2023 年上半年度
中国手机安全状况报告

2023 年 08 月

前言

在互联网飞速发展的当下，电信网络诈骗分子手段层出不穷，话术和技术不断更新换代，造成的电信网络诈骗犯罪发案最多、上升最快、涉及面最广、人民群众反映最强烈。诈骗分子通过各类新型的网络技术手段工具，利用完整的诈骗话术闭环洗脑受害人，严重侵害人民群众切身利益和财产安全。与之相应的，也催生了大量为不法分子实施诈骗提供帮助并从中获利的黑灰产业，此类黑灰产业又反向作用，成为电信网络诈骗犯罪多发高发的幕后推手和源头。

从 2023 年 360 安全大脑捕获到的黑产情报来看，电信网络诈骗及其背后的黑灰产业链出现“传统+网络”多种作案手法叠加的复合型犯罪形态。在引流渠道上，随着反诈力度的加强，黑灰产使用的电话、短信、网址等非接触式引流渠道受到重创，其将引流方式又从线上回归线下地推，一部分将含诈骗、博彩、色情内容的应用下载链（二维码）打印成卡片或贴纸，通过人工的方式张贴在汽车后视镜上，引导受害人下载诈骗 APP；一部分使用快递邮寄假冒的退款“红头文件”，引导受害人扫码添加“官方”账号，并诱使其在虚假投资平台投注。在“攻防对抗”上，黑产逐步使用云端 APP 生成技术，实现“免杀”，一方面制作 APK 时增加混淆手段，提高识别难度，当 APK 被识别后，重新更改包名+签名过免杀；另一方面直接将 APP 通过云端部署，实时生成或定期生成样本并替换原下载链的样本，达到受害人下载的应用均为未在互联网出现过的。

2020 年以来，公安部每年组织“净网”专项行动，依法重拳打击侵犯公民个人信息违法犯罪活动，累计侦破案件 3.6 万起，抓获犯罪嫌疑人 6.4 万名，查获手机黑卡 3000 余万张、网络黑号 3 亿余个，近 3 年来破获案件数量和抓获人数连续突破新高，打击力度和打击成果空前[1]。2023 年，公安部组织开展打击电信网络诈骗犯罪“鄂湘鲁豫”区域会战，指挥 4 省公安机关同步开展集中打击，成功抓获一大批涉诈违法犯罪嫌疑人，捣毁犯罪窝点 3300 余个，缴获手机、电脑、“两卡”等作案工具 10.4 万个（台），扣押现金、虚拟货币等涉案资产价值 5800 余万元[2]。

《2023 年上半年度中国手机安全报告》将持续从电信网络诈骗手法、攻防技术、产业链为切入点，依托 360 安全大脑能力，深度剖析电信网络诈骗及关联的重点黑灰产业链，360 也将积极发挥自身技术优势，综合运用人工智能、大数据、云计算等技术手段有效打击涉诈产业链，保障用户网络安全。

目录

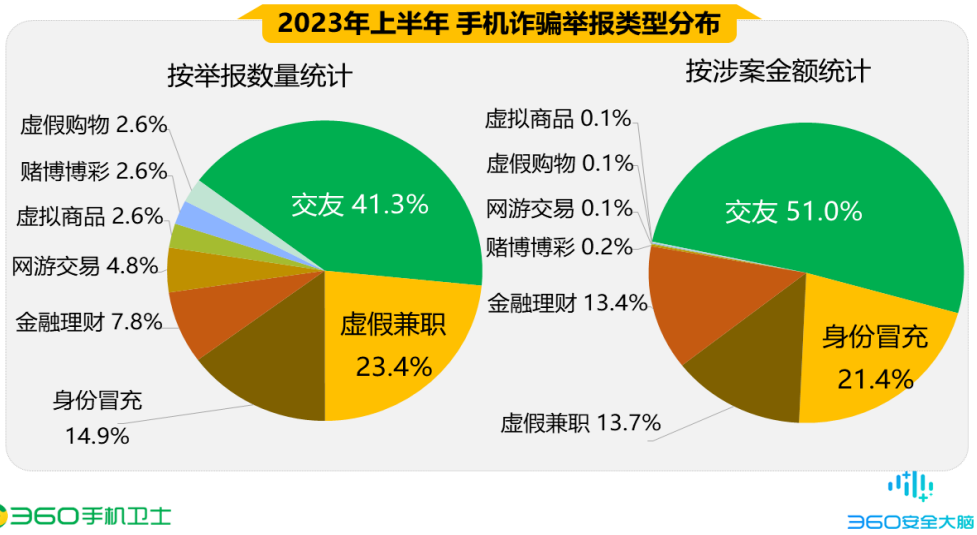
第一章　2023 年上半年度手机诈骗概况

在当下的网络化生活中，个人信息几乎遍布交易支付、娱乐、社交等生活的每一个场景，其背后的经济价值日益显著，也成为网络攻击、电信网络诈骗、敲诈勒索等网络违法犯罪的目标之一。360 安全大脑基于用户举报数据分析研究，发现 2023 年上半年手机诈骗呈现出交友类占比最高、身份冒充类涉案总金额最高、金融理财人均损失最高等特点。针对这些诈骗场景，用户需提高防范意识，不轻易相信陌生人的信息，避免上当受骗。同时，反诈行业应重点加强对此类场景的关注度，保障人民群众切身利益和财产安全。

一、 用户举报

1. 报案数量与类型

2023 年上半年度 360 反诈赔付保（原手机先赔）共接到 8 类手机诈骗举报，涉案总金额高达 1172.0 万元，人均损失 43568 元。在所有诈骗类型中，交友类占比最高达 41.3%；其次是虚假兼职（23.4%）、身份冒充（14.9%）、金融理财（7.8%）、网游交易（4.8%）等。从涉案总金额来看，也是交友类诈骗总金额最高，高达 598.1 万元，占比 51.0%；其次是身份冒充诈骗，涉案总金额 252.2 万元，占比 21.5%；虚假兼职排第三，涉案总金额为 160.2 万元，占比 13.7%。下图为 2023 年上半年度手机诈骗的举报类型与涉案金额分布情况：

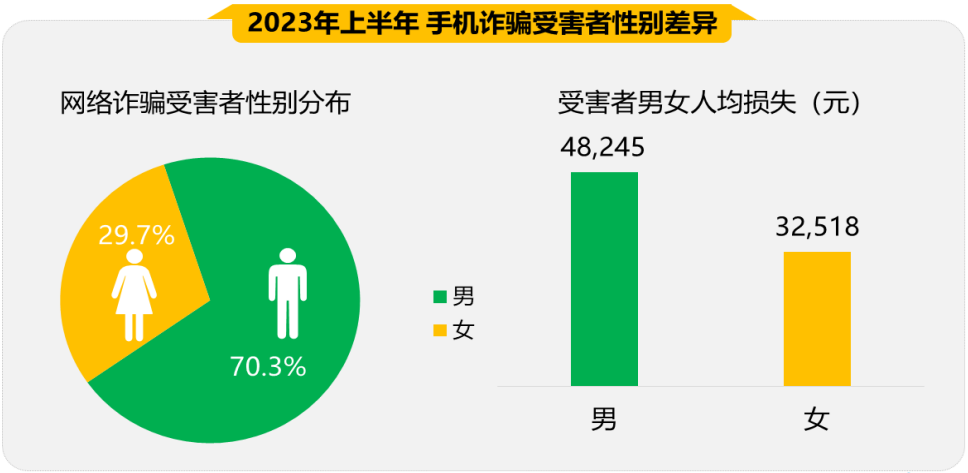


2023 年上半年度，手机诈骗中交友、身份冒充、虚假兼职、金融理财属于高危诈骗类型，其中，金融理财人均损失最高，约 7.5 万元；其次为身份冒充类，人均损失约为 6.3 万

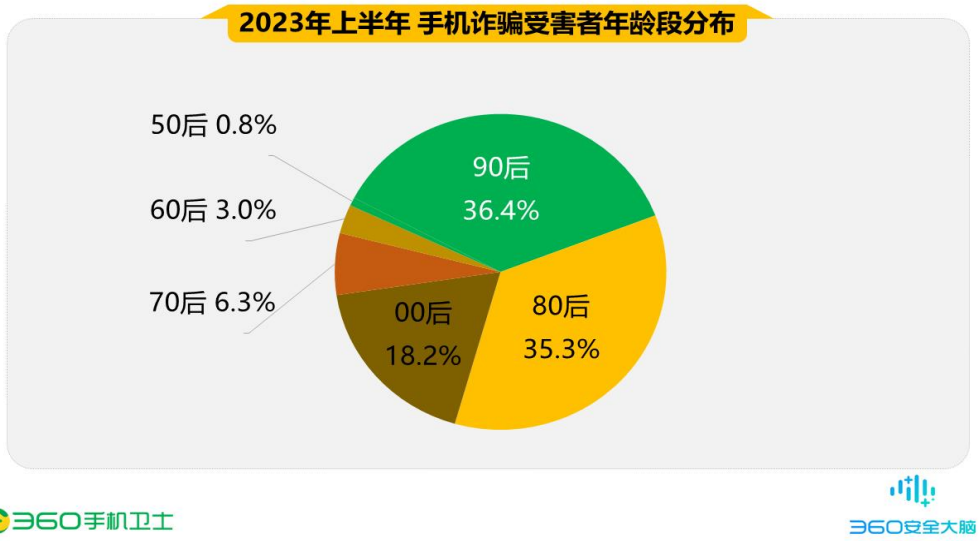
元。研究发现，上半年多类诈骗中的引流方式均发生了改变。例如，虚假兼职类诈骗由线上引流转向线下，通过邮寄印有二维码的免费小商品（茶杯、手机支架等）快递，用户扫描二维码进入指定群后，被引导参与刷单任务，后续无法提现，发现受骗。身份冒充中虚假教育机构类诈骗以往通过互联网进行引流，但随着反诈宣称力度的增加，大家对于互联网的信息提高了防范意识，黑产通过快递邮寄档案袋提高可信度，推荐清退方案，引导用户在平台进行投资理财，实际无法提现。

2. 受害者性别与年龄

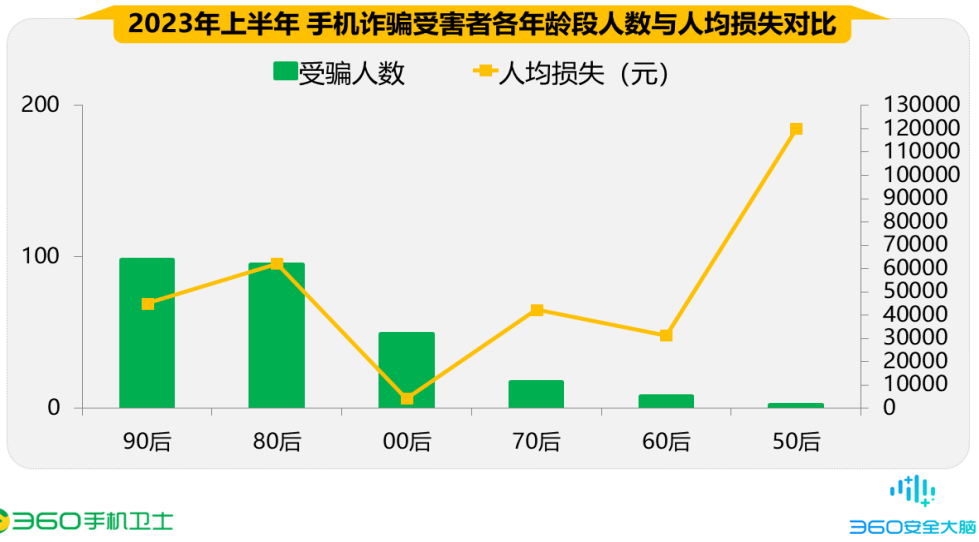
2023 年上半年度，从举报用户的性别差异来看，男性受害者占 70.3%，女性占 29.7%，男性受害者占比高于女性。从人均损失来看，男性为 48245 元，女性为 32518 元，男性人均损失高于女性。下图为 2023 年上半年度手机诈骗受害者性别差异：



从被骗网民的年龄段看，90 后的手机诈骗受害者占所有受害者总数的 36.4%，是不法分子从事网络诈骗的主要受众人群；其次是 80 后，占比为 35.3%；00 后占比为 18.2%；70 后占比为 6.3%、60 后占比 3.0%、50 后占比为 0.8%。下图为 2023 年上半年度手机诈骗受害者年龄段分布：



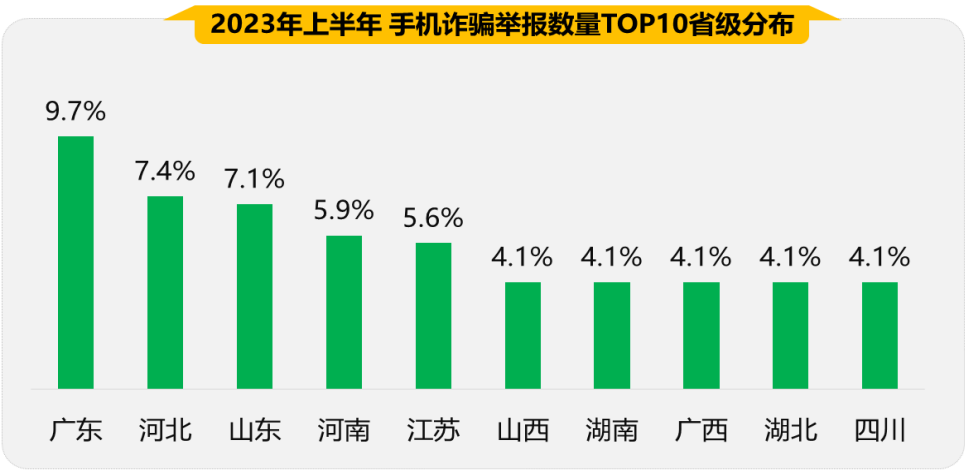
从被骗网民的年龄段人数来看，2023 年上半年度 90 后、80 后、00 后均为诈骗高发人群，受骗类型以交友类为主。诈骗人员在互联网社交平台撒网式交友，吸引用户上钩，通过话术套出该用户的工作、爱好进而了解这个人，再以话术聊感情，引诱该色粉用户开视频裸聊。之后以信号不好挂掉视频，诱导下载安装含窃取通讯录功能的 APP，并诱导获取相关的手机权限。获得通讯录后，以掌握到对方通讯录好友信息，会将其裸聊视频发送给其通讯录好友为由进行敲诈勒索。受害人为了保障自己的隐私不外泄，会源源不断的满足对方的多次勒索，造成巨大的财产损失。



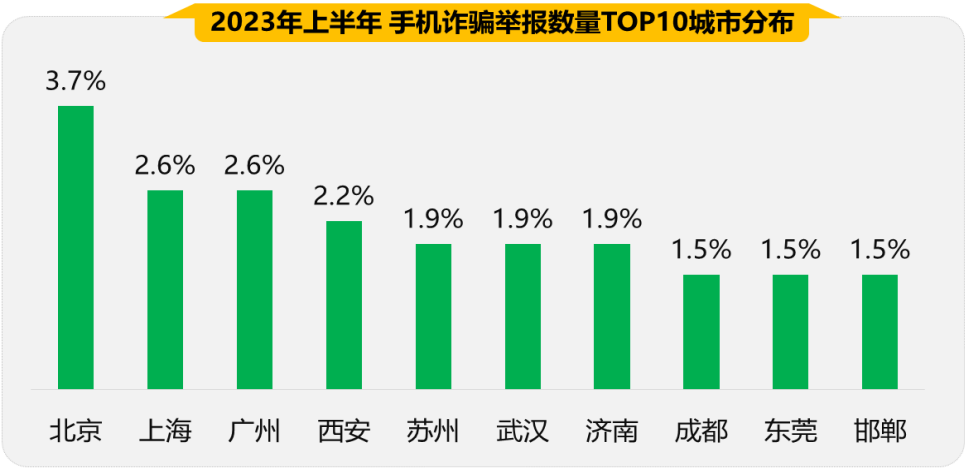
3. 受害者地域分布

2023 年上半年度，从各地区手机诈骗的举报情况来看，广东（9.7%）、河北（7.4%）、山

东（7.1%）、河南（5.9%）、江苏（5.6%）这 5 个地区的被骗用户最多，举报数量约占到了全国用户举报总量的 35.7%。下图给出了 2023 年上半年度手机诈骗举报数量最多的 10 个省份：



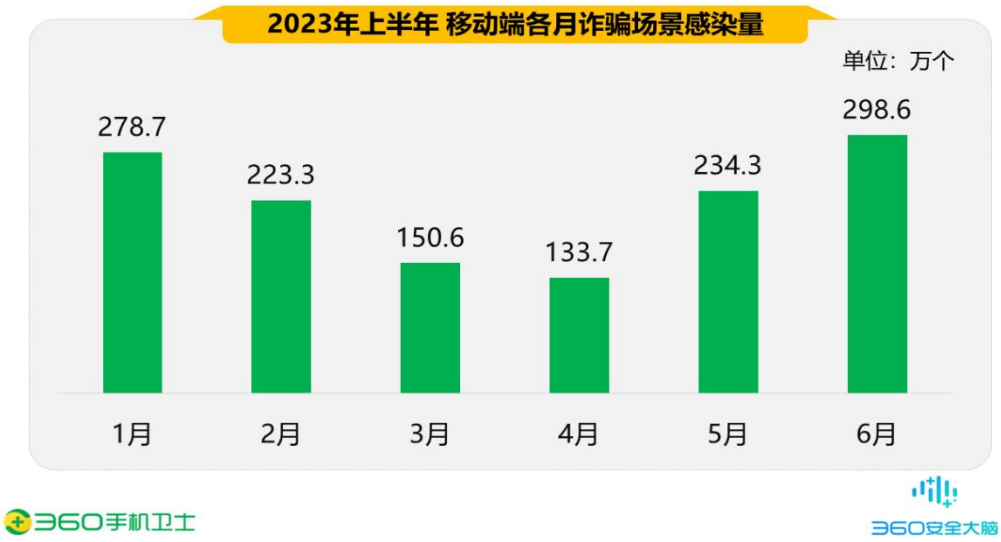
从各城市手机诈骗的举报情况来看，北京（3.7%）、上海（2.6%）、广州（2.6%）、西安（2.2%）、苏州（1.9%）这 5 个城市的被骗用户最多，举报数量约占到了全国用户举报总量的 13.0%。下图给出了 2023 年上半年度手机诈骗举报数量最多的 10 个城市：



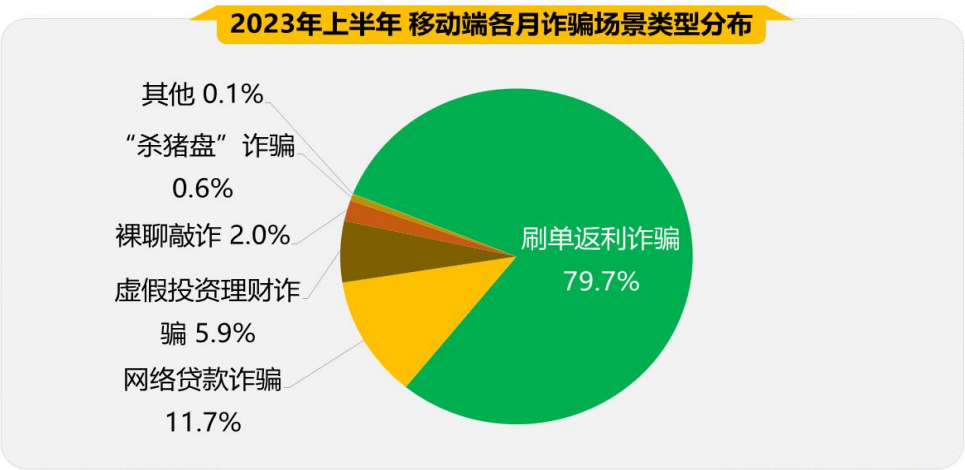
二、 移动端诈骗场景识别

1. 移动端诈骗场景感染量与类型分布

2023 年上半年度，360 安全大脑针对移动端涉诈应用进行分析研究，通过其共识别出主流诈骗场景感染量约 1319.2 万，下图为 2023 年上半年度移动端各月诈骗场景感染量统计：

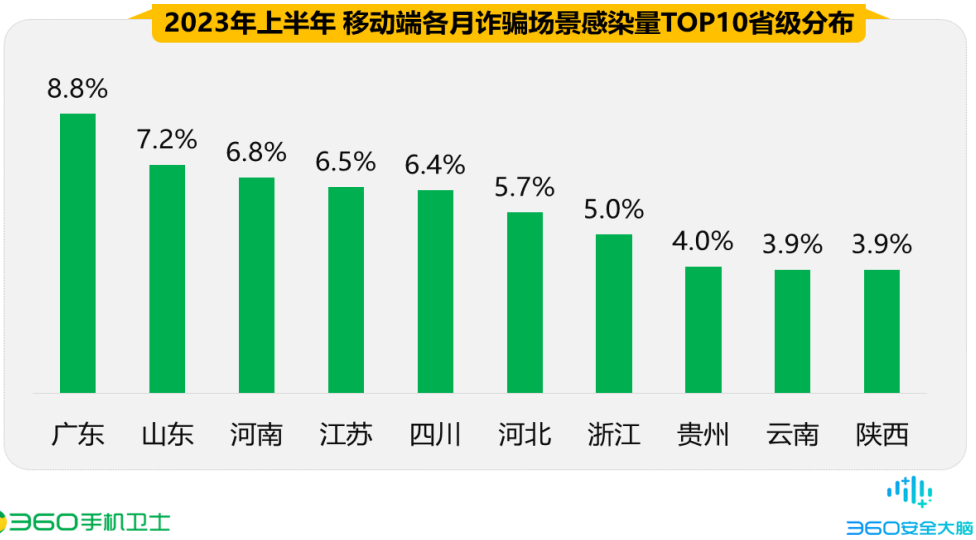


2023 年上半年度，移动端诈骗场景类型主要为刷单返利，占比 79.7%；其次为网络贷款（11.7%）、虚假投资理财（5.9%）、裸聊敲诈（2.0%）、“杀猪盘”（0.6%）等。针对持续高发的诈骗态势和日益激烈的攻防对抗，360 手机卫士安全攻防团队加大技术反制研发投入，通过各种模型策略增加黑灰产样本的识别能力和数量。下图为 2023 年上半年度移动端诈骗场景类型分布：

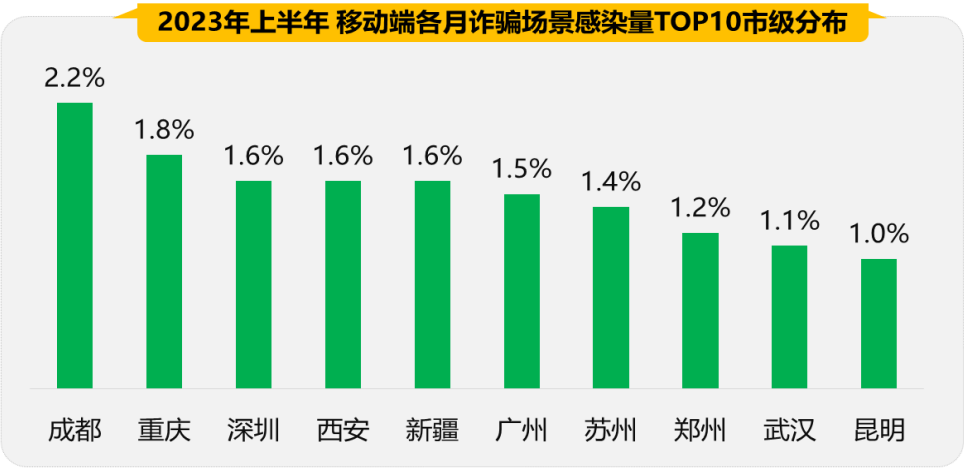


2. 移动端诈骗场景感染量地域分布

2023 年上半年度，从省级分布来看，诈骗场景感染量最多的地区为广东，占全国感染量的 8.8%；其次为山东（7.2%）、河南（6.8%）、江苏（6.5%）、四川（6.4%），此外河北、浙江、贵州、云南、陕西的诈骗场景感染量也排在前列。



从城市分布来看，诈骗场景感染量最多的地区为成都，占全国感染量的 2.2%；其次为重庆（1.8%）、深圳（1.6%）、西安（1.6%）、新疆（1.6%），此外广州、苏州、郑州、武汉、昆明的诈骗场景感染量也排在前列。


2023年上半年 移动端各月诈骗场景感染量TOP10市级分布
2.2%
1.8%
1.6%
1.6%
1.6%
1.5%
1.4%
1.2%
1.1%
1.0%
成都
重庆
深圳
西安
新疆
广州
苏州
郑州
武汉
昆明

第二章　黑灰产攻防技术

随着移动互联网的普及，网络“晒一晒”成为主流，网络分享后“遗留”在互联网的个人信息，成为黑产眼中的香饽饽，衍生出信息加工及利用个人信息实施定向诈骗的产业。随着公众反诈意识的提高，传统利用图片合成技术实施诈骗的方式，逐渐被黑产行业淘汰，开始向更加仿真化的视频合成转型，使用视频合成、手机虚拟相机技术实施诈骗。同时为防止诈骗 APP 被 360 手机卫士等反诈类 APP 所识别，黑产持续增加技术投入，迭代出 APP 混淆、云端生成、下载链更换等方式尝试绕过反诈 APP 识别，实现 APP“免杀”，攻防对抗逐渐从虚假图片、话术洗脑，转为纯技术的无硝烟战争。为应对这种攻防对抗的方式转移，360 将发挥在网络安全行业积累的攻防打击技术优势，赋能在反诈行业，增加反诈行业综合打击能力。

一、 眼见不一定为真，诈骗场景使用“换脸”技术

随着 2023 年上半年 AI 换脸技术诈骗被持续揭露，引发大众关注与担忧。从 360 安全大脑的安全情报中，我们发现“换脸”技术目前被黑产应用于裸聊敲诈、身份冒充等诈骗场景以及部分无人直播场景中，其原理是替换手机相机的画面，主要使用事前合成视频替换、实时替换两种方式。以下以黑灰产场景为切入点，针对这两类技术进行剖析。

1. 手机相机内容“劫持”替换指定视频

在裸聊敲诈场景中，诈骗人员在互联网社交平台撒网式交友，吸引用户上钩，通过话术套出该用户的工作、爱好进而了解这个人。再以话术聊感情，引诱该用户开视频裸聊，并让对方在视频过程中露脸、露下体，录制对方视频画面。以信号不好挂掉视频，诱导下载安装含窃取通讯录功能的 APP，并诱导给该 APP 相关的手机权限，获得通讯录后，以掌握到对方通讯录好友信息，会将其裸聊视频发送给通讯录好友为由进行敲诈勒索。

在这个诈骗场景中，受害人之所以相信对方，源于看到了对方的“裸聊”画面，但实际上，用户看到的裸聊画面是诈骗人员通过互联网收集的“美女视频”。通过 APP 劫持手机相机加载该“美女视频”，与受害人视频通话时，对方看到的就是预先加载的“美女视频”画面。原理是通过对手机 ROOT，获得手机“管理员”级别的权限，再使用相机劫持类 APP 接管手机相机内容，将事前通过互联网收集的视频画面，例如美女视频，导入到相机劫持类 APP，实现手机相机画面内容的替换。当视频通话时，视频软件调用手机相机，手机提供给视频软件的画面就是替换后的内容，可以理解为播放指定的视频内容给对方看。出于对手机安全性、

稳定性的保障，目前手机厂商均提高了对手机 ROOT 的难度，故黑产多采用 ROOT 难度低、系统版本低的手机搭建相机劫持设备，如下图展示，虚假相机类支持的系统版本及黑产售卖虚拟相机手机演示视频画面。

在无人直播场景中，黑灰产一方面也像裸聊敲诈场景那样使用提前收集的视频，替换直播 APP 相机的画面内容；一方面针对虚拟相机 APP 进行版本升级，如下图展示的增加视频推流功能，将主流直播平台中他人的直播内容，转播至自己的直播间，同时导入提前编写的话术，进行边播边评论，营造直播间有大量活跃观众的假象。

2. AI 合成高仿及实时换脸视频

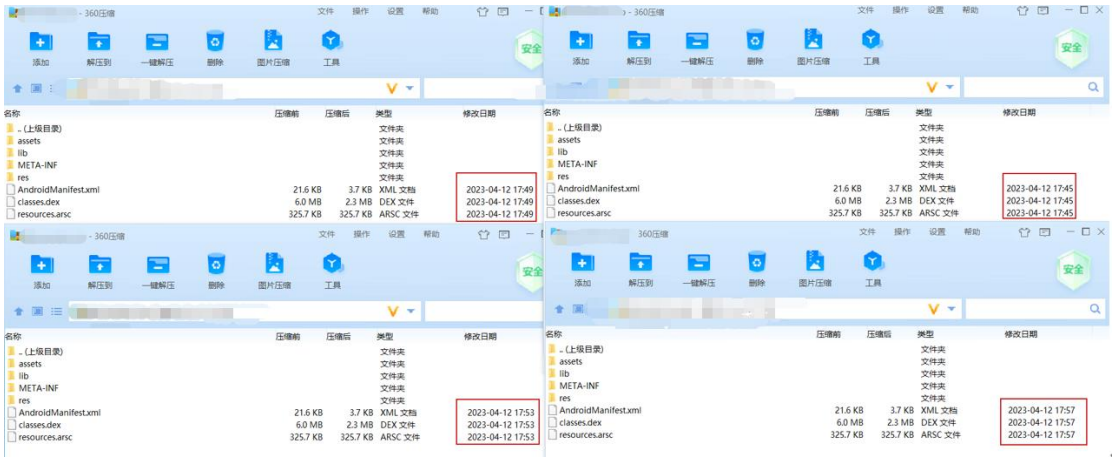
为了增加受害人的信任以及绕过某些平台的人脸认证，诈骗人员增加了对所使用的替换视频的真实性投入，使用经过模型训练的高仿合成视频或使用静态人脸转动态人脸工具。包括使用离线合成换脸视频和实时合成换脸视频，其主要原理是针对原视频、目标视频进行视频图片抽帧，分别提取图片中的人物脸部进行模型训练，随后使用新的人脸画面覆盖原视频中的人脸画面，合成换脸视频。再结合上述使用的手机虚拟相机类 APP，替换手机相机展示的内容，达到以假乱真的目的。

部分黑产将训练后的人脸模型，配合电脑视频推流+虚拟相机软件，用于诈骗、直播等换脸场景中，其原理是利用视频推流软件捕获电脑实时生成的换脸画面，将该视频推送给虚拟相机软件，虚拟相机软件替换原电脑的画面，展示给使用电脑相机的应用，实现展示换脸内容。

二、 黑产逐步使用云端 APP 生成技术，实现“免杀”

早期诈骗 APP 在制作时，会使用相同的签名证书生成多个 APP 或使用多个签名证书生成多个 APP，并将这些样本存储在不同的下载服务器或上架至应用分发平台生成不同的下载链。受害人在下载链失效前通过相同下载链下载的应用是相同的，此种情况下当该下载链、APP 被网络安全厂商识别为欺诈，后续在传播过程中用户看到网络安全厂商给予的安全提示，可能会发现自己处于诈骗场景从而醒悟。即涉诈 APP 一旦进入到网络安全厂商的病毒库中，该应用在后续传播的过程中存活周期变短，为了增加 APP 的存活周期，黑灰产分别在涉诈应用的生成、传播增加了攻防对抗策略，这里为冒充公检法 APP 为例。

如下图展示的冒充公检法应用的下载链，其下载链格式为 http://服务器 IP+/随机字符串，落地链为 http://服务器 IP/+packaged/+随机字符串.apk，每次点击时，生成的应用包名、签名均不相同。从这些应用生成时间来看，为下载应用附近时间点，说明不同时间段，用户通过同一个下载链下载到的应用并不相同，但其代码结构、使用 SDK-KEY 相同，推测是通过同一个源码生成的 APP，可能为云端实时生成类。



通过对此类 APP 的上游技术链分析，发现目前黑产针对 360 等具有涉诈 APP 识别能力的厂商进行 APP 免杀对抗。其主要方式是，制作 APK 时增加混淆手段，增加识别难度。当 APK 被识别后，重新更改包名+签名或直接将 APP 通过云端部署，实时生成或定期生成样本并替换原下载链的样本，达到下载链下载的样本均为未在互联网出现过的最新 APP。

相较于冒充公检法使用自建的下载服务器，攻防策略调整在于自身的攻防能力，例如虚

假兼职、裸聊敲诈多依托上游供应商提供的 APP 分发平台的攻防策略。早期的攻防主要判断访客的设备，只有检测到访客的设备为手机或移动端设备时才显示下载链，但从 2023 年上半年捕获到的虚假兼职、裸聊敲诈 APP 在分发平台的下载链，我们发现这些涉诈类 APP 在分发平台的下载链出现两种情况，第一种和冒充公检法样本一样，不同时间在相同下载链下载到的应用不相同，第二种不同时间在相同下载链会进行页面二次跳转至不同的 APK 落地下载链，下载应用也不相同。鉴于黑灰产技术供应链化，未来同链不同包技术将可能成为黑产的一个标准化对抗策略。

第三章　黑灰产业链现状

随着执法机关对黑灰产行业持续开展“打源头、摧平台、断链条”行动，互联网行业内部也纷纷迭代自有风控模型，传统黑产网络引流渠道受到重创，即诈骗电话和短信在收发两端双向受阻，被识别、被拦截。黑产开始调整引流方式及攻击目标，一方面从线上引流转向人工通过色情内容、免费小礼品等进行线下引流；另一方面将攻击人群从中国调整到目前反诈意识相对薄弱的一些国家。

一、 汽车张贴小广告、邮寄文件成黑产新型引流方式

黑灰产使用的电话、短信、网址等传统引流渠道，随着反诈力度的加强，受到重创，黑产开始将引流方式从线上转向线下地推。一部分将含诈骗、博彩、色情内容的应用下载链（二维码）打印成卡片或贴纸，通过人工的方式张贴在汽车后视镜上，引导受害人下载诈骗 APP。另一部分使用快递邮寄假冒的退款“红头文件”，让受害人以为之前购买的课程可以退款了，扫码添加清退人员“官方”社交账号，随后引导到虚假投资平台进行投注，即通过线下传播 APP、引流社交账号。

目前黑产使用的地推产业在全国多地“开花”，部分车主的车辆被黑产多次张贴后，为防止再次被贴，停车时使用包装袋将汽车后视镜包住，但事后发现包装袋被破坏，汽车后视镜仍被张贴，严重影响驾驶中后视镜的正常使用，更有车主的汽车后视镜、车身均被张贴多张。目前地推产业像狗皮膏药一样，撕掉又贴，甚至更多，影响十分恶劣。以下将从地推的运营模式、涉及的诈骗手法进行分析。

1. 线下引流背后的诈骗手法

1.1　通过车贴发布免费招嫖广告，引导至虚假刷单平台投注

这些车贴纸张主要包含“同城约”等涉黄词语以及网址二维码两部分内容，下载链多以色情内容为页面背景的 APP 下载链，但实际上应用与“招嫖”无关，多为披着色情外衣的诈骗应用。当受害人安装该应用后，APP 中的客服人员以用户完成投注任务即可免费“招嫖”为由，引导用户在指定的平台完成投注操作，当用户完成操作后拒绝用户提现。相较于以往的虚假兼职刷单场景，该手法以免费同城约为幌子，更易吸引更多人上当。

1.2　通过清退文件发布虚假清退信息，引导至虚假理财平台投资

黑灰产通过非法渠道掌握到了 P2P 平台、培训机构用户信息，宣称平台目前配合国家机关进行退费，吸引用户关注。此类诈骗以往通过互联网进行引流，但随着反诈宣称力度的增加，大家对于互联网的信息提高了防范意识。故黑产通过快递邮寄档案袋增加大家的信任度，当联系上用户后，骗子以用户购买项目的平台与第三方进行合作清退，并给用户推荐清退方案，在指定的理财平台购买项目，获利后返还学费。用户在前期操作中，骗子为增加用户的信任度会给予用户蝇头小利，待用户追加资金后，增加用户提现门槛，如任务还未完成，需要增加投资额，即使用户按照要求操作，后续仍拒绝用户提现。

2. 线下引流黑产运作模式

2.1 车贴黑产

车贴上线在黑灰产群，以每张 0.7-0.8 元的价格招收地推人员（卡手），向卡手提供涉诈、黑灰相关的 APP 下载链二维码、链接、卡片打印模板。卡手通过自备的打印机打印后，进行线下散播，如下图黑产发布在黑产群中的贴卡过程，贴在汽车主驾驶倒车镜上。为了保证张贴的效果，上线会要求卡手测卡，在打印纸张前录制访问二维码的过程，以确保二维码在张贴前还可正常访问。同时限制张贴时间、位置，在晚上 10 点至次日 10 点进行张贴，且只能贴主驾驶倒车镜或主驾驶雨刷器下面压住，不能贴女士车、路灯、消防栓或奇奇怪怪的建筑物，并且张贴过程中要记录张贴的位置轨迹。卡手张贴完后，上线为防止卡手造假，会根据二维码的访问情况、应用的下载应用数量，归属地进行 App 安装统计，结合卡手的交单数量给予结算。随着部分地区加强对车贴的打击力度，如下图展示，部分地推为保证车贴的下载成功率，在发布任务时，会动态调整限制地推的地区。

6.29贴纸最新禁止地区-单价

福建省	河南省	贵州省	黑龙江省	吉林省	沈阳
云南昆明	广东东莞	四川成都	陕西西安	陕西咸阳	广西南宁
湖南长沙	湖南娄底	湖北武汉	重庆	天津	河北石家庄
山东临沂	山东济南	山东菏泽			

不要重复地区做无效单，区不过3000，县不过2000，报量精确到市区街道或者区县街道

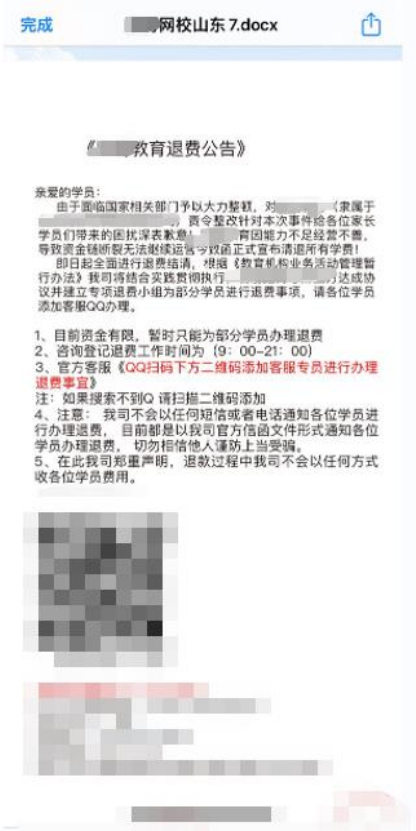
以上禁止地区做单无效

1 1000-10000每张0.8
2 10000-30000每张0.85
3 30000-50000每张0.88
4 50000-80000每张0.9
5 80000以上0.95
（以上再量大的私信群主谈）
最低1000张起，低于1q累计到1q结算
团队额外奖励
当日结算单量排名（满一万单）
第一 奖励199u
第二 奖励88u
第三 奖励66u
散人结算群每天都会发大额红包福利

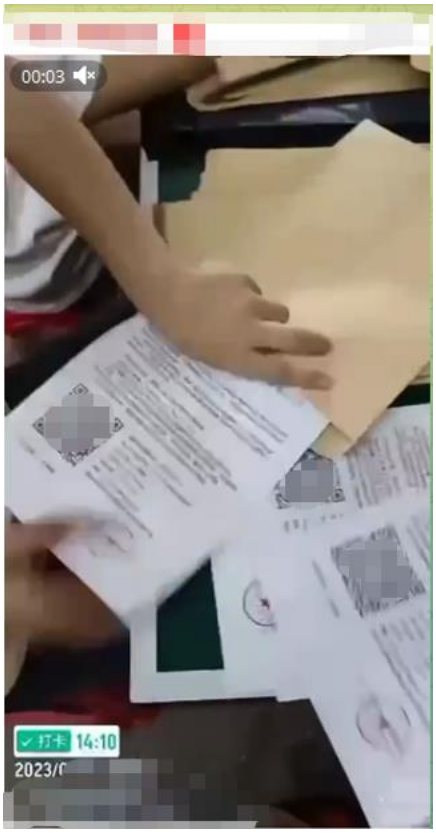
2.2 “清退”邮寄快递黑产

清退上线在黑灰产群招收代发快递人员，向其提供清退文件模板、受害人收件信息。快

递代发人员通过打印机打印诈骗人员制作的冒充“中华人民共和国教育部”发布的教育清退公告，并将纸质文件封装至牛皮纸文件袋中，再根据上线（诈骗人员）提供的受害人信息，在快递点邮寄快递。打印的“清退公告”如下图展示的，常用话术为“由于面临国家相关部门整顿，该教育集团因能力不足经营不善，导致资金链断裂无法继续运营。今致函正式清退所有学费，根据《教育机构业务活动管理暂行办法》该教育集团与第三方达成协议并建立专项退费小组为部分学员进行退费事项，请各位学员添加客服 QQ 办理。同时提醒收到函件的学员，该公司不会以任何短信或电话通知学员办理退费，仅会使用官方信函文件，退款过程中不会以任何方式收取各位学员费用，切勿相信他人谨防上当受骗”。话术内容可以总结为，公司经营不善要配合国家进行清退退款，退款通过合作的第三方企业办理，为后续引导用户到虚假投资平台增加铺垫。

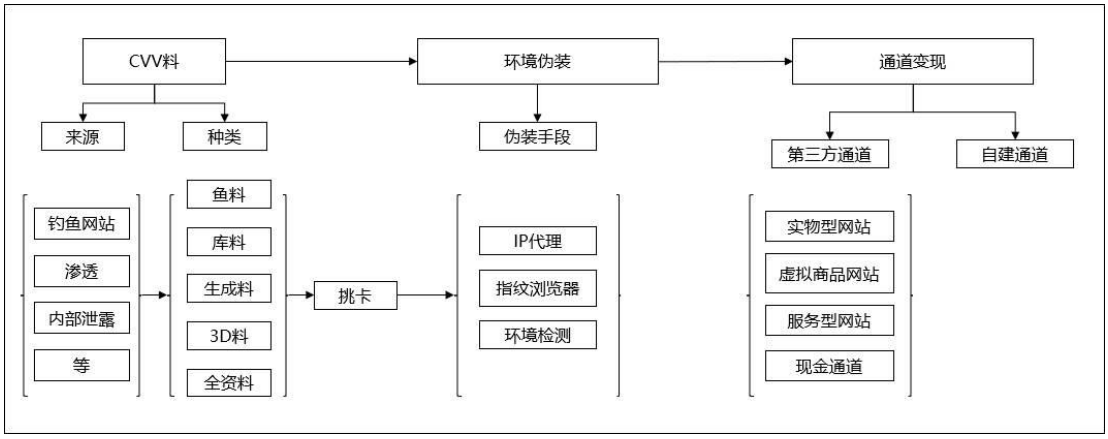


为了保证清退文档快递能够顺利发出、同时增加受害人的信任度，上线（诈骗人员）在给地推人员布置任务时，会要求代发人员打印模板前校对数据一致性，例如清退冒充的企业名称与收件人对应的平台、冒充机构的名称与公章名称一致性。文档使用牛皮纸文件袋封装，快递使用快递专用信件袋封装，发送的快递企业配送时效需在 3 日内，若超过 3 天则需要驱车前往受害人就近快递点发送。为防止快递代发人员造假，如下图展示的，上线（诈骗人员）要求快递代发人员录制打印文档、测试文档内联系方式是否有效，文档打包、快递邮寄的视频。



二、 黑产利用测活、指纹浏览器盗刷 CVV

在对黑灰产分析时发现目前银行卡安全校验码（CVV）盗刷在黑灰产圈内十分活跃，已形成师傅带徒弟、收费教学、抱团集中盗刷的模式，同时由于产业混乱，各种“黑吃黑”现象频发。从掌握到的情报看，CVV 盗刷产业，从早期的盗刷欧美国家信用卡，转向集中盗刷东南亚国家信用卡。其主要方式是盗取他人的 CVV 信息后，使用工具模拟搭建与原 CVV 持卡人相同的网络环境，在一些支持信用卡支付的平台进行消费套现，该攻击手法主要包含料、绕过风控、转运三个环节。以下主要针对与网络相关的前 2 个环节进行原理分析。

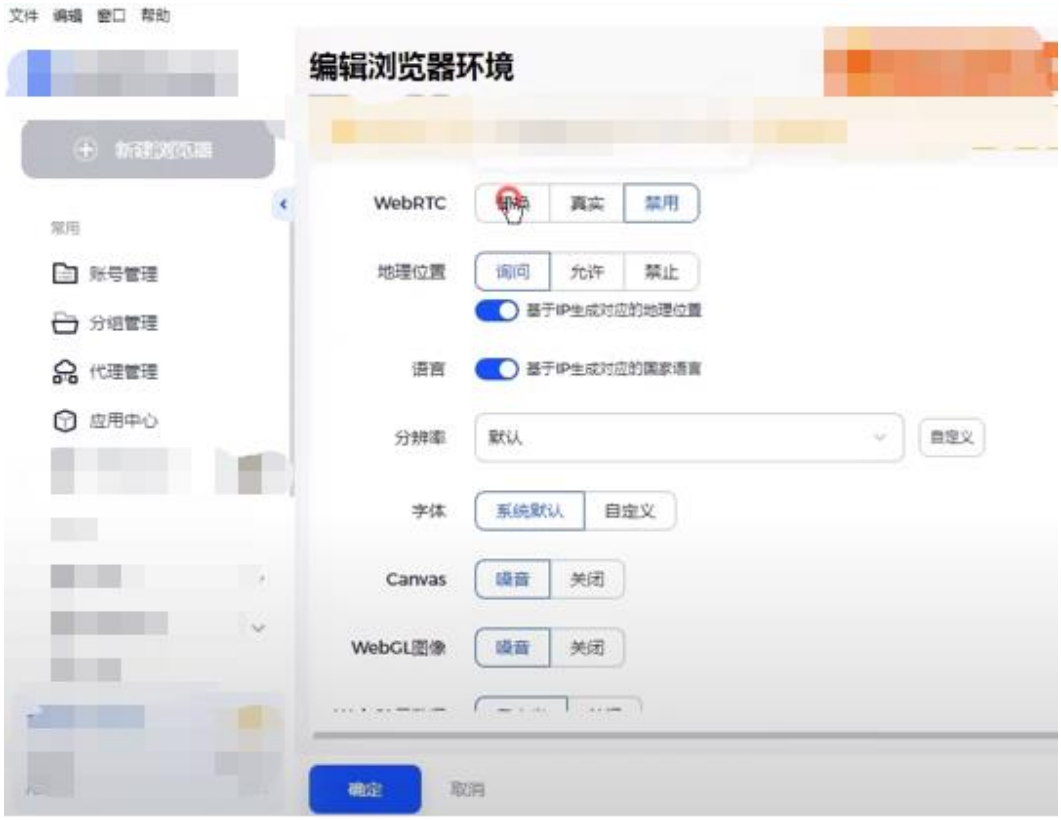


1. 黑产使用 CVV 批量生成、测活技术“清洗”CVV 信息

信用卡 CVV 在黑灰产行业被称为“C 料”，通过钓鱼网站盗取的被称为“鱼料”，根据黑产渠道售卖的 CVV 钓鱼源码来看，其主要是制作假电商网站，投放后诱导受害人点击填写信用卡信息。通过渗透平台获得的信息被称为“库料”、通过信息卡规则批量生成的信息被称为“生成料”。不同信用卡套现平台，对于不同的卡会使用不同的风控策略，同时由于 CVV 料的盗取方式不同，所含有的资料完整度也不相同，故黑产盗刷时会选择相对容易过风控的平台进行套现。一旦发现某些平台风控不严格，会使用卡号生成网站批量 CVV 信息，在正式套现之前也会使用一些 CVV 测试有效性网站进行 CVV 测活。

2. 通过指纹浏览器绕过平台的风控限制

掌握到信用卡信息后，黑产为了绕过平台的风控，使用 IP 代理、指纹浏览器等多种手段来模拟持卡人的行为习惯。根据“料主”的信息，推算持卡人常用的 IP 归属地城市及 IP 的运营商，使用 IP 代理将自身伪装成与卡主相同的城市及相同的运营商宽带。由于在访问网站的过程中，网站会通过浏览器获得设备的时区、屏幕分辨率、语言、字体等信息计算用户的设备指纹，故 CVV 盗刷产业使用如下图展示的指纹浏览器对设备信息进行修改，模仿 CVV 料中的信用卡持卡人的上网环境、IP 位置，再使用环境检测工具检测伪装后的设备信息是否成功。


文件 编辑 窗口 帮助
编辑浏览器环境
常用
账号管理
分组管理
代理管理
应用中心
WebRTC
真实
禁用
地理位置
询问
允许
禁止
基于IP生成对应的地理位置
语言
基于IP生成对应的国家语言
分辨率
默认
自定义
字体
系统默认
自定义
Canvas
噪音
关闭
WebGL图像
噪音
关闭
确定
取消

第四章　热门“诈骗剧本”

一、莫名收到快递，扫码进群后发现是刷单诈骗

今年 3 月用户收到一个快递，打开包装后是一个印有电商平台的平台名称和二维码的杯子，出于对平台活动的信任，用户使用手机扫描杯子上的二维码加入了“免费生活物资”群，在对方的引导下安装名为“*雅”的 APP 参与任务，用户一开始在 APP 中投入 2 万元参与刷单任务，但对方以用户做单错误为由，要求用户再缴纳 2 万元进行项目修复，用户缴纳后，对方又让用户继续充值刷单，用户发觉受骗。

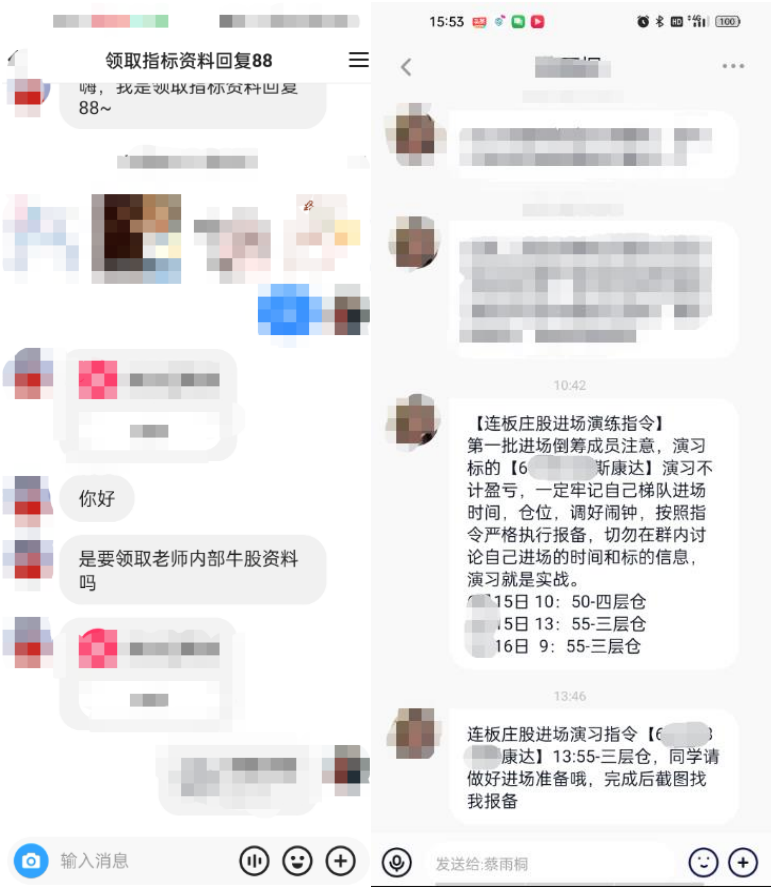
案例解读及安全提示

在收到快递之后，您可能在想是否是最近电商购物后，商家给予的福利奖品，为了感谢对方的好意便按照要求加入了指定的群，但这实际上是诈骗行业在反诈力度加强后，从线上转向线下的一种引流手段，进入指定群后，对方会以参与活动送礼品为由，引导参与对方的刷单任务，前期给予佣金甜头，当不断加大投入后，对方以操作失误等理由要求继续加大投入，即使满足了对方的要求，仍无法提现。收到陌生快递，切记勿贪图小便宜，扫码加群，更不要安装陌生人提供的 APP 安装包。

二、群里炒股的人都赚钱了，自己按照要求投资却无法提现

今年 5 月用户在短视频平台看到有人免费推荐股票，便私信对方，双方沟通后，对方引导用户下载名称为“多*聊”的软件进行深入沟通，并将用户邀请至“多*聊”中的专属投资群，用户在群里观察几日后，发现群里大家都发赚钱截图，便动心想加入，在对方的引荐下

安装了名为“华*券”的应用，通过联系该 APP 中的在线客服，获得充值账号进行充值转账，投资多笔，进行盈利提现时，无法提现，发觉受骗。

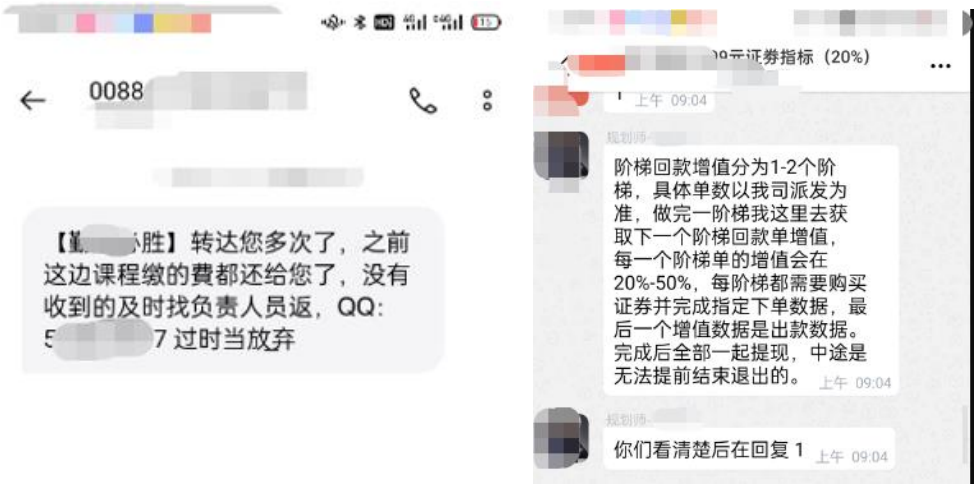


案例解读及安全提示

在这个案例中，不法分子通过短视频传播快、受众多的特点，以赠送牛股资料为幌子，吸引受害人关注，并引导用户使用事前制作的私有化聊天进行深入沟通，在该聊天软件中，不法分子通过炒群的方式，使用提前进群的小号大量发送赚钱信息，增大受害人的关注度和信任度，当受害人开始投注后，给予用户甜头诱导增加投入，最后拒绝用户提现操作。

三、退还买课的费用，却要求在理财平台投资进行返款

今年 6 月用户收到教育清退短信，“【***胜】传达您多次了，先前这边课程交的費都还给您了，没有收到的及时联络工作人员补，QQ：2**3 逾时当放弃”，便联系了短信中的工作人员 QQ，对方表示办理清退需要通过指定的平台购买证券，每次购买返回 20%用于退还买课的费用，用户按照操作后，对方又以用户买错证券，需要再购买 2 次大额证券消除失误记录才能提现为由要求用户继续充值，用户按照要求又多次进行购买但仍无法提现，得知受骗。

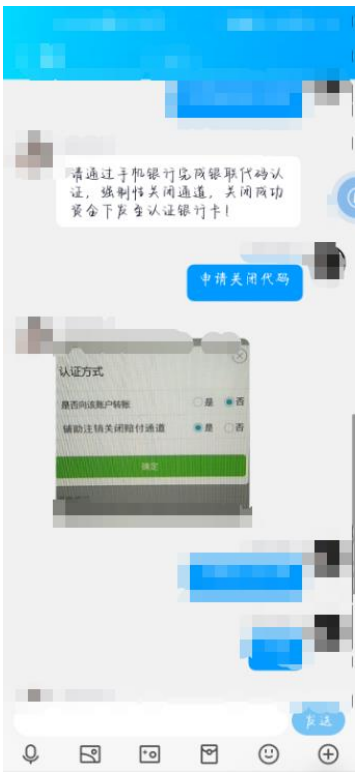


案例解读及安全提示

不法分子通过非法渠道获得教培机构的用户信息，通过短信告知用户之前买的课程可以申请获取信任。待用户上钩后，便以该教培机构的退款服务由第三方机构承接为由，将用户引导至虚假的投资理财平台，给用户安排退款计划，即在该投资平台充值，充值返利当作课程退款，并给用户安排规划师保障用户的投资能够盈利，前期投资过程中给予返款，待用户增大金额后，限制提现。当接收到培训机构称“退款”的短信时，切记要提高警惕，特别是提及需要在第三方平台进行投资返款的。

四、快递损坏进行赔偿，却误打开支付通道，关闭需要向对方转账

今年 6 月，用户收到快递电话，称用户的快递损坏，要给用户进行赔偿，随后双方添加了社交账号，客服以协议用户退款为由，引导用户安装名为“全**”的会议 APP，并开启屏幕共享功能，随后对方称已经赔偿款推给用户的账户中，但用户查询后未收到宣称的款项，对方联系“技术人员”后宣称用户被误打开支付通道，导致退款失败，若不关闭会影响用户的征信，用户在对方的引导下进行转账操作。



案例解读及安全提示

在这个场景中，不法分子冒充快递人员，以用户快递损坏给予赔款为由，吸引用户的信任，并以协议用户进行操作为由，诱导用户安装开启会议类 APP 的屏幕共享功能。“共享屏幕”相当于手机的录屏操作，它会把屏幕上显示的内容实时同步给对方，也就是说你在手机上的任何操作对方都能看到，包括输入银行卡账号、密码、收到的短信验证码等，对方掌握到此些信息后可能在自己无感知的情况下盗刷资金，切勿轻易向陌生人开启屏幕共享功能。

第五章　2023 年上半年度安全数据

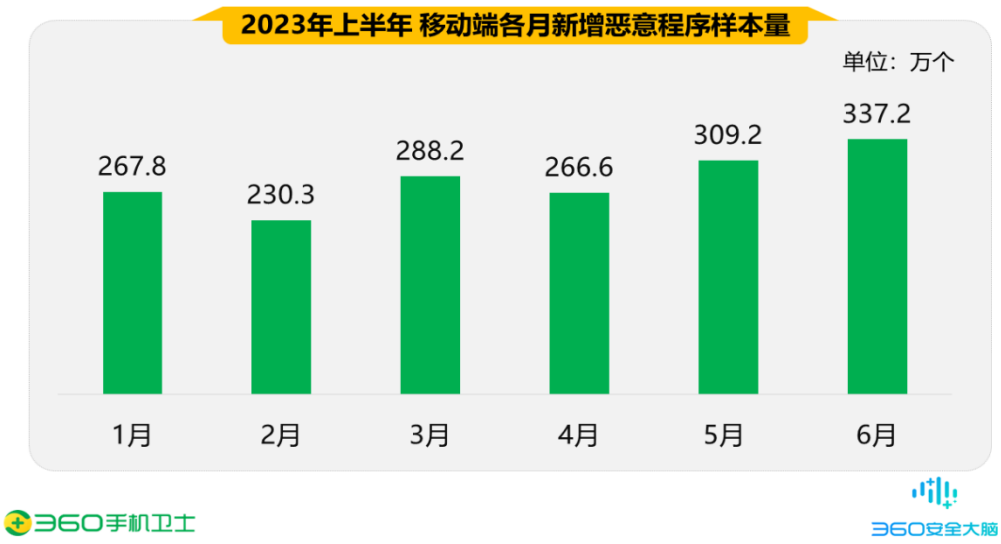
移动终端作为移动互联网的重要组成部分，安全风险形势牵动用户个人信息、财产安全。不法分子通过恶意程序、钓鱼网址、诈骗电话、短信等方式实施诈骗，对人们的日常生活产生恶劣影响的同时，更造成了个人财产的损失和隐私泄露。

2023 年上半年 360 安全大脑不断提升针对移动互联网恶意程序的识别收录能力，截获的移动端新增恶意程序同比有显著提升；同时对于骚扰电话以及垃圾短信的识别拦截量同比也有明显提升。基于自身海量数据进行实时研判，实现事前预警、事中阻断、事后溯源，不断提升黑灰产的诈骗成本，为移动互联网的健康有序发展提供强有力的技术支持。

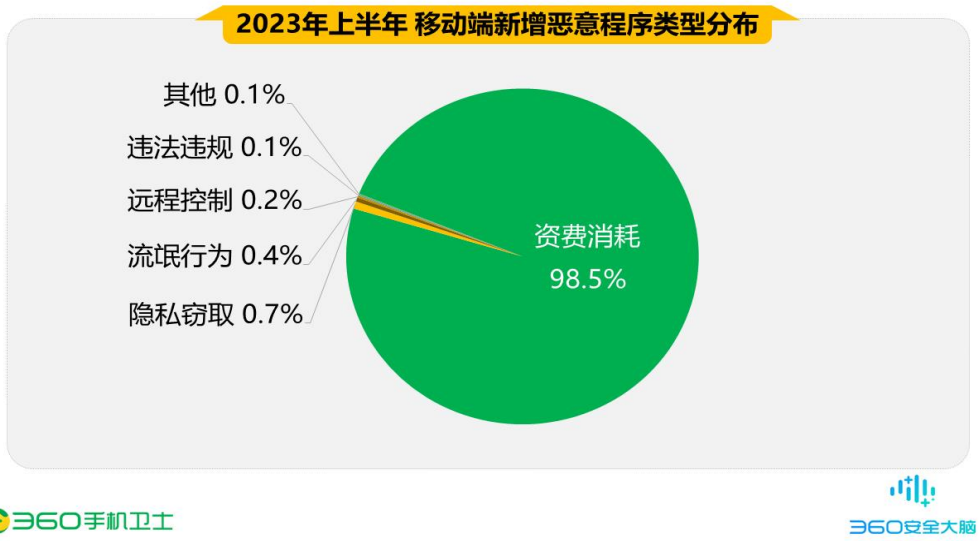
一、 恶意程序

1. 恶意程序新增样本量与类型分布

2023 年上半年度，360 安全大脑共截获移动端新增恶意程序样本约 1699.4 万个，同比 2022 年上半年度（1079.7 万个）上升了 57.4%，平均每天截获新增手机恶意程序样本约 9.4 万个。下图为 2023 年上半年度移动端各月新增恶意程序样本量统计：



2023 年上半年度，移动端新增恶意程序类型主要为资费消耗，占比 98.5%；其次为隐私窃取（0.7%）、流氓行为（0.4%）、远程控制（0.2%）、违法违规（0.1%）、等。下图为 2023 年上半年度移动端新增恶意程序类型分布：

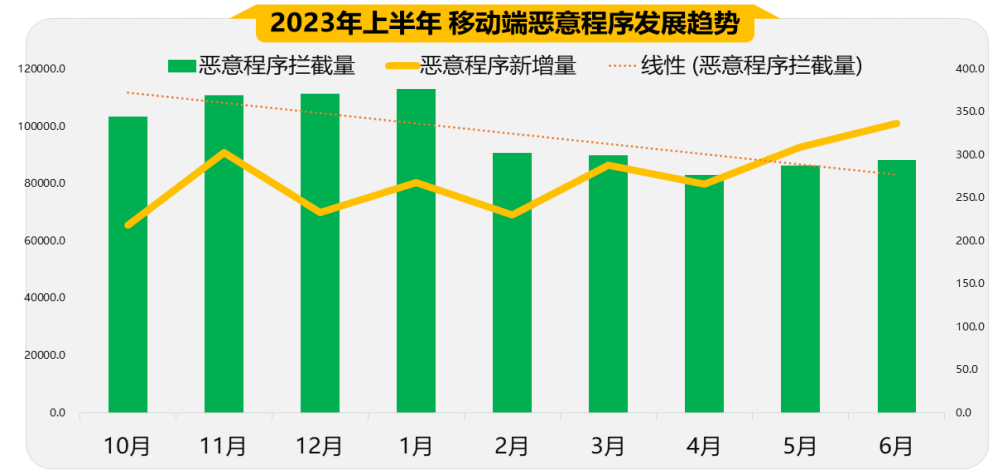


2. 恶意程序拦截量

2023 年上半年度，在 360 安全大脑的支撑下，360 手机卫士累计为全国手机用户拦截恶意程序攻击约 55.1 亿次，平均每天拦截手机恶意程序攻击约 3046.2 万次。下图为 2023 年上半年度移动端各月恶意程序拦截量统计：

3. 恶意程序发展趋势分析

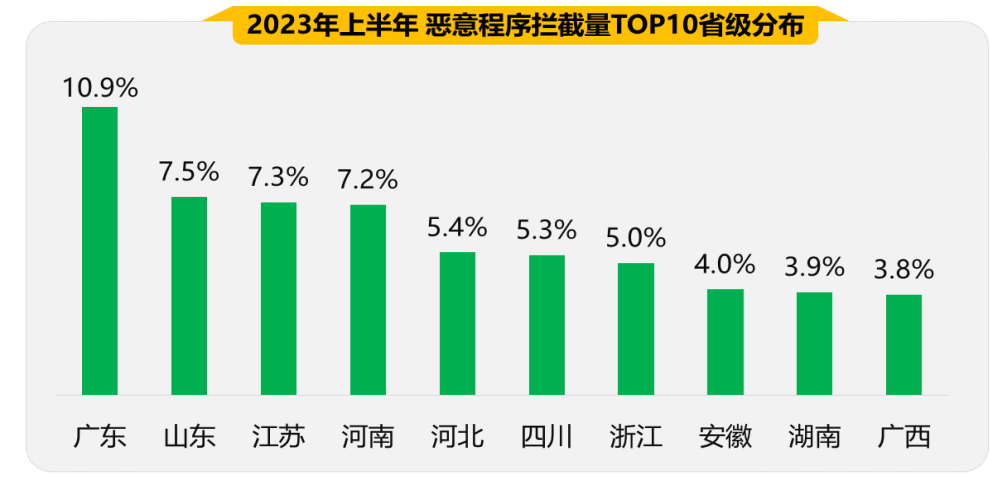
2023 年上半年，恶意程序新增量在稳步上涨，6 月达到最高峰，当月恶意程序新增量为 337.2 万，观察新增样本类型，主要体现在资费消耗类型。



360手机卫士　　单位：万　　360安全大脑

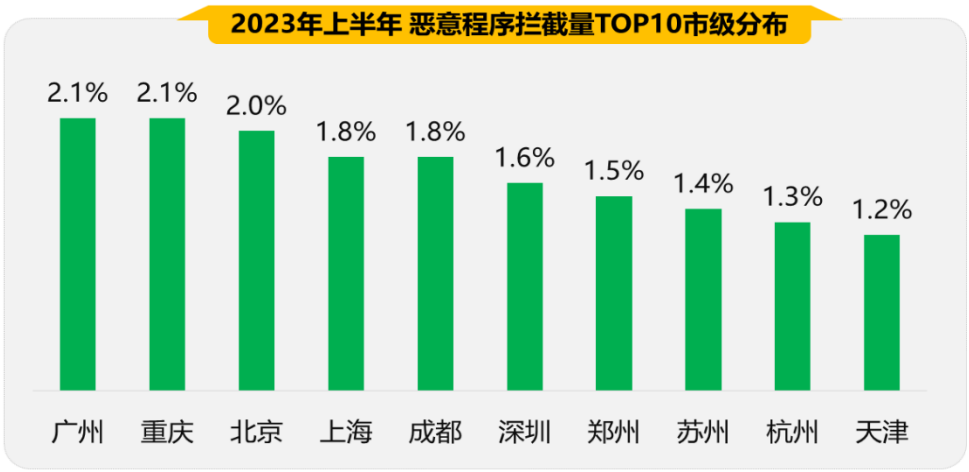
4. 恶意程序拦截量地域分布

2023 年上半年度，从省级分布来看，遭受手机恶意程序攻击最多的地区为广东省，占全国拦截量的 10.9%；其次为山东（7.5%）、江苏（7.3）、河南（7.2%）、河北（5.4%），此外四川、浙江、安徽、湖南、广西的恶意程序拦截量也排在前列。



360手机卫士　　360安全大脑

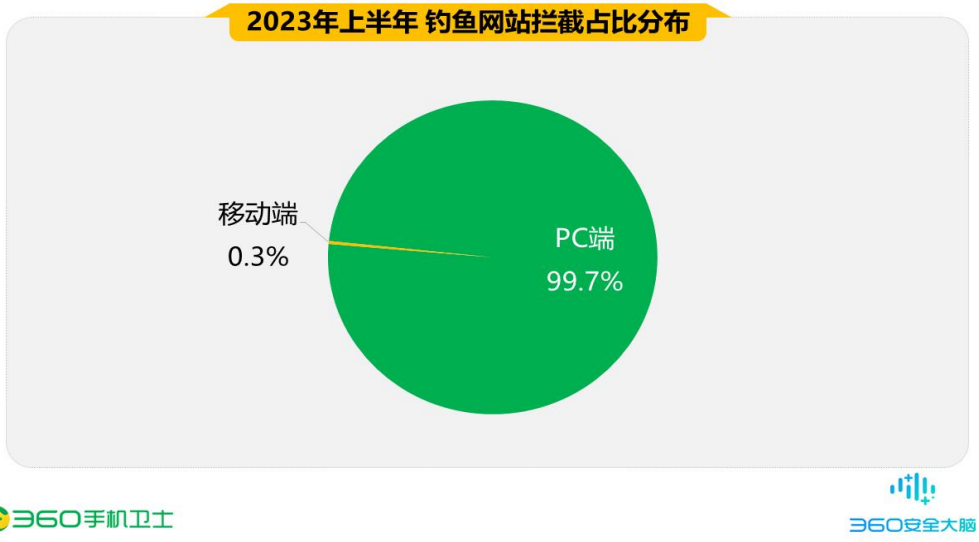
从城市分布来看，遭受手机恶意程序攻击最多的城市为广州市、重庆市，各占全国拦截的 2.1%；其次为北京（2.0%）、上海（1.8%）、成都（1.8%），此外深圳、郑州、苏州、杭州、天津的恶意程序拦截量也排在前列。



二、 钓鱼网站

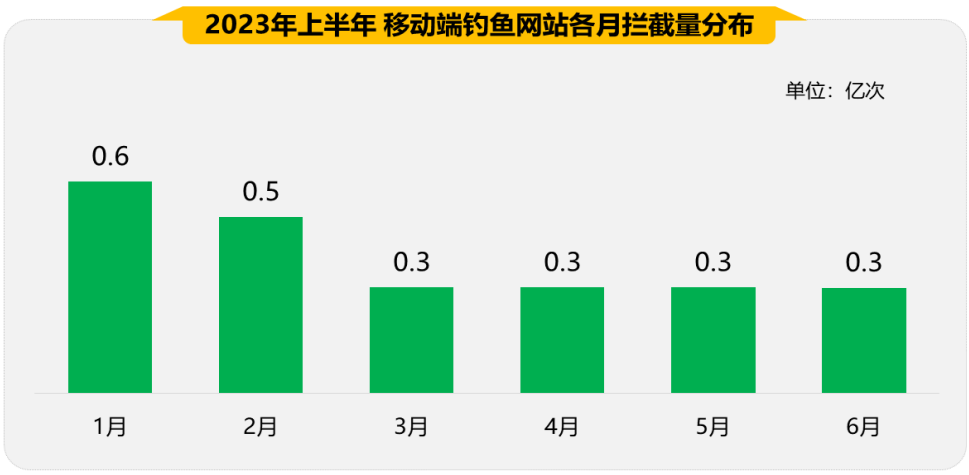
1. 移动端钓鱼网站拦截占比

2023 年上半年度，360 安全大脑在 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 777.5 亿次，同比 2022 年上半年度（399.2 亿次）上升了 94.8%。其中，PC 端拦截量约为 775.2 亿次，占总拦截量的 99.7%，平均每日拦截量约 4.3 亿次；移动端拦截量约为 2.3 亿次，占总拦截量的 0.3%，平均每日拦截量约 128.3 万次。下图为 2023 年上半年度钓鱼网站拦截占比分布：



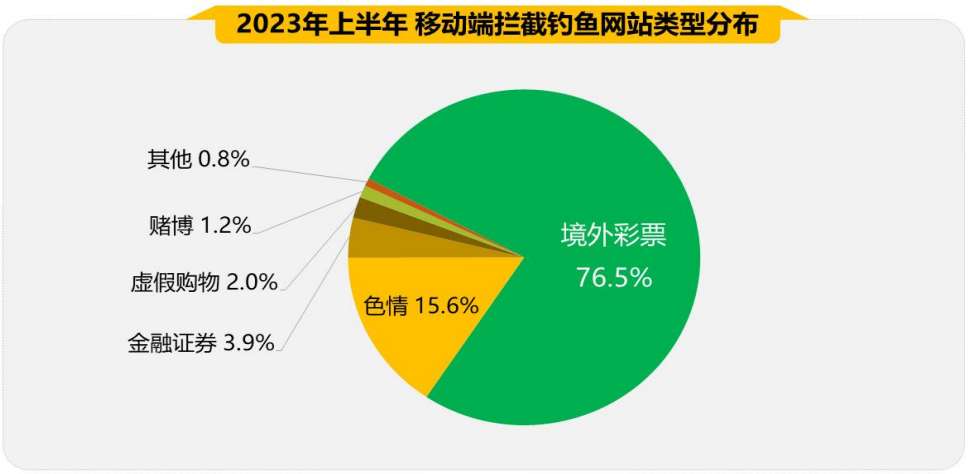
2. 移动端钓鱼网站各月拦截量分布

2023 年上半年度，360 安全大脑在移动端拦截钓鱼网站攻击约为 2.3 亿次，同比 2022 年上半年度（1.7 亿次）上升 35.0%。下图为 2023 年上半年度钓鱼网站各月拦截量分布：



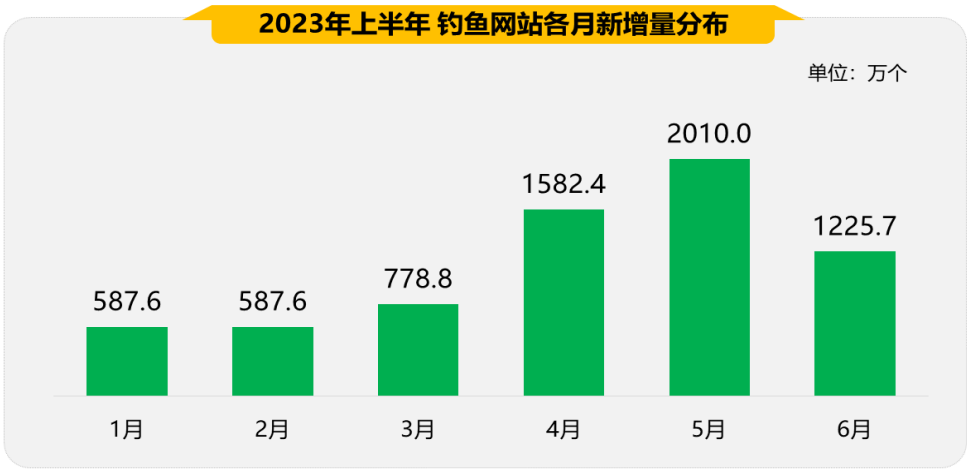
3. 移动端钓鱼网站类型分布

2023 年上半年度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 76.5%；其次为色情（15.6%）、金融证券（3.9%）、虚假购物（2.0%）、赌博（1.2%）等。下图为 2023 年上半年度移动端拦截钓鱼网站类型分布：

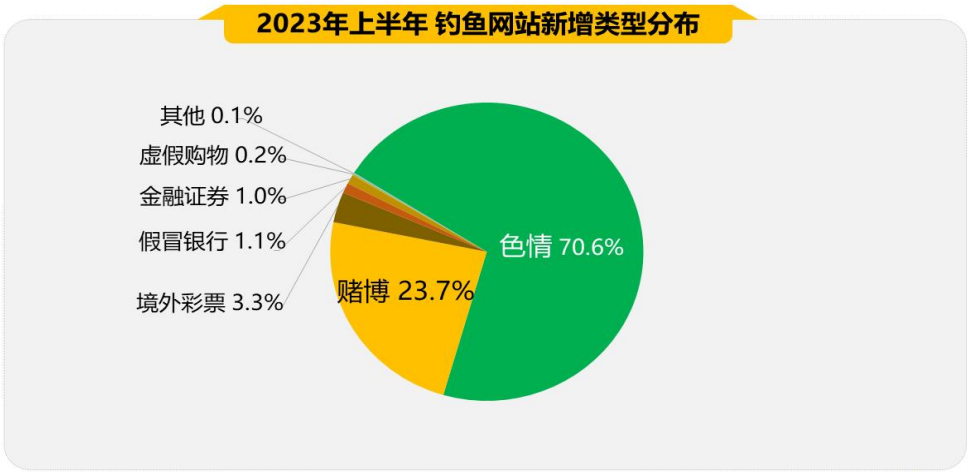


4. 移动端钓鱼网站新增量

2023 年上半年度，360 安全大脑共截获各类新增钓鱼网站 6772.1 万个，同比 2022 年上半年度（6754.5 万个）上升了 0.3%，平均每天新增 37.4 万个。下图为 2023 年上半年度移动端钓鱼网站新增量分布：

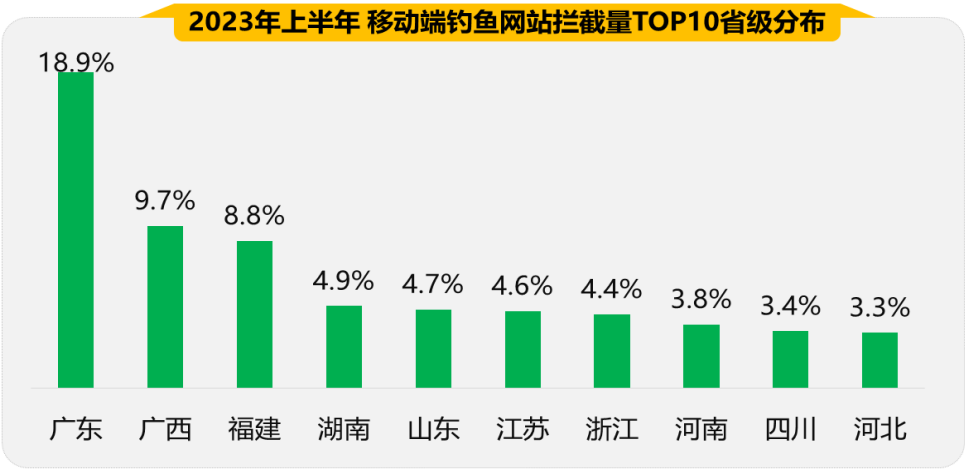


在钓鱼网站新增类型中，色情类占据首位，占比 70.6%；其次为赌博类，占比 23.7%。下图为 2023 年上半年度移动端新增钓鱼网站类型分布：

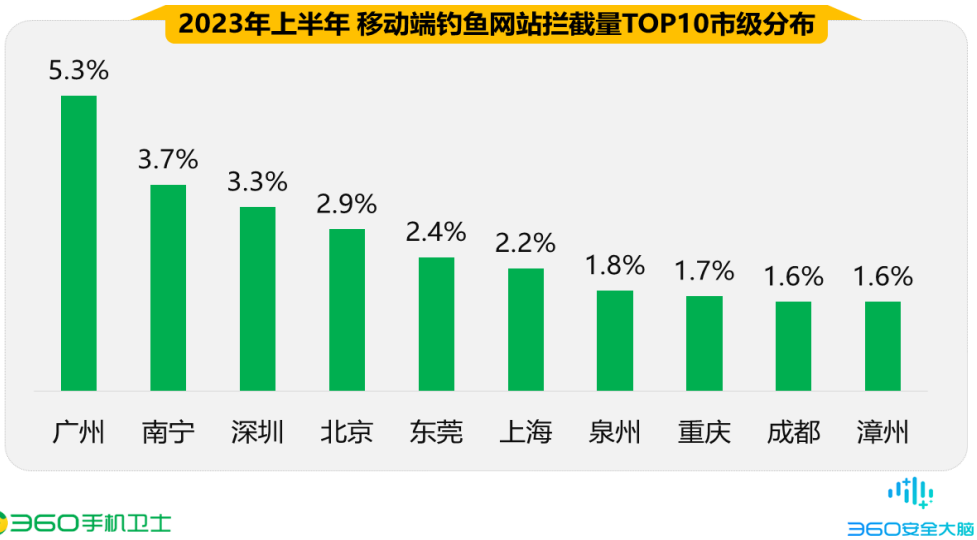


5. 移动端钓鱼网站拦截量地域分布

2023 年上半年度，从省级分布来看，移动端拦截钓鱼网站最多的地区为广东省，占全国拦截量的 18.9%；其次为广西（9.7%）、福建（8.8%）、湖南（4.9%）、山东（4.7%），此外江苏、浙江、河南、四川、河北的钓鱼网站拦截量也排在前列。



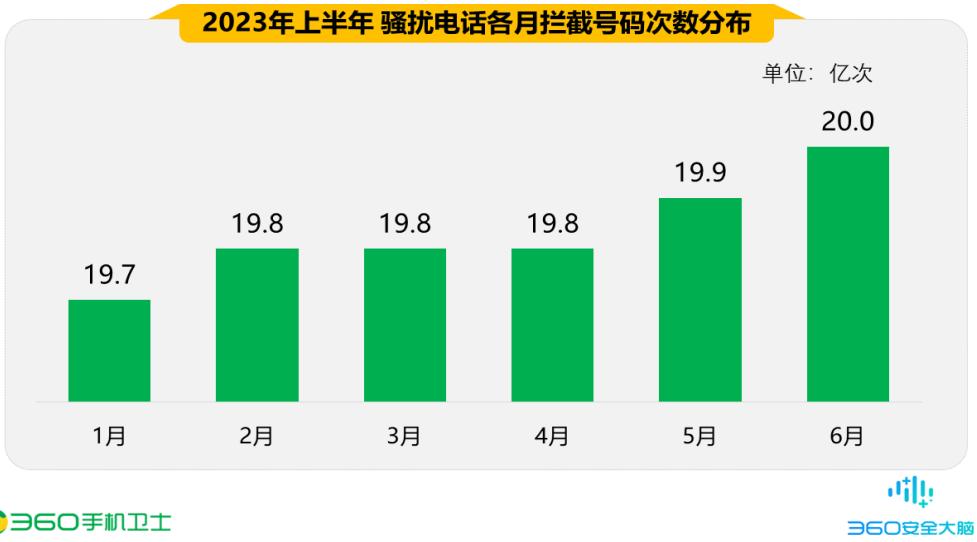
从城市分布来看，移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 5.3%；其次为南宁（3.7%）、深圳（3.3%）、北京（2.9%）、东莞（2.4%），此外上海、泉州、重庆、成都、漳州的钓鱼网站拦截量也排在前列。



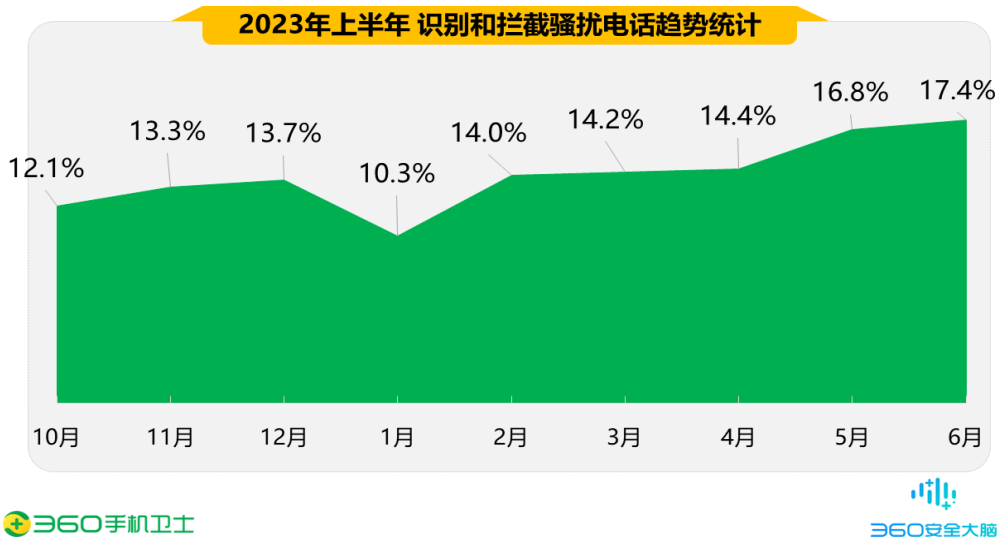
三、 骚扰电话

1. 骚扰电话标记拦截量

2023 年上半年度，结合 360 安全大脑骚扰电话基础数据，360 手机卫士共为全国用户识别和拦截各类骚扰电话约 118.9 亿次，平均每天识别和拦截骚扰电话约 0.7 亿次。同比 2022 年上半年度（116.7 亿次）上升了 1.9%。下图为 2023 年上半年度骚扰电话各月拦截号码次数分布：

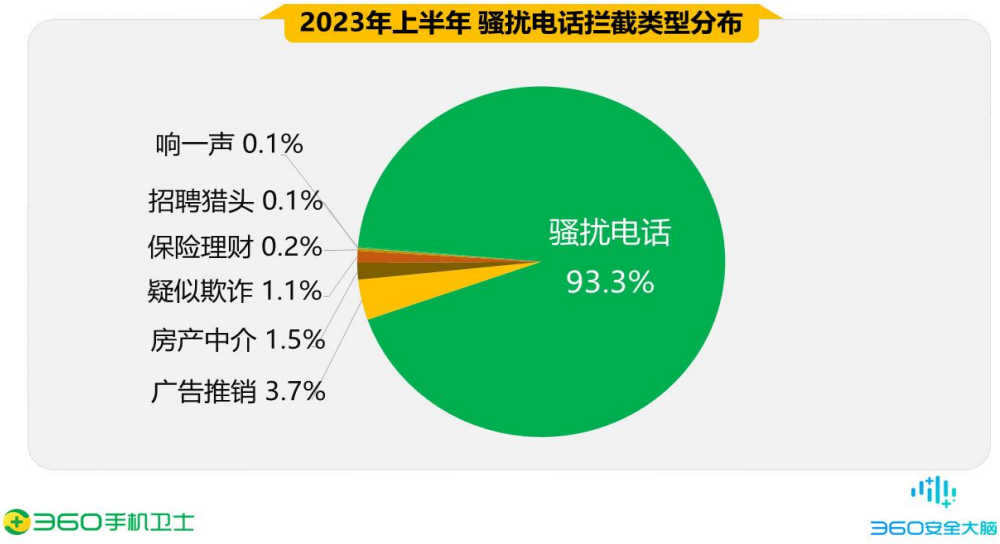


根据各月骚扰电话呼入占比分析，临近年底骚扰电话拦截量呈逐渐降低趋势，2023 年春节期间从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。但从 3 月份起，骚扰电话拦截量回升，持续增加到 6 月。下图为 2023 年上半年度识别与拦截骚扰电话趋势统计：



2. 骚扰电话拦截类型分布

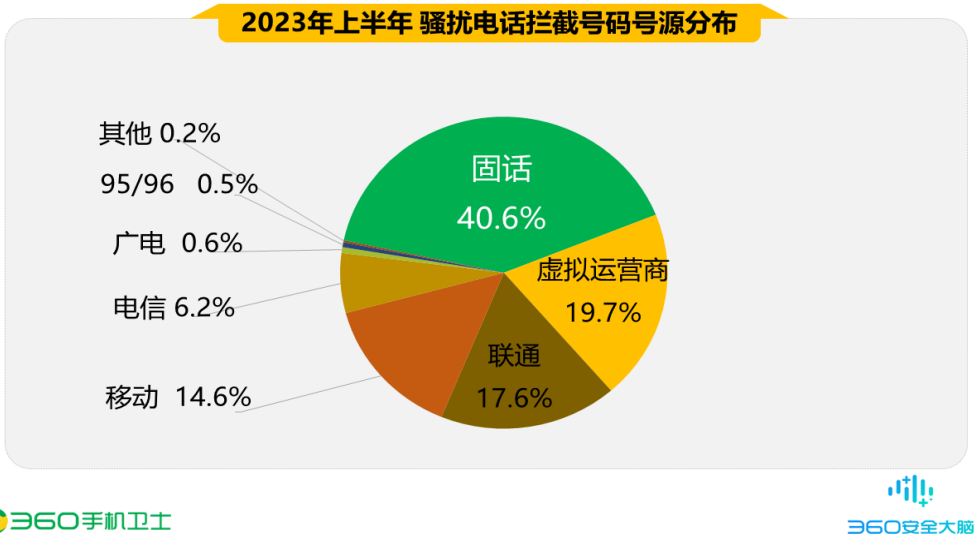
2023 年上半年度，综合 360 安全大脑的拦截监测情况及用户调研分析，从骚扰电话拦截类型来看，骚扰电话以 93.3%的比例高居首位；其次为广告推销（3.7%）、房产中介（1.5%）、疑似欺诈（1.1%）、保险理财（0.2%）、招聘猎头（0.1%）等。下图为 2023 年上半年度骚扰电话拦截类型分布：



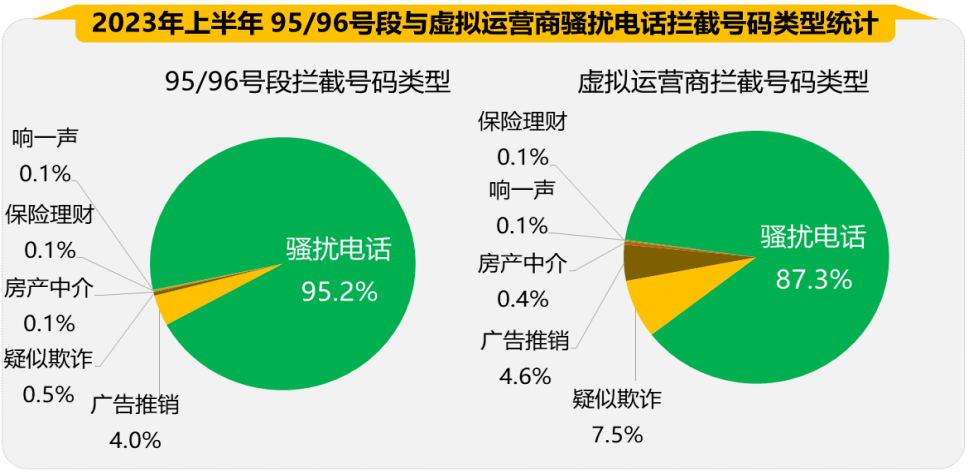
3. 骚扰电话拦截号码号源分布

2023 年上半年度，从骚扰电话拦截号码号源分布来看，被拦截号码为固话的占比最多，高达 40.6%，其次为运营商为虚拟运营商（19.7%）、运营商为中国联通的个人手机号（17.6%）、

运营商为中国移动的个人手机号（14.6%）、运营商为中国电信的个人手机号（6.2%）、运营商为中国广电的个人手机号码（0.6%）、95/96 开头号段（0.5%）等。观察过往骚扰电话以及诈骗电话数据，结合今年的新闻报道，“192”号段可能会成为骚扰电话乃至诈骗电话的新选择。首先新号段放号的资费从成本来看足够便宜，其次新号段在实名制开卡放号过程中，如果存在漏洞，会更有利于黑灰产的隐藏。对于新运营商，我们应该给予运营商更多时间去打击号码滥用行为，遏制黑灰产使用 192 号段的势头。同时 360 作为安全厂商，也一直在履行其职责，持续利用自身的人工智能、多维模型等方式，建立更为准确的号码识别拦截规则，为移动互联网的健康有序发展提供强有力的技术支持。下图为 2023 年上半年度骚扰电话拦截号码号源分布：



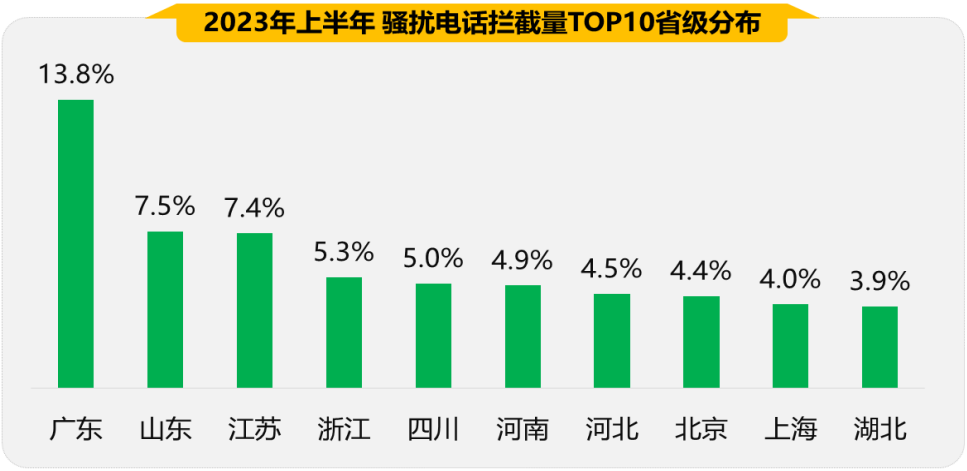
观察 95/96 号段与虚拟运营商骚扰电话拦截号码类型，95/96 号段骚扰电话类占据首位，占比 95.2%；虚拟运营商骚扰电话类占据首位，占比 87.3%；广告推销类分别占比 4.0%与 4.6%，类型比例占据前列。95/96 号段与虚拟运营商号码依然是不法分子从事非法行径的主要“工具”之一。



360手机卫士 360安全大脑

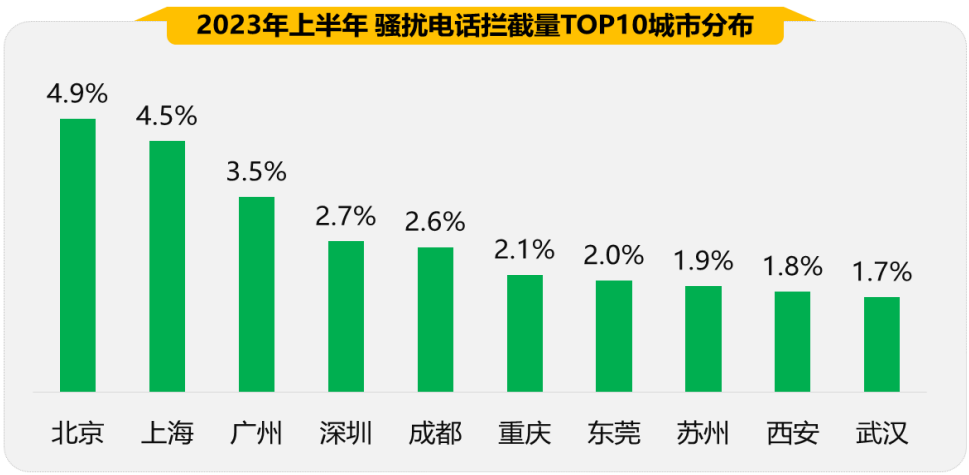
4. 骚扰电话归属地分布

2023 年上半年度，从各地骚扰电话的拦截量上分析，广东省用户接到骚扰电话最多，占全国骚扰电话拦截量的 13.8%；其次是山东（7.5%）、江苏（7.4%）、浙江（5.3%）、四川（5.0%），此外河南、河北、北京、上海、湖北的骚扰电话拦截量也排在前列。



360手机卫士 360安全大脑

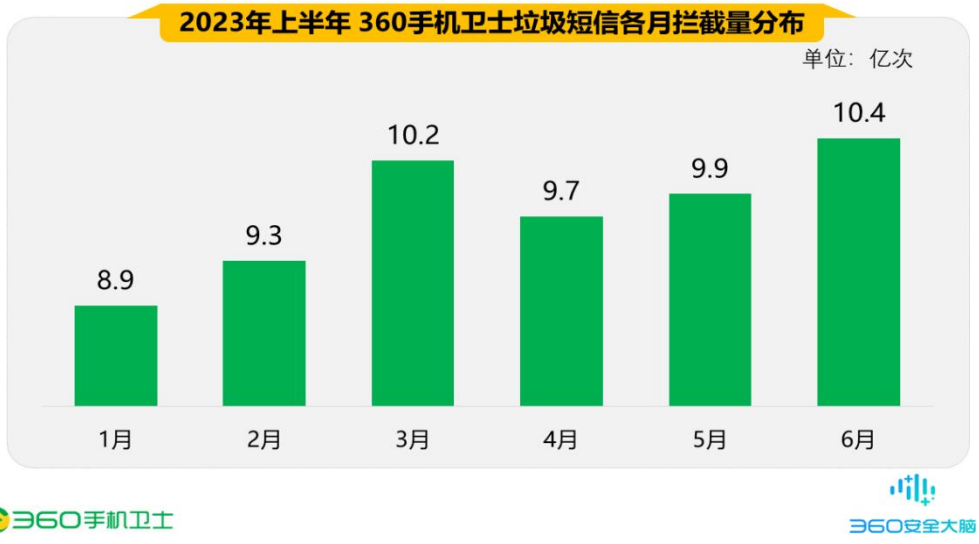
从城市分布来看，北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 4.9%；其次是上海（4.5%）、广州（3.5%）、深圳（2.7%）、成都（2.6%），此外重庆、东莞、苏州、西安、武汉的骚扰电话拦截量也排在前列。



四、 垃圾短信

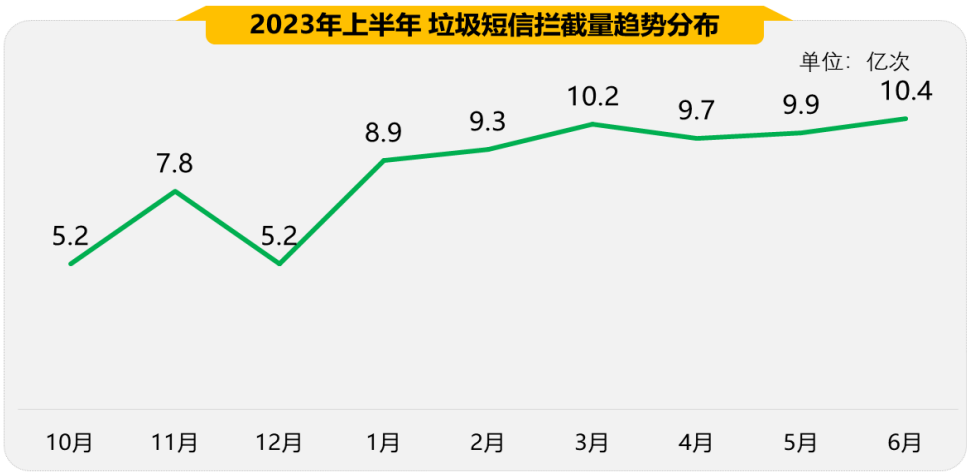
1. 垃圾短信拦截量

2023 年上半年度，在 360 安全大脑的支撑下，360 手机卫士共为全国用户拦截各类垃圾短信约 58.4 亿条，同比 2022 年上半年度（52.3 亿条）上升了 11.6%，平均每日拦截垃圾短信约 3227.5 万条。下图为 2023 年上半年度 360 手机卫士垃圾短信各月拦截量分布：



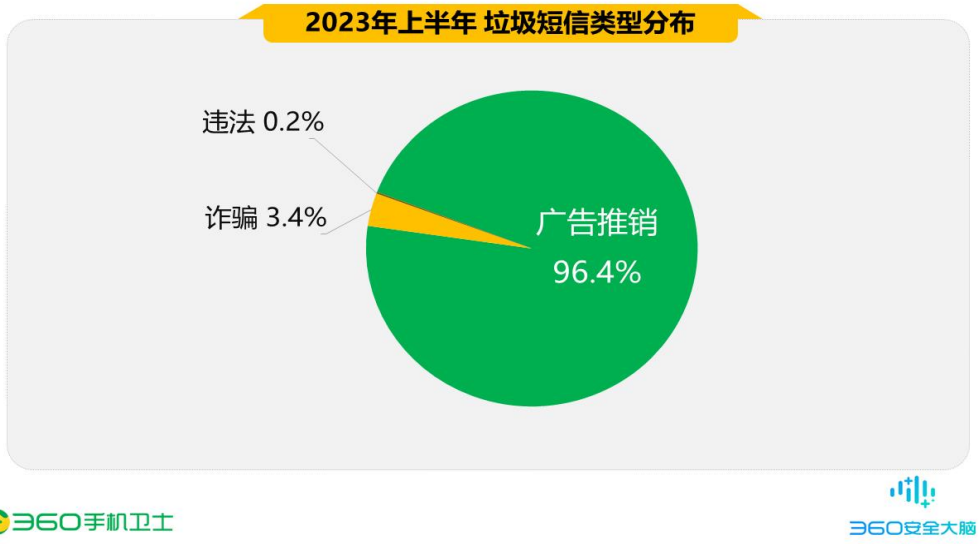
根据垃圾短信拦截量趋势分布，去年第四季度拦截量较低，从今年年初开始，逐步上升。春节期间各类发送垃圾短信的从业人员减少、企业放假休息，各类广告推销类型短信相对上半年整体较少，3 月份逐步回升，6 月由于电商活动短信量级最高。下图为垃圾短信拦截量

趋势分布：



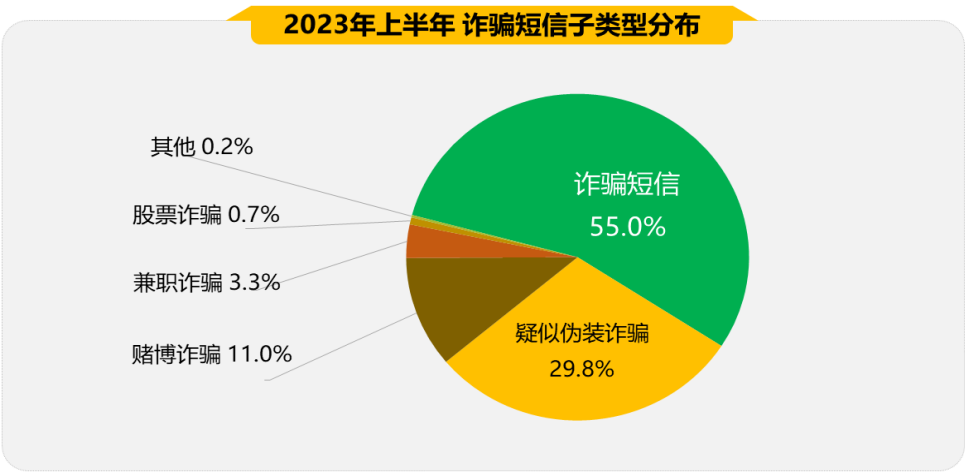
2. 垃圾短信类型分析

2023 年上半年度，垃圾短信的类型分布中广告推销短信最多，占比为 96.4%；诈骗短信占比 3.4%；违法短信占比 0.2%。

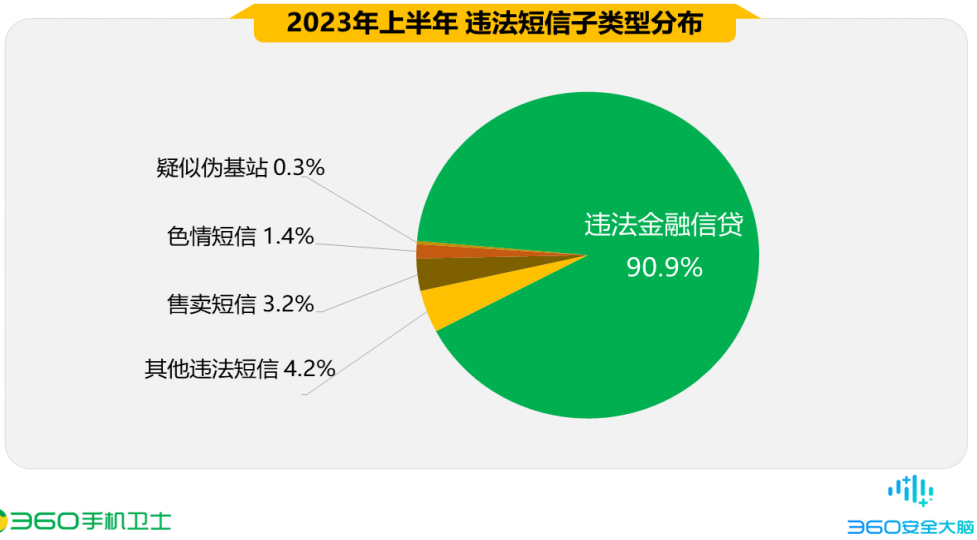


从诈骗短信拦截类型来看，诈骗短信以 55.0%的比例位居首位；其次为疑似伪装诈骗（29.8%）、赌博诈骗（11.0%）、兼职诈骗（3.3%）、股票诈骗（0.7%）等。如今，越来越多的诈骗短信中仅有单一网址，如“2.****.bid”，此类短信内容晦涩难懂，同时域名使用防拦截策略，识别难度大，360 安全大脑一直致力于完善拦截规则，增加黑样本库，优化本地算法模型，提升实时研判垃圾短信新增与变种的能力，提升的垃圾短信拦截量表明垃圾短信

治理依然是一场“持久战”。下图为 2023 年上半年度诈骗短信子类型分布：



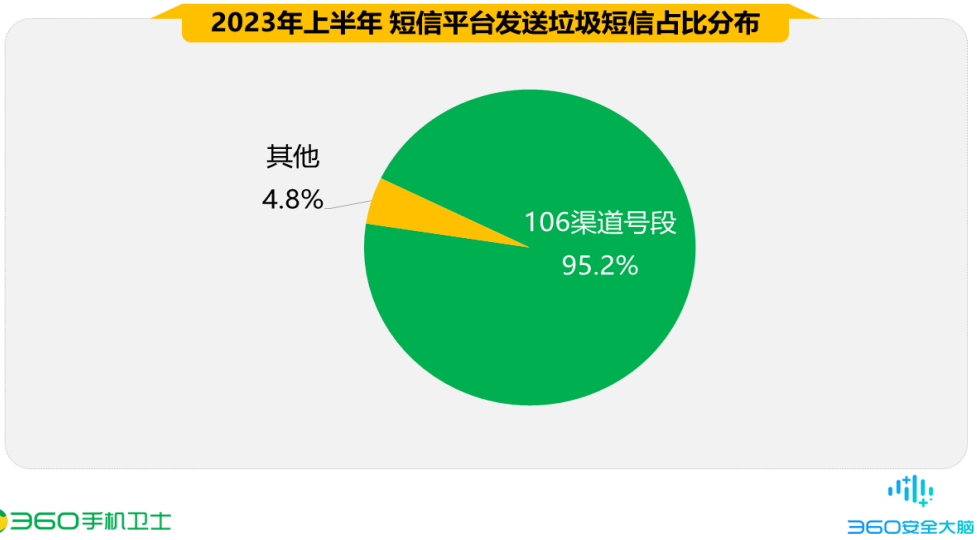
从违法短信拦截类型来看，违法金融信贷短信以 90.9%的比例位居首位；其次为售卖信息（3.2%）、色情短信（1.4%）、疑似伪基站发送（0.3%）等。下图为 2023 年上半年度违法短信子类型分布：



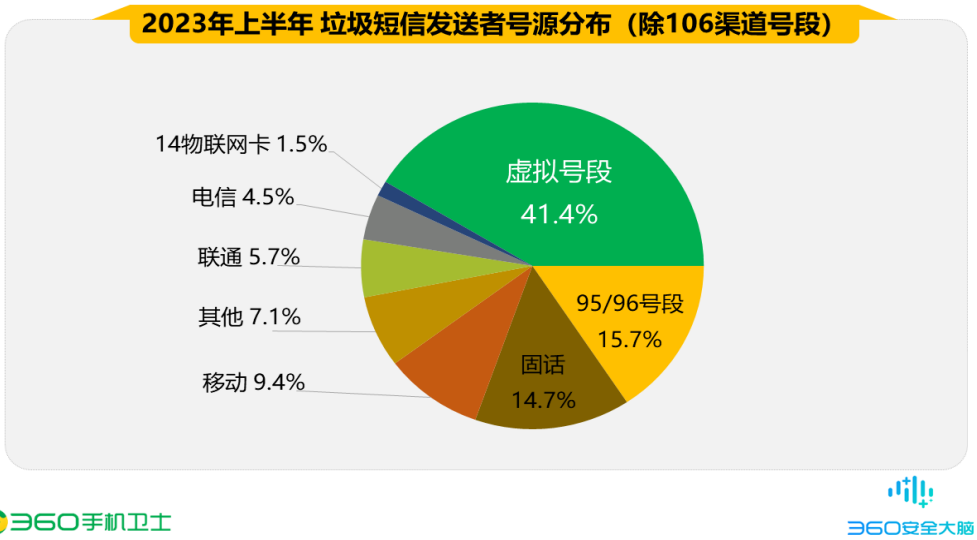
3. 垃圾短信发送者运营商号源分布

2023 年上半年度，短信平台 106 开头号段依然是传播垃圾短信的主要号源，占比高达 95.2%；利用其他号段传播垃圾短信占比约 4.8%。利用短信平台、虚拟运营商传播各类型短信依然是目前的主要途径，发送成本低、传播范围广的特点被黑灰产业利用。同时，诈骗短信越来越“短小精悍”，单一网址让普通用户摸不着头脑，无法识别。虽然针对短信平台传

播垃圾短信的现状持续在打击治理，但发展形势依然严峻。下图为 2023 年上半年度短信平台发送垃圾短信占比分布：



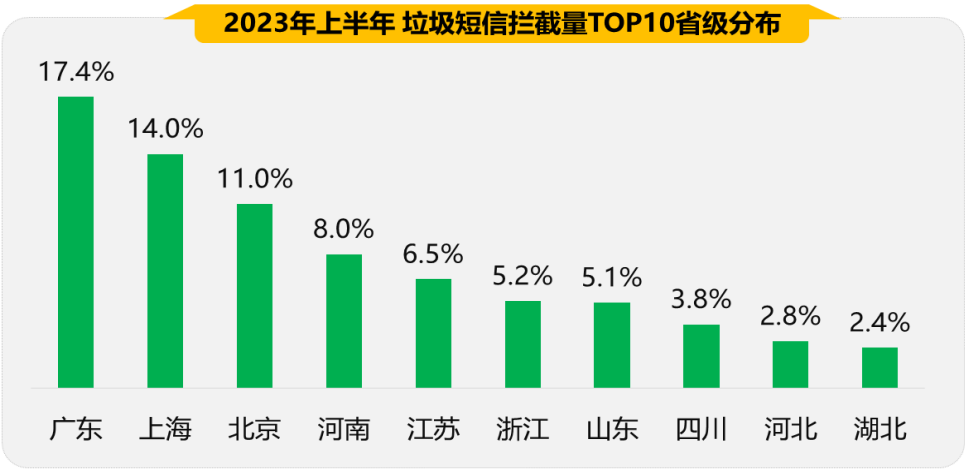
2023 年上半年度，除短信平台 106 开头号段发送垃圾短信外，从其他发送者号码个数分布看，利用虚拟运营商号段发送垃圾短信的最多，占比 41.4%；其次是 95/96 号段（15.7%）、固话（14.7%）、运营商为中国移动的个人手机号（9.4%）、运营商为中国联通的个人手机号（5.7%）、运营商为中国电信的个人手机号（4.5%）、与 14 物联网卡（1.5%）等。



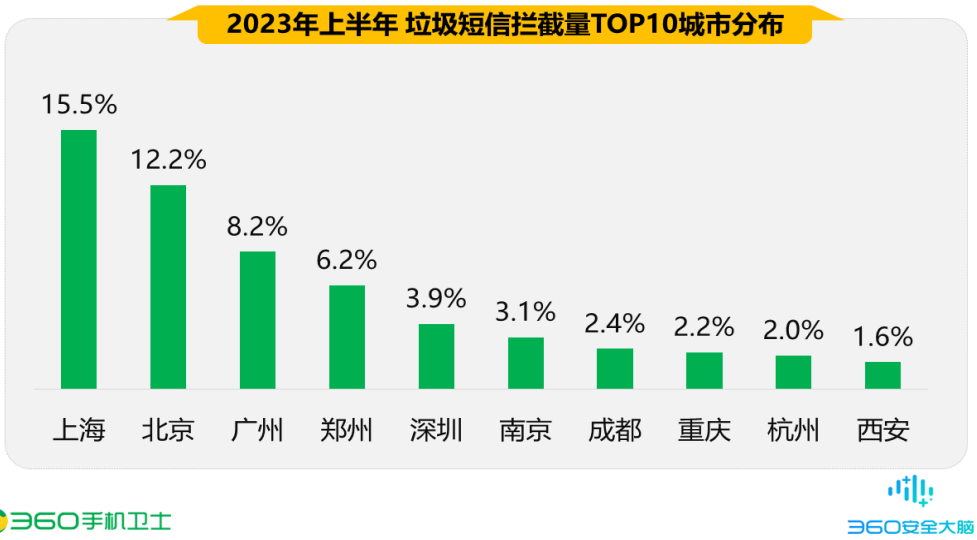
4. 垃圾短信拦截量地域分析

2023 年上半年度，从各地垃圾短信的拦截量上分析，广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的 17.4%；其次是上海（14.0%）、北京（11.0%）、河南（8.0%）、江苏

（6.5%），此外浙江、山东、四川、河北、湖北的垃圾短信拦截量也排在前列。



从城市分布来看，上海市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 15.5%；其次是北京（12.2%）、广州（8.2%）、郑州（6.2%）、深圳（3.9%），此外南京、成都、重庆、杭州、西安的垃圾短信拦截量也排在前列。



第六章 2023 上半年度网络安全行业动态

一、 中宣部公安部联合部署在全国开展“全民反诈在行动”集中宣传月活动

为深入贯彻落实习近平总书记重要指示精神，按照全国打击治理电信网络新型违法犯罪工作电视电话会议部署要求，紧密结合贯彻落实反电信网络诈骗法和中办国办《关于加强打击治理电信网络诈骗违法犯罪工作的意见》，中央宣传部、公安部于 6 月 15 日联合启动“全民反诈在行动”集中宣传月活动，进一步加强反诈宣传力度，不断提升群众防骗意识，切实营造全社会反诈浓厚氛围。

今年宣传月的主题是“预警劝阻别忽视，财产安全要重视”。根据活动安排，各地各部门将在全国范围内组织开展防范电信网络诈骗犯罪“进社区、进农村、进家庭、进学校、进企业”的“五进”活动，着力构建立足社区、覆盖全社会的反诈宣传体系。期间，公安部将组织国家反诈中心发布《2023 版防范电信网络诈骗宣传手册》，部署各地反诈中心深入基层、贴近实际，针对易受骗群体开展有针对性的防范宣传；会同相关行业主管部门督促金融机构、电信业务经营者、互联网服务提供者对本行业从业人员及服务对象深入开展反诈宣传；联合中国老龄协会举办全国老年人防诈反诈知识竞赛；联合教育部启动“反诈宣传进校园”活动，根据高校及中小学生年龄特点，开展反诈知识进课堂、反诈知识竞赛等教育宣传活动；联合中国电影集团在全国农村地区和中小学校园组织反诈优秀影片公益展映活动。同时，主要新闻媒体和新媒体平台将持续推出反诈系列报道，加强社会宣传教育防范，不断扩大宣传范围、提高宣传精度，持续掀起全民反诈、全社会反诈的新热潮。

据了解，2022 年，各地区各部门认真贯彻落实习近平总书记重要指示精神和党中央决策部署，牢固树立以人民为中心的发展思想，坚持“四专两合力”总体思路，全面加强打防管控各项措施，推动打击治理工作不断迈上新台阶。全国公安机关始终坚持依法严打方针，深入开展“云剑”“断卡”“断流”等专项行动，累计侦破案件 46.4 万起，缉捕电信网络诈骗犯罪集团头目和骨干 351 名，推动电信网络诈骗发案连续 17 个月同比下降，狠狠打击了诈骗分子嚣张气焰。各地区各部门密切配合、通力合作，累计拦截诈骗电话 21 亿次、短信 24.2 亿条，处置涉案域名网址 266 万个，紧急拦截涉案资金 3180 余亿元，形成了齐抓共管、群防群治的整体合力，有力维护了人民群众财产安全和合法权益[3]。

二、 打击治理电信网络新型违法犯罪成效明显

全国打击治理电信网络新型违法犯罪工作电视电话会议 5 月 30 日在京召开。从会上获悉，2022 年，各地区各部门认真贯彻落实习近平总书记重要指示精神和党中央决策部署，以前所未有的力度和举措，全面加强“四专两合力”建设，狠抓打击治理电信网络新型违法犯罪各项措施和行业监管主体责任的落实，全社会反诈局面初步形成，依法严打严惩战果丰硕，法律政策不断完善，全年共破案 46.4 万起，缉捕电信网络诈骗犯罪集团头目和骨干 351 名，有力维护了人民群众财产安全和合法权益。

工作中，中央政法委将打击治理电信网络新型违法犯罪工作纳入平安建设考评体系，推动落实属地责任。各级党委和政府牢固树立以人民为中心的发展思想，采取有效措施，狠抓工作落实。各部门坚持齐抓共管、源头治理，密切配合、通力协作，专群结合、发动群众，着力构建全社会反诈工作格局。公安部部署全国公安机关始终保持高压严打态势，全链条重拳打击涉诈犯罪生态系统，统筹开展“云剑”“断卡”“断流”等专项行动，会同国家移民管理局组织开展“斩链”“清源”“利剑”三大战役，会同外交部、最高法、最高检联合部署开展“拔钉”行动，形成了打击涉诈犯罪的强大震慑。同时，各地区各部门坚持打防结合、防范为先，采取一系列综合性防范举措，有效压制案件高发态势，推动电信网络诈骗发案连续 17 个月同比下降。公安部建立分级分类预警劝阻机制，推动“厦门经验”落地生效，累计向各地推送预警指令 2.4 亿条；工信部持续提升行业监测、预警、处置能力，累计拦截诈骗电话 21 亿次、短信 24.2 亿条，处置涉案域名网址 266 万个；中央网信办封堵境外涉诈网址 79.9 万个、IP 地址 3.8 万个；人民银行持续优化涉诈资金查控，协助公安机关紧急拦截涉案资金 3180 余亿元；中宣部、公安部、教育部、财政部等坚持广泛宣传和精准宣传相结合，组织开展“五进”宣传活动，不断提升群众识骗防骗能力。

为深入推进打击治理电信网络新型违法犯罪工作，十三届全国人大常委会第三十六次会议审议通过反电信网络诈骗法，中办国办印发了《关于加强打击治理电信网络诈骗违法犯罪工作的意见》，最高法、最高检、公安部联合制定有关法律指导意见，为打击治理工作提供了强有力的政策保障和法律支撑。各部门坚持系统观念、法治思维，持续深入推进行业监督管理。公安部牵头各有关部门加强统筹督促，对行业整治工作情况实施红黄牌警告通报制度；工信部积极构建反诈标准体系，督促电信企业落实反诈责任；人民银行深入推进涉诈“资金链”治理工作，推出“一键查卡”防范银行账户非法买卖；中央网信办加大网上巡查力度，深入整治有害信息；市场监管总局将“一人多企”“一址多照”纳入通用性企业信用风险分类指标体系，有力挤压了涉诈犯罪生存空间[4]。

三、 工信部：今年上半年拦截涉诈电话 14.2 亿次和涉诈短信 15.1 亿条

中国工业和信息化部新闻发言人、总工程师赵志国 19 日在国务院新闻办公室举行的新闻发布会上表示，工业和信息化部深化垃圾信息和诈骗电话治理，上半年，共拦截垃圾信息超过 90 亿次，拦截涉诈电话 14.2 亿次和涉诈短信 15.1 亿条。

赵志国表示，信息通信与民众利益息息相关。上半年，工业和信息化部多措并举，加快健全行业现代化综合服务体系，着力整治重点问题。加强 APP 重点问题监管，压实应用商店“守门员”责任，公开通报 188 款违规 APP。深化垃圾信息和诈骗电话治理，上半年，共拦截垃圾信息超过 90 亿次，拦截涉诈电话 14.2 亿次和涉诈短信 15.1 亿条，营造更安全的信息服务环境。

对于下一步重点工作，赵志国表示，要规范引导，营造良好行业生态。细化标准规范，利用应用商店、智能终端等关键环节，加强移动互联网应用全生命周期管理，推动行业上下游协同规范发展。研究制定电信服务合规指南，引导企业突出服务导向，营造让民众放心满意的信息消费环境。

同时，维护用户合法权益。加快移动互联网应用程序公共服务平台建设，建立完善 APP 认证签名体系，高效支撑行业监管和服务行业发展。

赵志国强调，要重点整治用户反映突出的欺骗误导下载、强制自动续费等痛点问题。推广“骚扰电话拒接”服务，强化电信网络诈骗一体化技防手段，进一步筑牢安全防线[5]。

参考文献

[1] 央视网. 公安部：打击侵犯公民个人信息犯罪 近三年破案数连破新高[EB/OL].

https://news.cctv.com/2023/08/10/ARTIgqk2vS5E9OHDG5UY4WzZ230810.shtml，2023/08/10

[2] 人民网.公安部打击电信网络诈骗犯罪集中捣毁电诈犯罪窝点 3300 余个[EB/OL].

http://paper.people.com.cn/rmrb/html/2023-07/04/nw.D110000renmrb_20230704_5-07.htm，2023/07/04

[3] 公安部. 中宣部公安部联合部署在全国开展“全民反诈在行动”集中宣传月活动[EB/OL]

https://www.mps.gov.cn/n2253534/n2253535/c9077841/content.html，2023/06/15

[4] 中国政府网. 打击治理电信网络新型违法犯罪成效明显[EB/OL].

https://www.gov.cn/govweb/lianbo/bumen/202305/content_6883876.htm，2023/05/31

[5] 中国新闻网. 工信部：今年上半年拦截涉诈电话 14.2 亿次和涉诈短信 15.1 亿条 [EB/OL].

https://www.chinanews.com.cn/cj/2023/07-19/10045881.shtml，2023/07/19