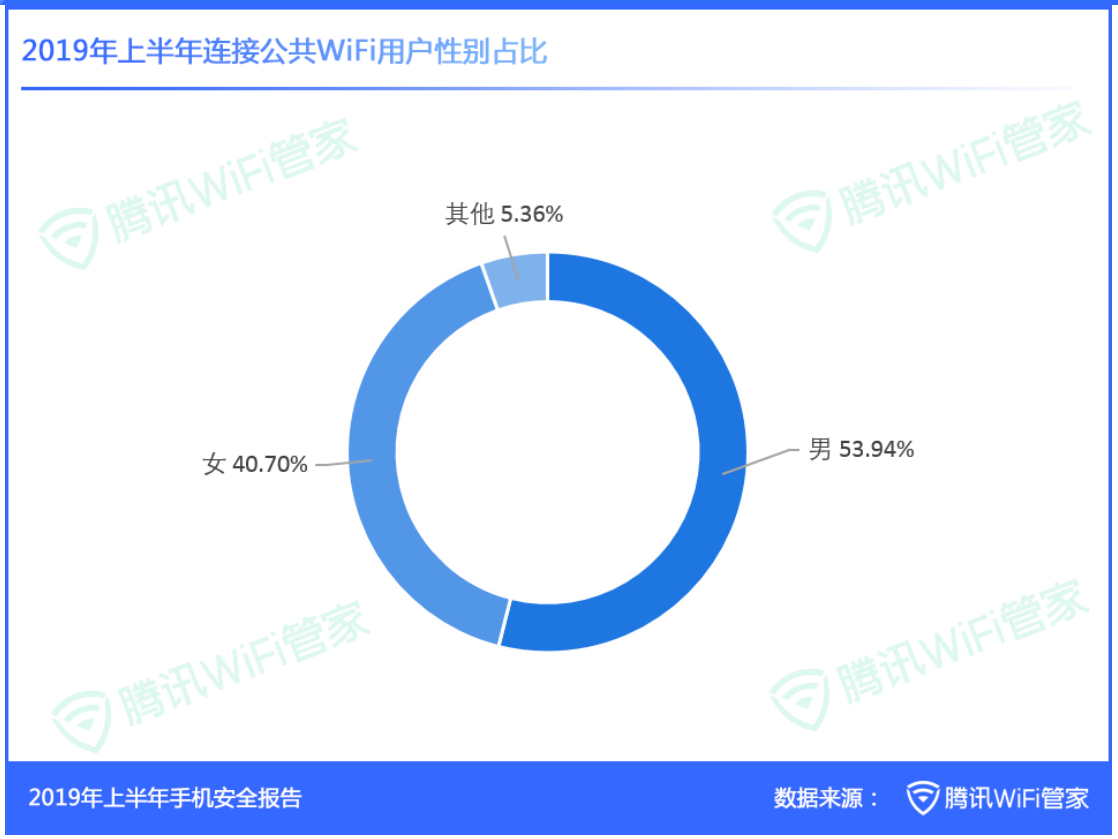


根据腾讯 WiFi 管家数据显示，截至 6 月，已发现的公共 WiFi 总量从 1 月份的 8.16 亿增长至 9.14 亿，在商场、餐厅、旅游景点、地铁、公交、机场等场所，公共 WiFi 随处可见。

5.2 2019 年上半年公共 WiFi 连接主力军：30 岁以下人群 男性多于女性

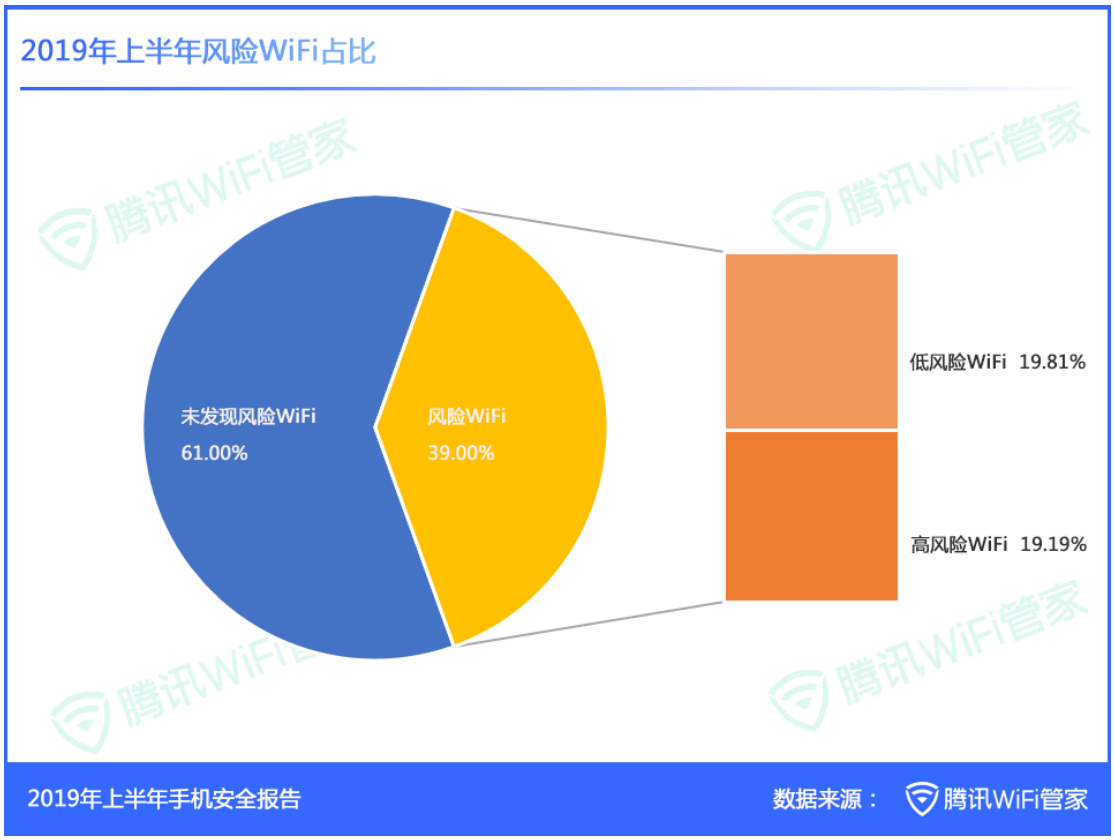


从年龄段上看，2019 年上半年连接公共 WiFi 的主体是 30 岁以下人群，占比 60.79%，30-42 岁、42-54 岁和 54 岁以上人群连接公共 WiFi 的占比则分别为 24.96%，12.13%和 2.12%。



性别方面，2019 年上半年连接 WiFi 用户中，男性多于女性，男性占比为 53.94%，女性占比 40.70%。

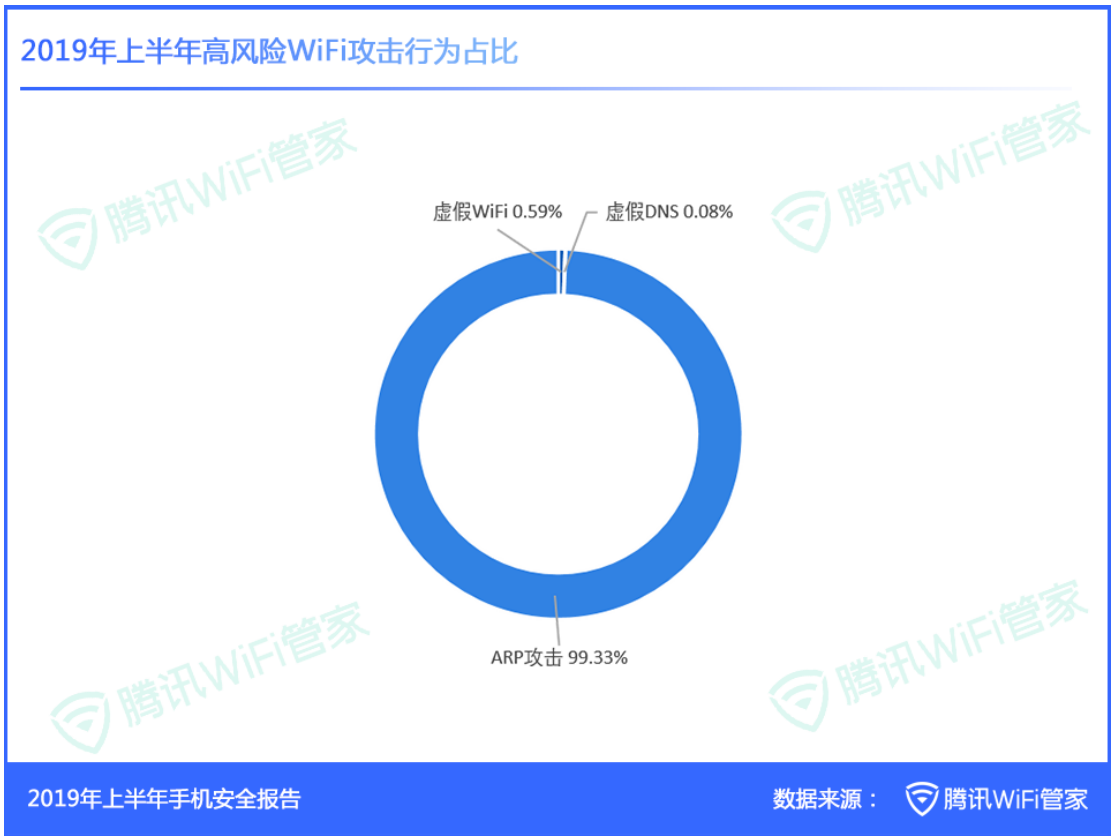
5.3 2019 年上半年风险 WiFi 占比 39.00%



从腾讯 WiFi 管家监测数据可以看出，2019 年上半年公共 WiFi 中，未发现风险 WiFi 占比 58.18%，风险 WiFi 占比 41.82%。

由于公共 WiFi 的开放性，易被攻击者利用漏洞，如果用户连接上这些风险 WiFi，其信息安全和财产安全将受到威胁。已经确认有 ARP 攻击、DNS 攻击或虚假 WiFi 行为的 WiFi，属于高风险 WiFi，占比 19.19%。未加密、未经认证，存在潜在风险的 WiFi 则是低风险 WiFi 指，占比 19.81%。

5.4 2019 年上半年高风险 WiFi 攻击行为以 ARP 攻击为主

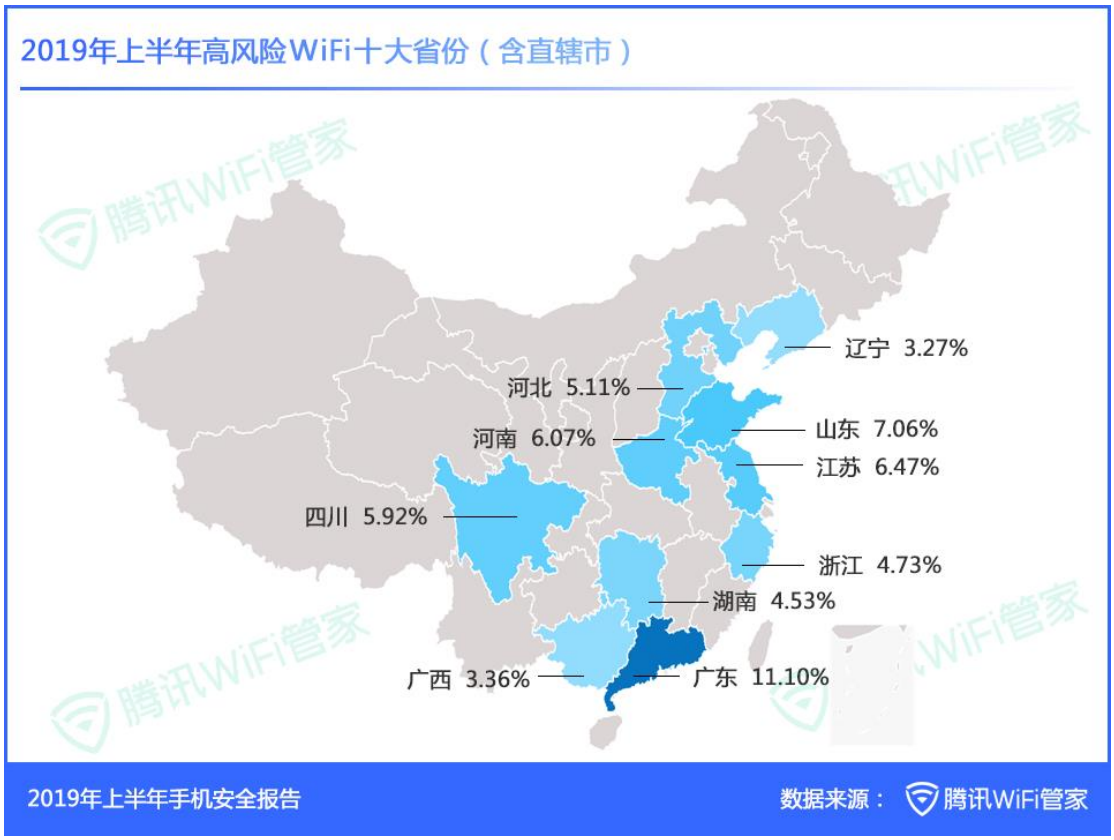


2019 年上半年，高风险 WiFi 攻击行为以 ARP 攻击为主，占比 99.33%。ARP 攻击通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，在网络中产生大量的 ARP 通信量使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP-MAC 条目，造成网络中断或中间人攻击。

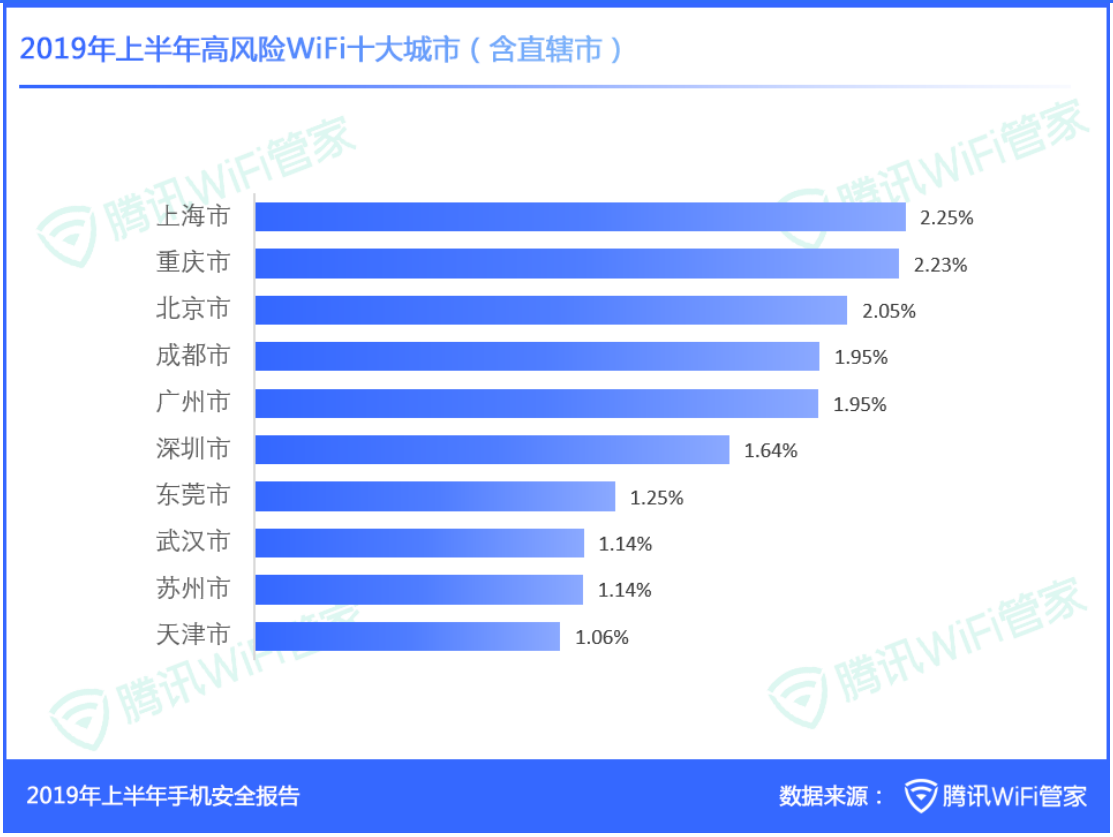
虚假 WiFi 占比 0.59%，一般通过伪装成知名路由器和运营商的默认 WiFi 热点来诱骗用户连接。虽然该类攻击占比较小，但由于是发生在用户熟悉的生活场景中，用户比较容易中招，一旦被不法分子窃取个人隐私信息、盗取钱财等，后果堪忧。

还有一种攻击行为是伪造虚假 DNS，又称域名劫持，指在劫持的网络范围内拦截域名解析的请求，分析请求的域名，把审查范围以外的请求放行，否则返回假的 IP 地址或者什么都不做使请求失去响应，导致用户对特定的网络不能反应或访问的是假网址。

5.5 2019 年上半年高风险 WiFi 主要分布在广东、山东及江苏



高风险 WiFi 分布最多的省份是广东、山东和江苏，占比分别为 11.10%、7.06%和 6.47%。



在城市方面，高风险 WiFi 在各个城市之间的分布较均匀，主要分布在上海（2.25%）、重庆（2.23%）和北京（2.05%）。

第六章 2019 年上半年手机安全特征与趋势分析

1. 四部门开展并不断深化 APP 违法违规专项治理工作

手机存储着越来越多个人信息和隐私，与此同时，APP 在采集和泄露数据信息方面却出现了不少安全问题。手机 APP 为用户提供方便和服务，但也可能存在窃取手机号、通讯录、通话记录、短信记录等隐私信息的行为。如何遏制 APP 强制授权、过度索权、超范围收集个人信息现象，成了公众最关心的问题之一。

今年 1 月 25 日，中央网信办、工信部、公安部、市场监管总局四部门联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》（以下简称《公告》）。根据《公告》，全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协

会成立 APP 专项治理工作组，制定了“APP 违法违规收集使用个人信息自评估指南”，供 APP 运营者参照指南对其收集使用个人信息的情况进行自查自纠，同时对用户数量大、与民众生活密切相关的 App 隐私政策和个人信息收集使用情况进行评估，受理对 APP 违法违规收集使用个人信息的举报。

“APP 违法违规收集使用个人信息自评估指南”从隐私政策文本、APP 收集个人信息行为和 APP 运营者对用户权利的保障三个方面，明确提出 9 个评估项：隐私政策的独立性、易读性；清晰说明各项业务功能及所需的个人信息类型；不应在隐私政策等文件中设置不合理条款等等。

目前，专项治理工作取得了阶段性成效，完成了对百余款用户投诉量大、社会关注度高的 APP 检查评估。近日，工信部印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，提出在今年 10 月底前完成全部基础电信企业、50 家重点互联网企业以及 200 款主流 APP 的数据安全检查，不断深化 APP 违法违规专项治理，持续推进 APP 违法违规收集使用个人信息专项治理行动。

2. 个人信息保护法已列入立法规划，为个人信息保护提供法律支持

今年 3 月，收录超 1.6 亿人的简历大数据公司巧达科技涉嫌提供海量简历数据进行牟利被查，非法爬取用户数据，数量之大、牟利之巨，令人咋舌。但这也只不过是掀开大数据行业中数据造假，窃取、买卖公民信息等乱象的冰山一角。

个人信息作为个人隐私的一部分，其重要性不言而喻，但相关现行法律在保护个人信息方面尚存在不完善之处，给不法分子提供可乘之机，非法收集、利用、传播、贩卖个人信息的现象大量出现，导致一系列的问题随之产生：垃圾短信、骚扰电话和邮件的不停轰炸，甚至遭遇精准诈骗等。

近年来，个人信息安全问题是社会各界十分关注的一个焦点，全国人大及其常委会高度

重视个人信息保护相关立法工作。今年上半年，十三届全国人大常委会将个人信息保护法列入立法规划，这意味着，国家在立法和执法上对于个人信息的保护在不断加强。

3. 电信网络诈骗专业化，打击治理电信网络诈骗形势严峻

虽然从 2015 年开始我国开展打击电信诈骗专项行动取得了显著效果，但随着移动互联网的快速发展，在高压严打形势下，电信诈骗犯罪并未禁绝，相反地，诈骗团伙的手段不断升级，上下游分工精细化、专业化和职业化，逐渐形成恶意注册、引流、诈骗、洗钱等环节完整的链条，犯罪效率越来越高。

从诈骗发生场景来看，以往诈骗团伙只借助单一的场景，比如借助电话，利用受害人的恐惧和服从心理，以最终引导受害人到银行转账为最终目的。如今诈骗场景越来越跨平台化，时间维度被拉长，犯罪在进行过程更难被察觉，其中较为严重和典型的是：东南亚“杀猪盘”交友诈骗和贷款类诈骗。作为全国受骗金额最大的诈骗类型“杀猪盘”，诈骗团伙先在婚恋网站和交友网站上，利用包装出来的虚拟形象取得受害人的好感，把受害人引导到社交平台进一步交流、铺垫，然后看时机又将受害人引导至赌博平台、博彩网站等第三方平台充值赌博，甚至在榨干受害人的积蓄后，引导受害人到借贷类 APP 贷款。

从地域上来看，电信网络诈骗从沿海地区向东南亚地区转移蔓延，甚至有外国人参与诈骗。国内诈骗团伙窃取了大量公民信息后转卖给躲藏在东南亚等地的诈骗团伙，冒充电商客服或快递员等角色，实施精准诈骗。

电信网络诈骗是一个长期性、系统性和持续性打击治理的社会问题，需要全社会各行各业共同来应对。

4. 支付领域的强监管仍在持续，“第四方支付”将迎来统一监管

2018 年，中国人民银行办公厅为进一步加强支付领域网络与信息安全管理，有效防范支付风险，切实保障消费者合法权益，发布《关于开展支付安全风险专项排查工作的通知》，

开展支付安全风险专项排查工作。

2019 年以来，多个一直游走在法律监管边缘，从事非法行为的“第四方支付”平台被捣毁。福建省公安机关成功破获一起侵犯公民个人信息案，捣毁 5 个非法“第四方支付”平台，查明平台充值资金流水 1.1 亿余元，抓获犯罪嫌疑人 40 余名。广东警方也通报了多起“第四方支付”接黑灰产的案件。

所谓“第四方支付”平台是指未获得国家支付结算许可，违反国家支付结算制度，依托支付宝、财付通等正规第三方支付平台，通过大量注册商户或个人账户，非法搭建的支付通道。

这些非法第四方支付平台通过开设所谓的网络科技公司或利用员工个人信息注册大量的第三方支付账号,利用技术手段搭建平台,聚合账号收取客户资金,为黑灰产业犯罪提供资金结算，从中赚取手续费。

据了解，相关部门正在推动第四方支付新的管理办法的制定，以明确行业准入等安全要求。

第七章 安全专家建议

2019 年上半年， Android 手机的安全形势仍不容乐观，手机用户要提高保护手机安全意识，养成使用手机的良好习惯。腾讯移动安全实验室专家对此提出如下建议：

1. 通过正规渠道下载安装 APP，授取权限时少点“允许”。由于安卓系统的开放性，大多数的 APP 应用存在不同类型的安全风险，尤其是影音播放类、通讯社交类和网上购物类应用。用户应通过官网或正规应用商店下载，避开可能潜藏恶意软件的渠道，如网页弹窗、来历不明的二维码或链接等渠道；警惕打着“破解版”旗号的 APP，可能被植入了恶意代码；在日常使用 APP 过程中也要加强自我信息的保护，认真阅读隐私条款，关闭不合理的访问权限或在必要时再授予相应的权限。

2. 谨防电信网络诈骗，增强防骗意识。2019 年上半年，用户标记的诈骗电话 2793.87 万个，举报诈骗短信 5425.31 万条，电信网络诈骗复杂多样，套路贷、东南亚杀猪盘等，都是迷惑性较强、诈骗金额较大的诈骗类型。

3. 确保移动支付 APP 安全，避开非法支付平台。认准合规合法的网络支付平台，不要轻信平台虚假宣传，不要随意扫来源不明的支付二维码，避免将个人资金转入此类非法支付平台。此外，通过正规渠道下载安全移动支付 APP，非正规渠道的 APP 容易被反编译、篡改或进行二次打包，存在漏洞或安全隐患，对用户的支付安全造成严重的安全威胁。

4. 安装手机安全软件，给手机多一份保护。腾讯手机管家依托自研 AI 反病毒引擎 TRP-AI 和自研杀毒引擎 TAV，在用户下载软件时进行安全扫描，识别其中存在的风险，并及时进行安全处理，保障手机设备的网络环境、病毒木马、支付环境、账号保护、隐私保护等方面的安全。此外，开启腾讯手机管家骚扰拦截功能，能够精准拦截骚扰诈骗电话，还生活一份清静。

腾讯手机管家官方网站：http://m.qq.com

腾讯手机管家新浪微博：http://weibo.com/txmanager

腾讯手机管家微信公众号：微信搜索“腾讯手机管家”或扫描以下二维码即可关注

腾讯移动安全实验室 2019 年 7 月 15 日

腾讯手机管家

有实力 无所惧

腾讯出品 值得信赖