2022 年上半年度
中国手机安全状况报告

2022 年 08 月 15 日

前言

近年来，电信网络诈骗已成为发案最多、上升最快、人民群众反映最强烈的犯罪类型，严重侵害人民群众切身利益和财产安全。电信网络诈骗的迅猛发展，庞大的黑灰产业是重要的幕后推手和源头，是案件多发高发、屡打不绝的重要根源。随着打击治理、攻防对抗的不断深入，2022 年上半年电信网络诈骗及其背后的黑灰产业链出现了一些新变化、新特点。

在诈骗话术方面，根据 360 接到的用户举报情况看，出现了以“P2P 清退”、“教育清退”等名义欺骗群众的案例。诈骗分子借助媒体平台发布帖子的便利性及平台本身的“权威性”，误导用户相信“清退”的真实性，从而引导用户在指定的“投资理财平台”投注，骗取资金。

在引流渠道方面，早期时候，由于“GOIP”设备具有人机分离、远程操控、异地拨号通话和支持多张电话卡等特点，大量藏匿在境外的电信网络诈骗团伙通过远程操控的方式，使用搭建在境内的“GOIP”设备向受害人拨打电话。随着公安机关对“GOIP”设备打击力度持续加强，为逃避侦查打击，一些犯罪分子使用音频线、远控 APP、多部手机搭建简易组网 GOIP 设备，成本更低、隐蔽性更强、操作更简单。

在洗钱通道方面，随着“断卡行动”的加强，诈骗分子逐渐减少使用第三方支付、对公账户进行洗钱，转而利用跑分平台加虚拟货币的方式洗钱。通过上半年监测发现，某些诈骗平台甚至直接取消了第三方充值、提现渠道。为增强洗钱能力，在线上博彩产业链中，还形成了以博彩联盟为核心的产业，博彩联盟为博彩平台提供技术、支付通道，博彩网站、色情网站为博彩联盟推广旗下洗钱跑分平台，三者通过押金方式进行约束及佣金结算，逐步增强传播范围及洗钱能力。

在诈骗窝点方面，上半年通过对涉诈网址、应用的攻防手段分析，我们发现了三大黑灰产组织，包括为东南亚线上博彩平台提供技术、支付通道的境外博彩联盟和中国某地区 B**N 集团，以及针对中国大陆企业进行精准邮件钓鱼的缅北魔方 G 团伙。在研判中发现，这些组织是诈骗产业上游技术供应链，危害巨大，但是由于其使用的攻击行为隐蔽在“合法”的行为中，让安全防护、识别难度骤增。

《2022 年上半年度中国手机安全报告》将从电信网络诈骗手法、洗钱方式、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，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，维护用户网络安全。

目录

第一章 2022 年上半年度手机诈骗概况

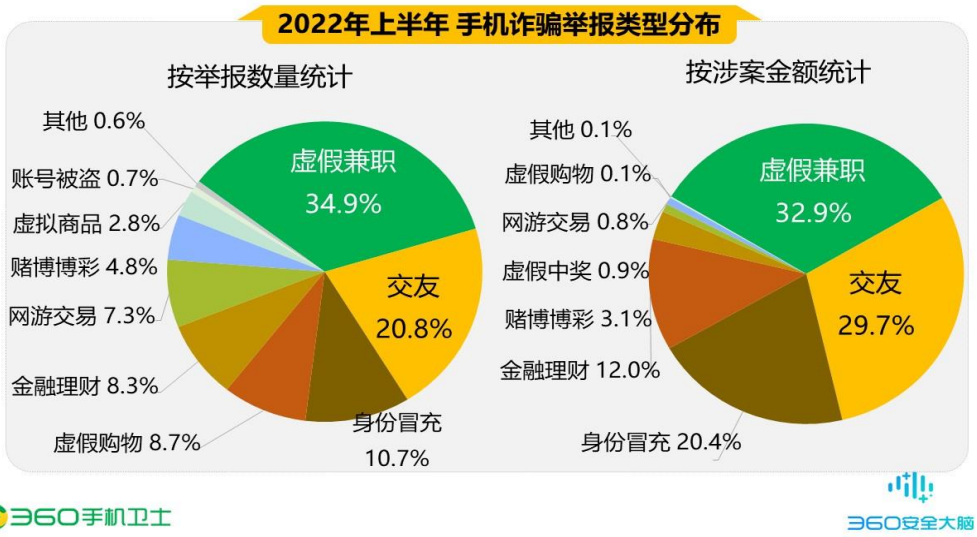
近年来电信网络诈骗逐渐成为发案最多、上升最快、人民群众反映最强烈的犯罪类型，严重侵害人民群众切身利益和财产安全，对此各地区各部门各行业和全国公安机关都在重拳出击，打击治理电信网络诈骗违法犯罪。今年 4 月中共中央办公厅、国务院办公厅印发了《关于加强打击治理电信网络诈骗违法犯罪工作的意见》[1]，致力于推动构建“党委领导、政府主导、部门主责、行业监管、有关方面齐抓共管、社会各界广泛参与”的工作格局，有效提升打击治理能力，坚决遏制电信网络诈骗违法犯罪多发高发态势。

2022 年上半年，360 安全大脑基于用户举报数据分析研究，发现虚假兼职、交友、身份冒充仍是手机诈骗中的高危诈骗类型，互联网原住民 90、00 后逐渐成为最容易被网络诈骗的“主力军”。

一、 用户举报

1. 报案数量与类型

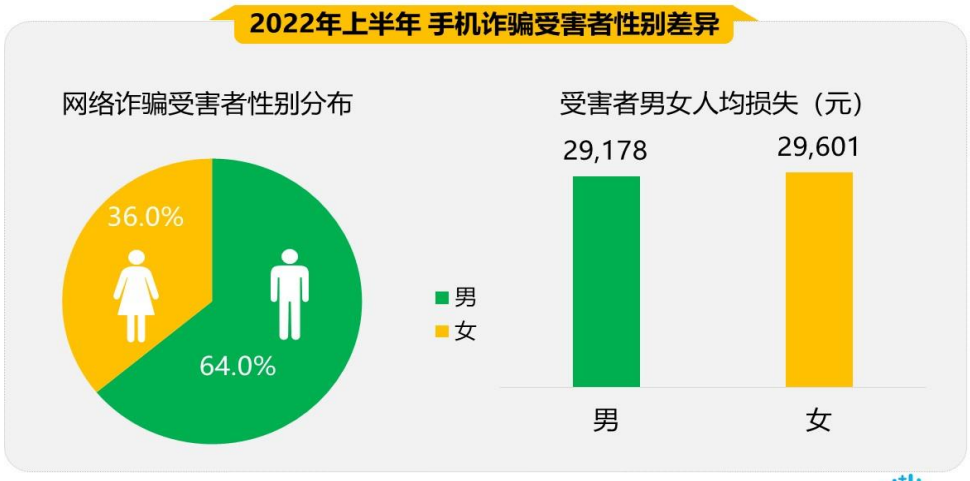
2022 年上半年度 360 反诈赔付保（原手机先赔）共接到 12 类手机诈骗举报，涉案总金额高达 847.6 万元，人均损失 29330 元。在所有诈骗类型中，虚假兼职占比最高达 34.9%；其次是交友（20.8%）、身份冒充（10.7%）、虚假购物（8.7%）、金融理财（8.3%）等。从涉案总金额来看，虚假兼职类诈骗总金额最高，高达 278.8 万元，占比 32.9%；其次是交友诈骗，涉案总金额 251.6 万元，占比 29.7%；身份冒充排第三，涉案总金额为 172.7 万元，占比 20.4%。下图为 2022 年上半年度手机诈骗的举报类型与涉案金额分布情况：



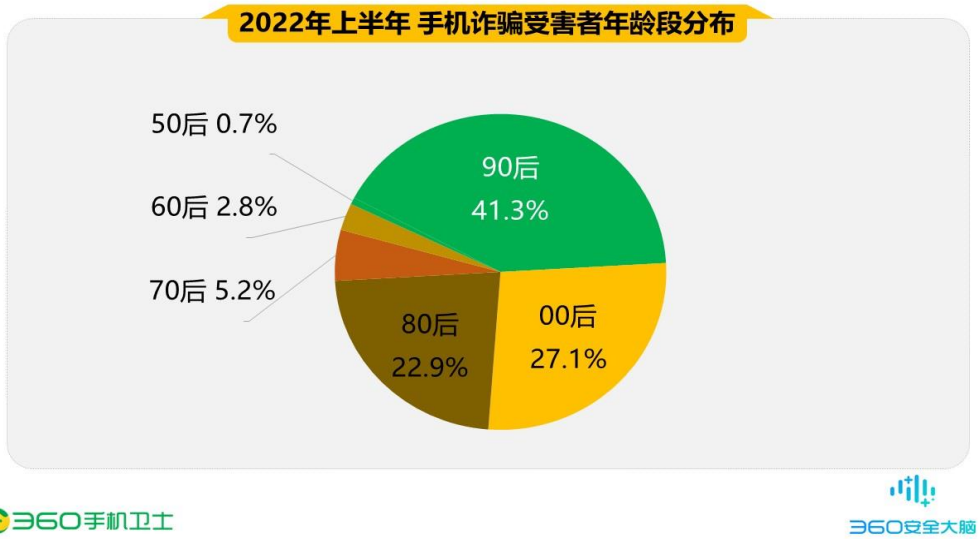
2022 年上半年度，手机诈骗中虚假兼职、交友、身份冒充属于高危诈骗类型，其中，虚假中奖人均损失最高，约 7.5 万元；其次为身份冒充类，人均损失约为 5.6 万元。上半年中虚假兼职类诈骗在数量以及金额上均为最高，相较于传统以“电商刷单返利”为噱头的虚假兼职，今年的兼职更多以包装后的公益项目（博彩）为主，任务速度快，投入成本高，受骗金额高，因此对于受害人来说迷惑性更强，识别难度更大。

2. 受害者性别与年龄

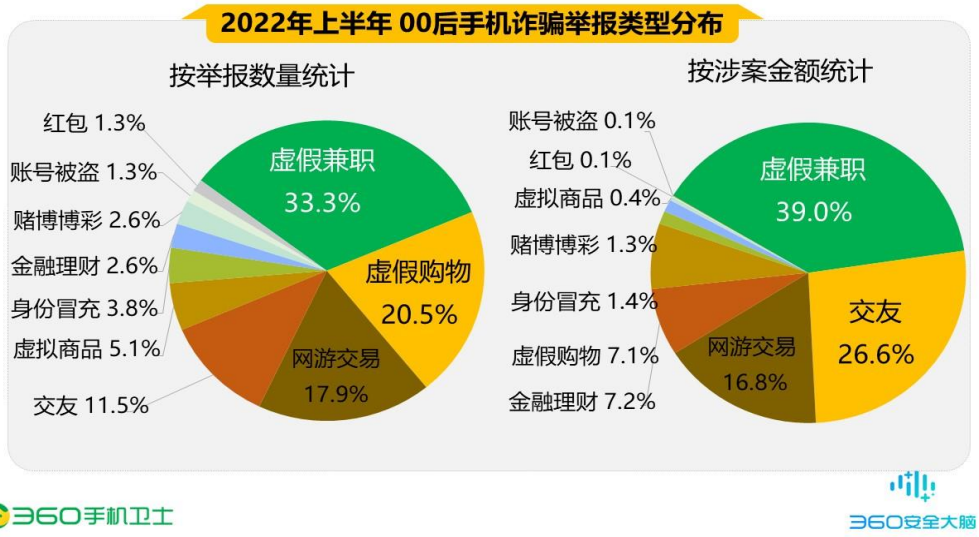
2022 年上半年度，从举报用户的性别差异来看，男性受害者占 64.0%，女性占 36.0%，男性受害者占比高于女性。从人均损失来看，男性为 29178 元，女性为 29601 元，男性人均损失低于女性。下图为 2022 年上半年度手机诈骗受害者性别差异：



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 41.3%，是不法分子从事网络诈骗的主要受众人群；其次是 00 后，占比为 27.1%；80 后占比为 22.9%；70 后占比为 5.2%、60 后占比 2.8%、50 后占比为 0.7%。下图为 2022 年上半年度手机诈骗受害者年龄段分布：

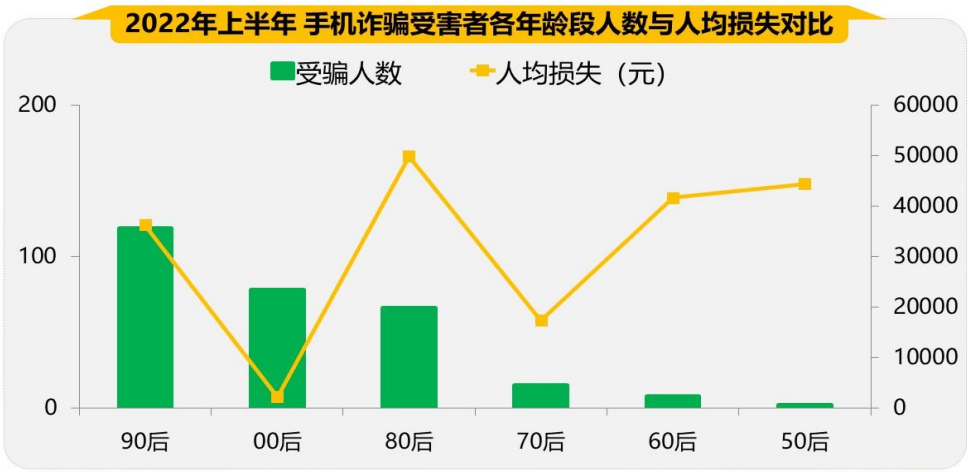


作为互联网原住民的“Z 世代”青年，已逐渐成为最容易被网络诈骗套路的一大群体，诈骗分子正逐步把目标转向熟悉互联网但风险防范意识较差的年轻学生群体。00 后接触网络时间长、深度深，但由于缺少社会经验，对各类网络信息的甄别能力较弱，更容易掉入专业诈骗团伙设置的圈套。虚假兼职类诈骗是他们受骗最多的类型，诈骗分子正是瞄准其初入社会、没有稳定经济来源、想赚钱的心理，诱惑他们步步落入陷阱。



从被骗网民的年龄段人数来看，2022 年上半年度 90 后、00 后、80 后均为诈骗高发人群，受骗类型也以虚假兼职为主。但是实际根据诈骗场景来看，00 后的人均损失明显低于

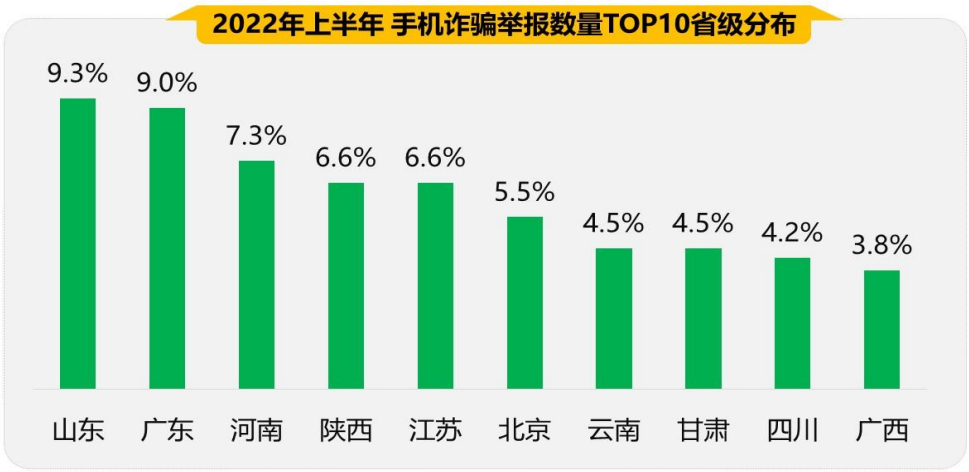
其他人群。因为 90 后、80 后更多遭遇的是前期给予甜头，逐步增加投入的刷单返利性诈骗；而 00 后由于年龄阅历，遭受更多的是兼职保证金诈骗，在缴纳 100-200 元的保证金后，发现无法收益，才醒悟被骗。



360手机卫士　360安全大脑

3. 受害者地域分布

2022 年上半年度，从各地区手机诈骗的举报情况来看，山东（9.3%）、广东（9.0%）、河南（7.3%）、陕西（6.6%）、江苏（6.6%）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 38.8%。下图给出了 2022 年上半年度手机诈骗举报数量最多的 10 个省份：



360手机卫士　360安全大脑

从各城市手机诈骗的举报情况来看，北京（5.5%）、西安（2.8%）、天津（2.1%）、昆明

（2.1%）、盐城（1.4%）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 13.8%。下图给出了 2022 年上半年度手机诈骗举报数量最多的 10 个城市：

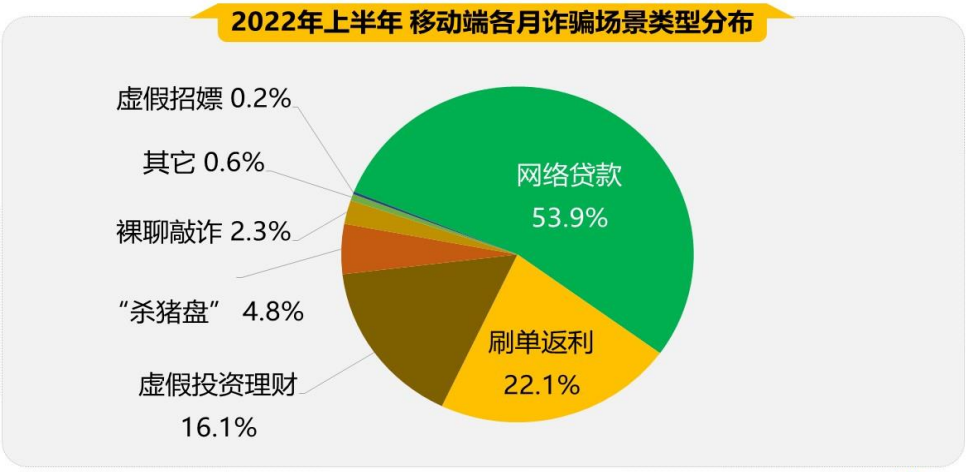
二、 场景识别

1. 移动端诈骗场景感染量与类型分布

2022 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 776.3 万，下图为 2022 年上半年度移动端各月诈骗场景感染量统计：

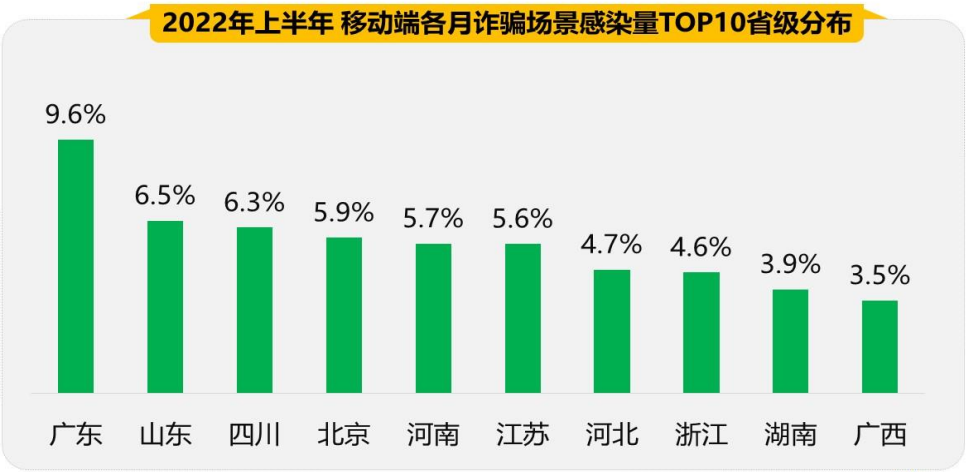
2022 年上半年度，移动端诈骗场景类型主要为网络贷款，占比 53.9%；其次为刷单返利（22.1%）、虚假投资理财（16.1%）、“杀猪盘”（4.8%）、裸聊敲诈（2.3%）和虚假招嫖（0.2%）

等。360 手机卫士安全攻防团队通过对黑灰产近年来的持续研究，发现通联类应用（使用聊天 SDK 框架生成的内嵌诈骗网页的 APP）为刷单返利场景中的主流应用，此类应用具有云控、自有生态、监管难度大等特点，Q2 季度通联应用增加了混淆、加固等攻防对抗手段，360 安全大脑目前对此类应用可以实现独家识别。下图为 2022 年上半年度移动端诈骗场景类型分布：

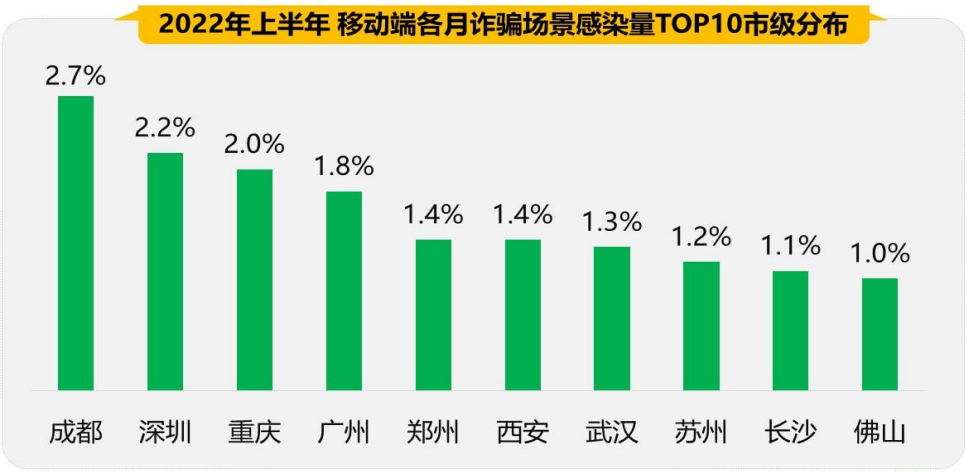


2. 移动端诈骗场景感染量地域分布

2022 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 9.6%；其次为山东（6.5%）、四川（6.3%）、北京（5.9%）、河南（5.7%），此外江苏、河北、浙江、湖南、广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 2.7%；其次为深圳（2.2%）、重庆（2.0%）、广州（1.8%）、郑州（1.4%），此外西安、武汉、苏州、长沙、佛山的诈骗场景感染量也排在前列。



第二章　黑灰产趋势分析

通过上半年的研究发现，黑灰产为了躲避监管打击，在攻防手段上不断进行“更新优化”。在引流渠道方面，从早期使用的“GOIP（多卡宝）”设备逐步向成本更低、隐蔽性更强、操作更简单的简易组网 GOIP 设备“进化”；在洗钱通道上，逐渐减少使用第三方支付、对公账户进行洗钱，转而利用跑分平台加虚拟货币的方式洗钱，导致追溯难度增大。下面将详细分析今年上半年发现的一些趋势变化情况。

一、　黑灰产利用免签、跑分平台、虚拟货币等多种手段洗钱

在黑产链条里，洗钱犯罪与上游犯罪呈链条式发展，存在明显的相互依存关系，特别是对资金流转需求巨大的电信网络诈骗产业。根据 360 手机卫士团队多年研究，电信网络诈骗主要通过虚假兼职、身份冒充、交友敲诈等诈骗场景、话术，利用 GOIP、远程操控、共享屏幕等新技术骗取受害人资金，借助大量银行卡、对公账号等手段进行资金流转，并衍生出用于账户对账的免签技术与第四方支付平台。随着技术对抗的升级，传统的第三方支付、对公账户洗钱占比已减少，转而利用跑分平台加虚拟货币洗钱。如下图所示的黑灰产网站充值入口，已经取消了某宝、某信的充值入口，转而更换为虚拟货币充值的入口，使用的虚拟货币中，主要以 USDT（泰达币）为主。以下将分别对洗钱产业中使用的免签、跑分、虚拟货币进行解读。

图-黑灰产网站充值入口

1. 绕过第三方支付平台接口限制的免签支付

由于非企业用户无法开通某信、某宝接口，在缺乏支付接口的状态下，黑产无法及时将支付订单与支付金额进行匹配，其通过免签 APP 做某信、某宝的支付回调完成订单匹配。免签支付相当于绕过了支付平台的接口开通限制，自己搭建了一套支付接口。此种技术早期主要用于发卡平台（卡盟），随着黑产市场需求的增加，已逐渐被“杀猪盘”、虚假刷单等电信网络诈骗产业所采用，故而在大量的诈骗平台可以看到其收款账户为个人账户形式的二维码。

免签技术主要使用了免签 APP、第四方支付平台，前者用于监控手机通知栏中的某宝、某信的收付款信息，后者用于对接回调及对账。使用者首先将洗钱手机登录的收款（某宝/某信）二维码与第四方支付平台绑定，获得监控端绑定二维码，随后在收款手机端安装带有监听手机通知栏功能的免签 APP，填入监控端二维码完成第四方管理后台与免签 APP 的绑定。当手机收到某宝/某信的收款通知信息后，将信息回传至第四方平台，由第四方平台完成与诈骗平台支付订单的对接，实现支付接口的效果。在对免签产业分析的过程中，还发现其为逃避打击，将免签 APP 安装在云手机中，以实现被控制端 IP 与实际使用者网络分离。

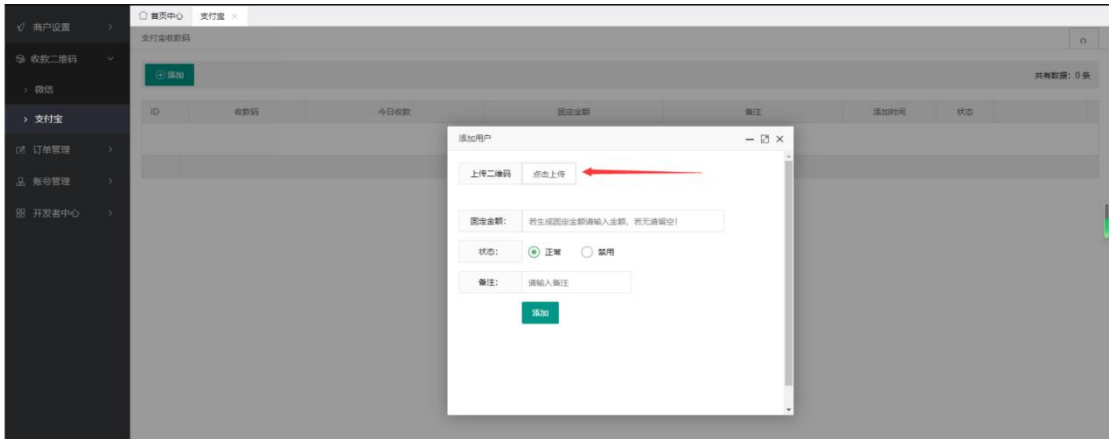


图-第四方平台绑定收款二维码界面

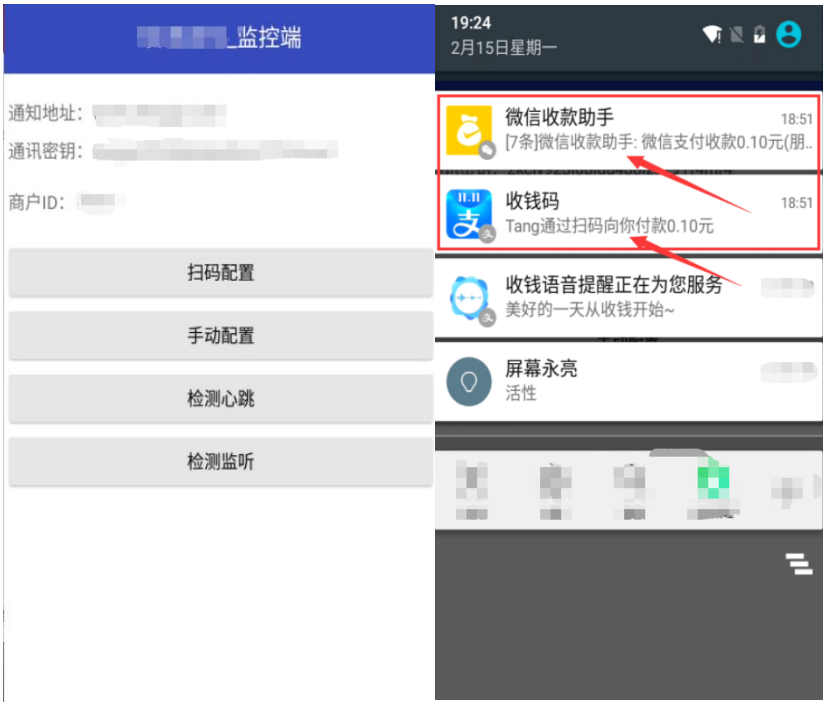


图-免签 APP 界面、收款通知栏

2. 吸纳“公众”收款账户充当洗钱资金池的跑分通道

免签支付一定程度上解决了电信诈骗等黑灰产平台支付通道接口短缺，实现自动化账单对账，但自有资金池搭建存在资金、渠道等行业门槛，同时随着“断卡行动”的持续开展，黑灰产手中的收款账户消失殆尽，难以应对大量黑灰产特别是电信网络诈骗中频繁的账户切换需求。因此黑灰产将目光盯上了涉世未深的学生，通过兼职任务的方式，吸纳学生参与到洗钱流程中，增加其洗钱通道，即众包式跑分。

跑分平台以网赚为名，进行兼职众包，吸引跑分客向跑分平台提供收款二维码/银行卡号，跑分平台再提供给诈骗平台，充当收款账户。诈骗团伙以话术诱导诈骗受害人向该二维码/银行卡号转账后，跑分平台给予跑分客佣金。这个过程中，跑分客的收款账户变成了洗钱通道。利用“白账户”进行涉诈资金的流转，既规避了风控监管，又大大提高转账成功率。跑分平台无需过度担忧洗钱资金池的银行卡被冻结的问题，为后期跑分平台与黑产/诈骗团伙利益分成转账，提供了充足的时间。同时跑分客在跑分平台进行兼职任务时，需缴纳保证金，跑分平台和诈骗平台也不怕跑分客拿钱跑路。由于诈骗受害人的资金流向了跑分客的账户，跑分客的佣金通过其他形式进行变现，执法机关在进行资金流向追溯时，很难发现跑分客上游的跑分平台。

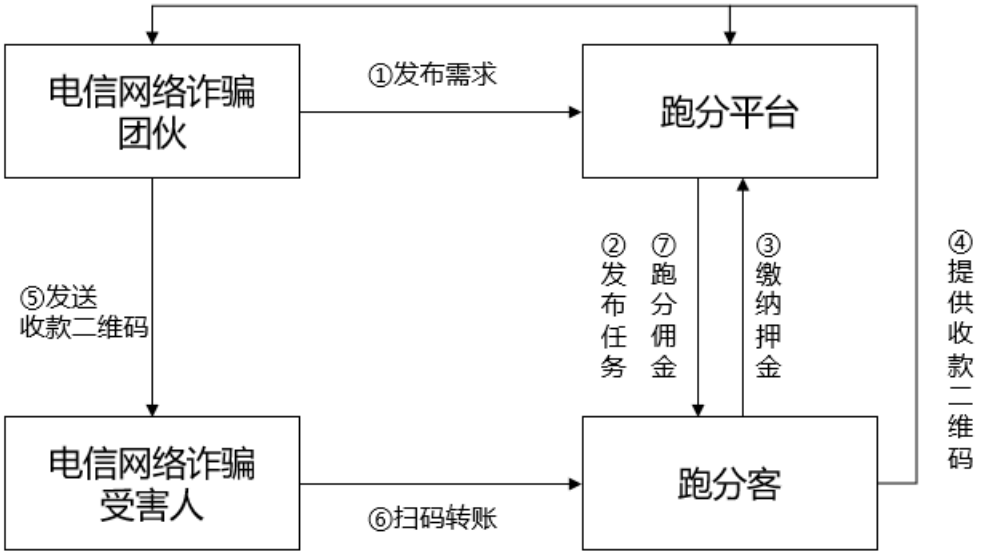


图-跑分流程

部分黑灰团伙为了保证支付渠道的稳定性，不使用公开的源码进行二次修改，而是开发具有自己特点的跑分应用，且应用名称多与订餐、食品相关，提高攻防对抗难度。例如在 2022 年发现的跑分应用“**订餐”，其特点是境外跑分团伙/诈骗团伙使用跑分客的银行账户进行收转款时，该应用可实时将跑分客手机收到的银行短信上传至指定的服务器，无需跑分客进行手动操作，即黑产宣传的跑分方案“一次性交付押金，国内存放手机，全自动化，不需要雇佣人力，更有超高技术保护，无任何技术可以发现你的手机位置”。

图-跑分 APP 界面

```
public static boolean requestShortMessageTest(Context context, int i, String str, String str2) {
    boolean z;
    String charSequence = context.getApplicationInfo().loadLabel(context.getPackageManager()).toString();
    String str3 = ("" + charSequence + "确认短信收发{" + Utils.getRandomString(8) + "}，请将本短信转发至" + str2 + "，5分钟内有效。["
    if (i == 0) {
        z = SmsBox.sendMessage(context, str, str3);
    } else {
        z = SmsBox.sendMessage(context, str, str3, i);
    }
    log.info("fromSlot->" + i + "; toPhoneNumber->" + str + "; backPhoneNumber->" + str2 + "; rc->" + z);
    return z;
```

图-跑分 APP 运行代码逻辑

3. 躲避监管的虚拟货币

早期的跑分产业，由于上游黑产使用某宝、某信、银行卡收款，跑分过程及押金也使用网银、某宝、某信等，存在被风控的风险。随着虚拟货币“隐匿化”优势的显现、稳定币（法币与虚拟货币价值绑定）的兴起，上述涉及的跑分场景（即抢单式跑分）开始采用稳定币。目前稳定币中，以 USDT 为主，即多使用 USDT 进行跑分。与抢单式跑分相伴随的是代买币跑分及传统第四方支付平台升级对接虚拟货币。

由于“断卡行动”及各平台验证手段的升级，诈骗团伙从购买他人支付账户转向直接雇佣他人在虚拟货币交易所认证开户，代买卖虚拟货币，一方面跳过了断卡行动的封堵，另一个方面又避免了虚拟货币交易所的实名制认证机制。

从目前一些诈骗平台使用的虚拟货币入口来看，包含虚拟货币钱包、虚拟货币直转两种方式，在页面点击充值后，可以看出该二维码为虚拟货币收款地址，与早期使用的某信、某宝收款二维码作用相似。通过支付请求的回连地址，发现其背后使用了第四方平台，在原有支付页面展示某信、某宝收款二维码外，增加了虚拟货币收款二维码的展示。同时提供了一键调用 API 接口、一键生成 USDT 钱包、一键自动实现 USDT 充提、一键归集全部地址、一键实名寄售 USDT 等功能，形成一个极其复杂的交易网络，增加了执法机关追查资金的难度。

图-黑灰产网站充值入口展示的收款方式

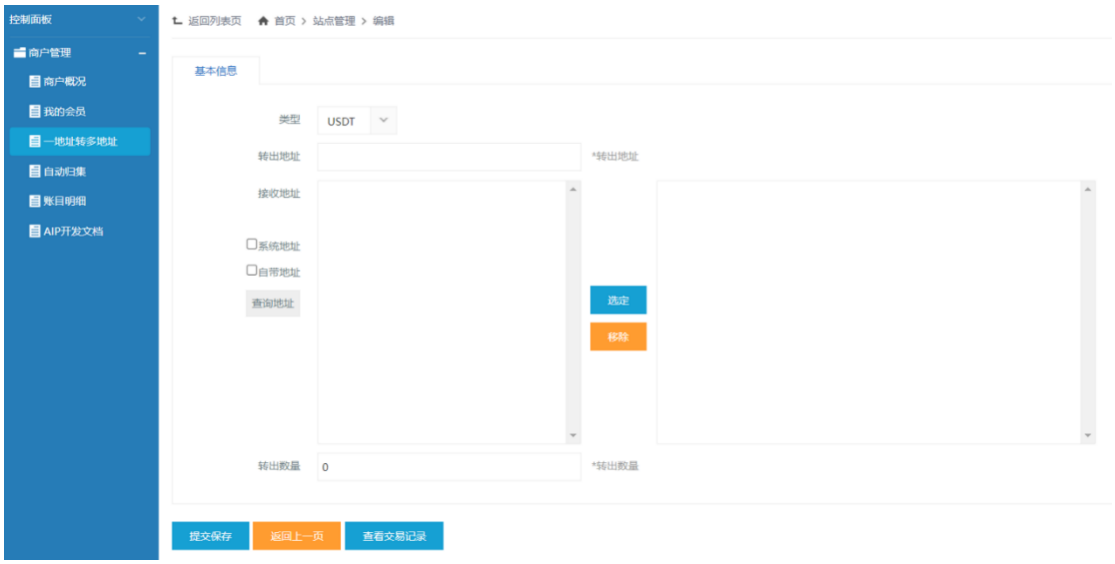


图-升级后的第四方支付平台

二、 移动网络秒拨成黑灰产热门 IP 代理手段

有市场，有需求，就意味着机会丛生。说到“IP”属性的应用场景，早已渗透到我们的生活当中。比如：一个手机号码，只能在平台注册一个账号；网上投票，一个 ID 只能投一票，这里的 ID 的“唯一性”就是平台或者活动方为了保证活动公平性及自身利益，做出的限制。因为在我们看不到的网络世界，诈骗、群控、挂机、“羊毛党”、刷量等黑灰产行为时刻发生着，这些行为从悄然滋生到发展为成熟的产业链，始终绕不开最底层的 IP 支撑。360 手机卫士团队在长期对黑灰产的溯源分析中，发现一些黑灰产使用的 IP 呈现出“境外设备偏爱使用境内固网或 IDC 机房 IP，境内设备偏爱使用境内移动流量 IP”的特点。推测此种偏好方式，境外的黑灰产可能是为了防止其使用的社交账号、支付账号被冻结或满足一定的上网娱乐需求；境内的黑灰产可能是为了防止具体位置信息暴露、提高追溯难度。而这两种身份伪装的方式，代表了目前主流的两种 IP 代理手段，固网 IP 秒拨和移动网络 IP 秒拨，以下将对其进行详细阐述。

1. 固网 IP 秒拨原理及实现方式

由于 IPV4 资源的有限性，国内家用宽带主要是共享 IP，即设备联网时，运营商从 IP 池中分配 1 个 IP 给用户，用户断网时，IP 回收至 IP 池供给其他人使用，即重新拨号，运营商会重新分配 IP。秒拨利用了这种特性，短期内不断重新拨号，此时设备的 IP 就产生了变化，若把多个省市地区的秒拨资源打通，就可实现混拨。

固网秒拨指的是通过自建机房或民用宽带，向外提供代理 IP。2021 年，某地公安机关侦破一起利用“秒拨”网络设备获取电信运营商动态 IP 资源，为境外不法分子提供动态 IP 代理、动态 VPS 服务非法牟利的网络黑产案件。该案件中，不法分子利用了空壳公司，在多个地区设立多个非法机房窝点，国内多起涉赌、涉诈案件线索均指向该公司提供的 IP 资源。

2. 移动网络 IP 秒拨原理及实现方式

移动网络秒拨指的是利用移动网络提供的 IP，向外提供代理 IP。随着攻防对抗的升级，传统固网式的 IP 多已被标记识别，目前黑产将视线转移到更为隐蔽的移动网络 IP 上。从已掌握的情报来看，其实现方式有 4 种：手机热点、USB 上网卡、IP 魔盒、移动 IP 代理软件。其中手机热点、USB 上网卡需要手动断网才能获得新的 IP，存在不足，而 IP 魔盒和移动 IP 代理属于自动化类产物，弥补了手机热点和 USB 上网卡的不足，已渐渐成为主流。

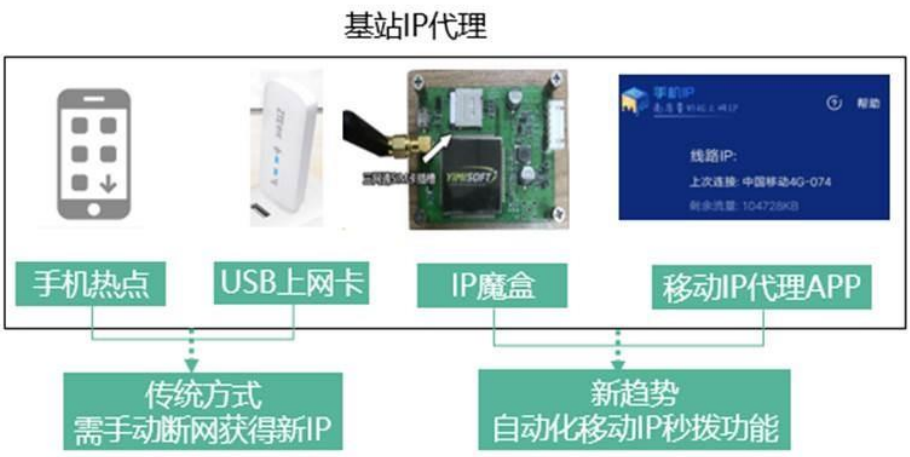


图-代理 IP 方式

USB 上网卡即便携式网络热点，插入手机卡，供电后即可共享网络。这些 USB 上网卡使用的流量业务，主要是一些第三方公司在运营，向运营商采买流量后，分包卖给上网卡用户。

IP 魔盒为一款硬件盒子，支持多种类型的手机卡，接入电脑后可以使电脑拥有移动网络 IP，通过其自带的脚本可实现 IP 自动切换。USB 上网卡、IP 魔盒本质上是同一类产品，两者都可以通过断网再联网实现切换 IP，只是 IP 魔盒增加了自动化秒拨的功能。

除了利用硬件产品实现移动网络秒拨外，目前一些代理软件也提供移动网络 IP，安装此类应用后，可根据其提供的移动网络线路 IP 进行 IP 伪装。利用移动网络秒拨 IP，黑产分子能实现快速变换 IP 或指定 IP 归属地，绕过时间、地域、次数的限制。同时随着 5G 网络的普及，在 5G 高带宽的背景下，黑灰产可能会以此衍生出其他的攻击手段。但从目前已知的风控手段来看，针对移动网络类秒拨 IP 并未迭代出良好的反制手段，IP 伪装攻防对抗将是一场持久战。

图-移动网络秒拨 APP

三、 简易组网 GOIP 手段曝光，人机分离、远程操控

近年来，由于“GOIP 设备”具有人机分离、远程操控、异地拨号通话和支持多张电话卡等特点，大量藏匿在境外的电信网络诈骗团伙通过远程操控的方式，使用搭建在境内的“GOIP 设备”向受害人拨打电话，从而实施诈骗，危害十分严重。随着全国“断卡”行动不断深入，公安机关持续加大对“GOIP 设备”打击力度，打掉了一批违法犯罪团伙，收缴了一批作案工具，有效挤压了相关犯罪生存空间。为逃避侦查打击，一些犯罪分子研发升级出成本更低、隐蔽性更强、操作更简单的新型“简易组网 GOIP”设备，迅速成为各类电信网络诈骗团伙拨打诈骗电话的作案工具。

1. 诈骗电话从“多卡宝”转向简易组网 GOIP

诈骗产业早期，盘踞在境外的诈骗分子，通过境外电话线路直接向境内拨打诈骗电话。由于呼叫过程涉及到国际网关，易被运营商发现，因此诈骗分子开始将号码及呼叫行为迁移至国内。简单来说就是骗子在 A 地（境外），雇佣他人在 B 地（境内）架设猫池、卡池，插入大量的手机卡后，组成 GOIP 设备。骗子在 A 地通过 SIP 类软件，远程调用 B 地架设的 GOIP 设备进行呼叫及短信行为。由于电话的实际呼叫行为从 B 地产生，使用的是 B 地的基站服务，避免了直接从境外向境内呼叫。此种 GOIP 设备特点是通过 sip 协议进行交互，可支持插入大量手机卡，但体积比较庞大，搭建好后移动困难，导致号码在基站下过于积聚容暴露自身的位置。虽后期诈骗分子将 GOIP 设备使用便携式电源搬运至汽车上，全城移动躲

避监管，但由于 sip 协议的存在，仍存在暴露的风险，一种通过远程协助+IM 语音的组合式 GOIP 开始出现。

2. 简易组网 GOIP 原理

为避免从境外直接向国内拨打电话触发国际网关风控限制，使用境内猫池、多卡宝搭建的 GOIP 触发 SIP 协议及聚集风控，诈骗分子将呼叫行为及通话行为分开。境外手机 A 安装远控 APP，控制境内的手机 C 拨打诈骗电话，境外手机 B 安装具有语音聊天的 APP，与境内手机 D 进行语音通话，境内手机 C 与境内手机 D 通过声卡连接线串联，实现 C 与 D 实时共享音频，从而实现手机 B 代替手机 C，与手机 C 所电话呼叫的人员进行实时通话。

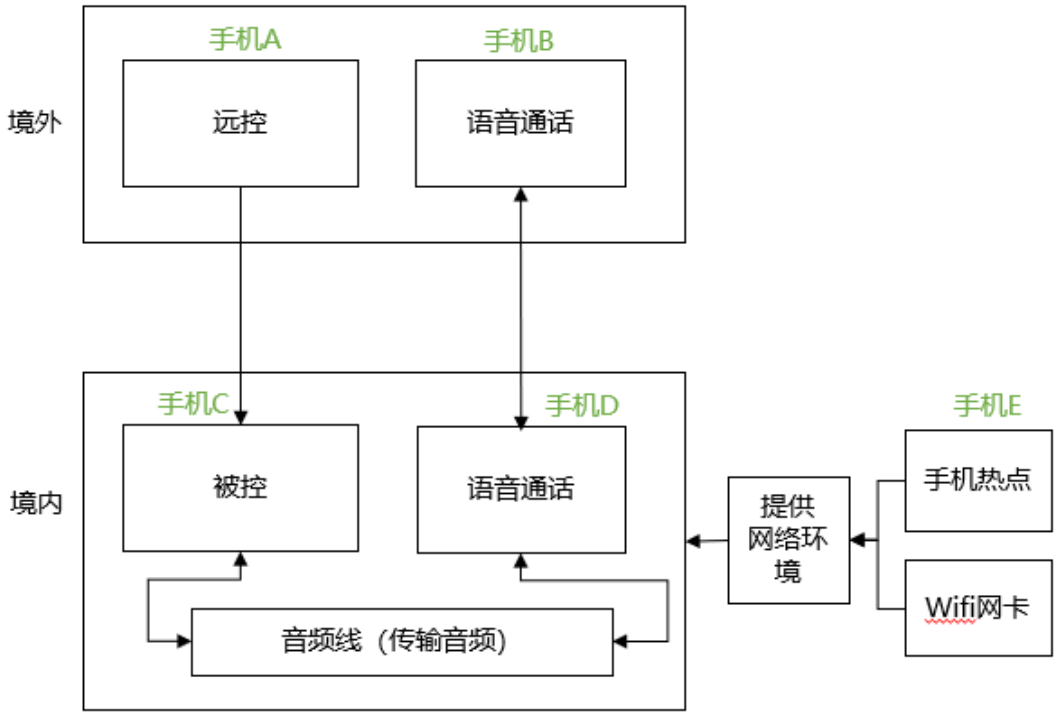


图-简易组网 GOIP 原理

随着生活水平的提高、生活节奏的加快，现如今双持手机成为越来越多追求生活品质的选择，而从简易组网 GOIP 整个环节来看，其本质上也是成对出现的手机，只是语音音频进行了共享，很难将此种形式作为某些风控特征，及时发现潜在的 GOIP。

同时，由于通话语音使用音频线进行了共享，国内 GOIP 的搭建人员无法获悉远程诈骗话务员与受害人的通话内容，保证了 GOIP 运行的稳定性，攻防对抗将是一场持久战。

第三章　黑灰产组织攻击行为揭露

今年上半年，通过对涉诈网址、应用的攻防手段分析，我们发现了三大黑灰产组织，包括为东南亚线上博彩平台提供技术、支付通道的境外博彩联盟和中国某地区 B**N 集团，以及针对中国大陆企业进行精准邮件钓鱼的缅北魔方 G 团伙。这些组织是诈骗产业上游技术供应链，危害巨大，但是由于其使用的攻击行为隐蔽在“合法”的行为中，让安全防护、识别难度骤增。

一、 继包网平台之后，博彩联盟成博彩平台新技术、渠道商

360 手机卫士安全攻防团队在研判一款名为恒*的博彩 APP 时，发现其有别于常见的博彩应用，无注册入口，页面在线客服也不直接提供注册入口，而是引导赌客通过搜索引擎寻找注册入口，根据搜索结果页跳转的博彩导航平台入口进行注册。汇总这些博彩导航页面后发现其页面标题多包含联盟字样，例如多*联盟、凤*联盟，跳转的博彩注册链接含有特定的博彩返点参数。结合博彩平台客服描述的平台无注册入口原因“为保证代理权益，给予代理更好的发展空间，平台客服严禁参与任何开户，所以客服无法提供注册链接。请您**搜索平台关键词进行注册”。推测此类博彩平台背后可能存在一个集博彩平台开发、支付通道、游戏接口、挂机应用、跑分平台、担保中心、色情推广于一身的博彩联盟产业。

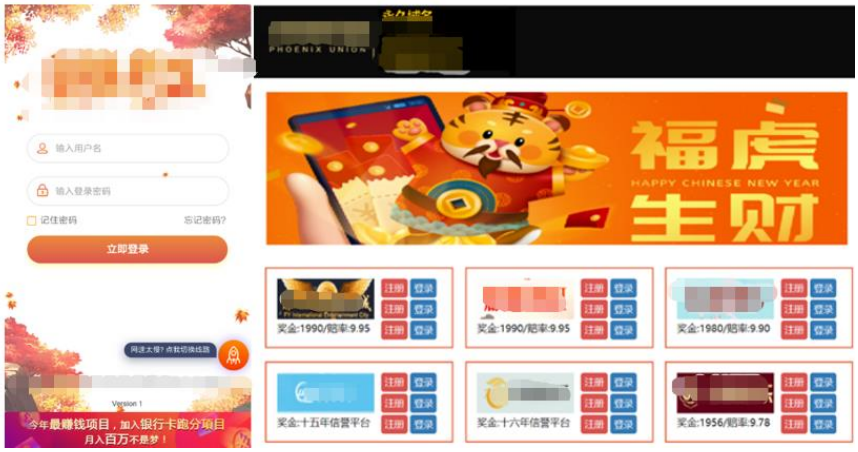


图-博彩联盟 APP 及网站界面

1. 博彩平台隐藏注册入口，通过搜索引擎、色情网站引流

恒*APP 打开后，首先映入眼帘的是界面中的“跑分”关键词，由于没有注册入口，很难将其与博彩平台相关联，会误以为是跑分应用。通过 360 安全大脑对 APP 分析，发现其为封装 WEB 类 APP，并使用了博彩平台常用的 CDN 平台，进一步证实其为博彩类应用。通过其隐

藏的注册入口，注册成功进入页面后，观察到该平台相较于常见的博彩平台，页面除了彩票、真人、棋牌、电竞等博彩板块外，还多了奖源认证和托管跑分。点击页面中的奖源认证，会跳转至多*联盟的会员认证入口，其页面内容介绍“恒*为多*联盟认证钻石级会员，已缴交100 万保证金”，从而让赌客相信赌博平台不会“跑路”。

图-博彩网站首页

点击页面中的犀*、金**富，则跳转至跑分平台，并在页面发现了其使用的三种跑分方案。在对犀*和金*财富的上游引流页分析时，发现其除通过博彩平台引流外，还在色情网站进行引流，且通过色情平台进行赔付承保。

图-黑灰产平台关于跑分项目介绍

2. 博彩平台背后的技术、支付承兑商

在多*联盟的会员功能介绍页面，我们注意到金*正是其旗下的产品。除此之外，还包含*支付、**娱乐、k**棋牌、**挂机、**统计等多种产品，即多*联盟为博彩平台提供了支付接口，博彩平台为多*平台的跑分通道提供引流页面，增强其产业洗钱通道。

图-博彩联盟开发的产品

通过以上的分析，博彩联盟产业主要包含博彩平台、博彩联盟平台、色情网站、赌客/跑分客几个部分。博彩联盟为博彩平台提供技术、支付通道，是整个产业的核心，同时通过博彩网站、色情网站为其推广旗下跑分平台，增强自身的支付通道及洗钱能力。博彩联盟、

博彩平台、推广平台相互间通过押金方式进行约束。赌博平台向多*联盟缴费成为其会员后，多*联盟为赌博平台与赌客之间提供纠纷处理服务；博彩联盟/跑分平台向色情网站缴纳押金，依托色情网站推广跑分平台，色情网站为跑分平台承担纠纷处理服务。博彩平台不直接展示注册入口，通过博彩联盟进行 SEO，或依托博彩代理的推广页拉新，实现双方佣金结算。

二、 以 B**N 集团为攻防技术核心的东南亚博彩产业链

反诈力度的加强，大量涉诈、涉赌网址遭到拦截、封停，诈骗网站的生存空间得以压制，但在今年 6 月，我们监测到部分涉诈、涉赌网站通过专属浏览器的方式跳过域名的拦截策略。深入分析后，发现该攻防浏览器背后产业可能是以中国某地区的 B**N 集团为技术核心，该集团为东南亚博彩集团、“杀猪盘”提供应用定制开发，实现躲避网络安全厂商、执法机构的识别拦截，东南亚博彩集团、诈骗团伙进行平台运营，最终面向中国境内开展博彩、杀猪盘等活动。

图-诈骗网站提供的网址不能访问解决方案

1. 黑灰产攻防浏览器背后的开发者 B**N

在一些博彩网站和杀猪盘网站中，我们发现平台会引导用户下载指定浏览器，以“帮助”用户解决无法访问网址的问题，这些浏览器多宣称“使用了独家线路加速技术，解决无法访问、被劫持、跳转非法网页问题”。推荐的浏览器中，以*宇浏览器以主，也存在部分与博彩平台同名的专属浏览器。相较于传统通过布置多条服务器节点、多个域名，用户手动选择最新未拦截博彩网址的方式，专属浏览器的方式更加的“智能化”，降低了域名被拦截的风险，由于其无痕模式，又增加了取证研判的难度。

*宇浏览器包名为 b**n.mobile.browser，签名证书为 CN=*，OU=b**n，O=b**n，L=t*，ST=t*，C= t*，根据包名、签名关键词，推测该应用开发者是位于中国某地区的 B**N 集团。通过 360 安全大脑，发现其证书信息涉及过万个应用，其名称类型大致分为博彩、直播、浏览器，其中博彩类应用名称包含巴黎人、金沙、万博、永利国际等关键词，浏览器名称包含

太阳城、金沙、永信，其中还包括专用字样，可以看出均为博彩行业关键词，说明这些浏览器都是为博彩平台定制开发的。

图-博彩网站推荐使用专属浏览器引流页面

2. B**N 开发应用关联产业

B**N 集团开发的过万个应用中，部分包名含 demo、test，例如应用名 B* Games，包名为*.game.*.test1，应用名为*ball，包名为*.b*.*.demo，推测为测试包。应用逆向分析后，发现作者来源于中国某地区，与签名中城市信息相吻合。同时发现疑似该作者开发的博彩代理应用 demo，包名为*bet.agent.*，应用指向*bet.com，但页面展示内容不全，推测为早期测试版本，目前已失效。根据*bet 关键词，在搜索引擎中，我们发现该关键词指向多个博彩网站，说明该应用是一个博彩代理 APP。

通过这批应用流转地址及关联节点来看，境外节点中以菲律宾、缅甸、柬埔寨数量最多，其中菲律宾、柬埔寨的节点中还发现了其他的博彩信息，说明该批应用的实际运营者位于菲律宾、缅甸、柬埔寨。该产业是 B**N 集团为核心，其为东南亚博彩集团、杀猪盘提供应用定制开发，躲避境内网络安全厂商、执法机构的拦截，东南亚博彩集团、诈骗团伙进行平台运营，最终面向中国开展博彩、杀猪盘等活动。

三、 钓鱼邮件攻击背后的“缅北魔方 G”组织

2021 年 9 月，互联网开始频繁出现冒充公司给员工发工资补贴邮件进行诈骗的新闻，但由于“过于”小众，没有引起广泛的重视。随着此类手法的爆发，2022 年又再次出现在公众视野中。今年 5 月 360 手机卫士收到用户反馈，其收到“关于发布最新工资补贴通知，请打开附件查收!”的邮件，扫码访问邮件中的二维码，并按照提示填写姓名、电话号码、

银行卡号、验证码后，资金被盗刷。这些邮件使用的钓鱼页面与虚假 ETC 短信钓鱼网站在界面、功能上相似，推测为同一个团伙或供应商。随着研究的深入，我们发现这些钓鱼网站背后是位于缅北的黑灰产团伙，其开发了冒充工资补贴、ETC、社保、医保等钓鱼网站，并通过短信群发、邮箱群发等方式进行引流。鉴于此种引流方式大多使用**魔方工具进行数据清洗，我们将此类攻击行为统称为“缅北魔方”。同时本次发现的组织在钓鱼中使用的中转域名均为 site*.g*.r*，基于此将其命名为“缅北魔方 G”组织。

1. “缅北魔方 G”攻防特点

通过邮件中涉及的钓鱼域名来看，其主要是通过 Cname 的方式解析至 site01.g*.r*。根据域名的上线时间，我们发现诈骗团伙十分谨慎，域名在传播前才上线，从而降低域名过早外露导致被拦截。site01.g*.r*共解析至 18 个中国某地区服务器，最早解析时间为 2021 年 12 月，最近解析时间为 2022 年 5 月，说明该黑产团伙从 2021 年 12 月已开始实施攻击行为，随后在引起广泛关注后下线域名。Cname 至 site01.g*.r*的域名达 500+，其域名后缀主要为 xyz、uno、fun、love、ws、loan 等，其中 xyz、uho 的域名使用的最多达 400+，并生成不同的钓鱼子域名，如冒充 ETC、冒充国家医疗保障局。

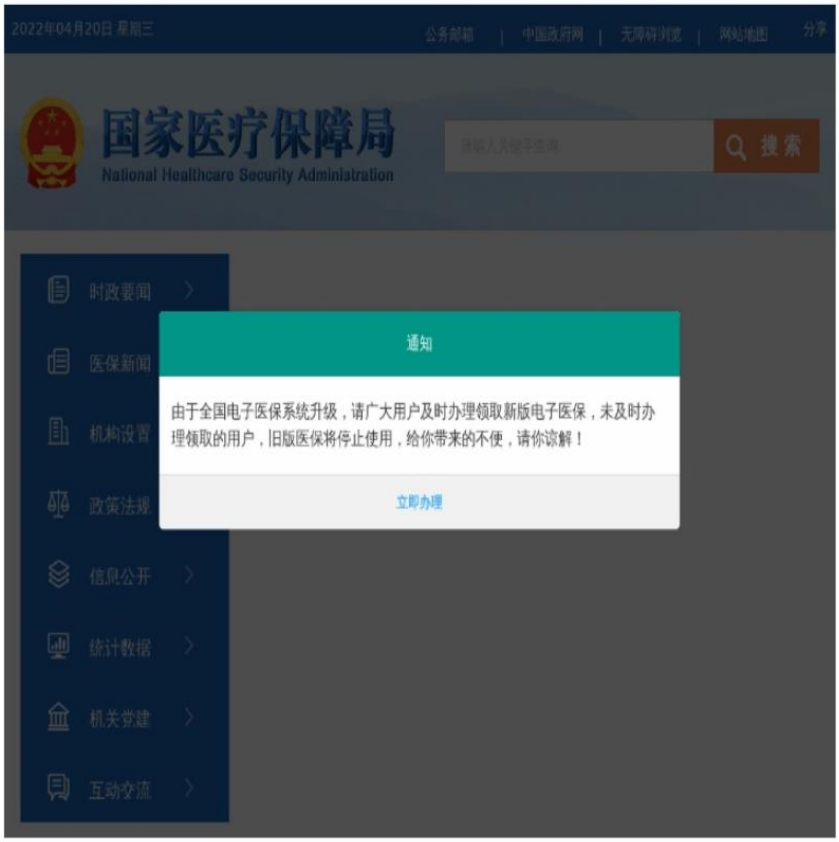


图-冒充国家医疗保障局钓鱼网站界面

通过 g*.r*域名解析记录来看，其 2022 年使用的子域名过百个，使用的服务器 IP 超过

10 个，域名服务器分布在阿根廷、美国等地。其中可能用于做域名解析跳转的子域名共 9 个，其特点是子域名为 site*，IP 均指向中国某地区。从攻防手段来看，“缅北魔方”组织，使用了多级域名轮换进行域名防护和隐藏自身，但相较于缅北其他的诈骗组织使用的攻防手段，缺少了使用 CDN 对服务器 IP 的保护。

从目前掌握的情报来看，推测“缅北魔方”组织通过搜索引擎、商业信息服务平台批量检索并爬取了大量的企业邮箱。由于这些企业邮箱的特点是公网可以访问，其盗取到财务的邮箱密码后，冒充财务向企业内部发送钓鱼邮件。目前被攻击的企业类型可能涉及通讯、保险、餐饮、纺织、可再生能源、大学、住宅物业等多个行业。

2. 钓鱼邮件攻击路径分析

从目前钓鱼邮件的攻击手法来看，其主要是先向某些员工（特别是财务人员）发送含钓鱼网址的钓鱼邮件，通过伪装的网站页面，引导该员工在页面中填写邮箱账号和密码，进而利用该员工的邮箱向企业内部群发钓鱼邮件。但这里会存在一种情况，如果企业限制内部邮箱非公网访问，仅仅掌握到邮箱密码，可能连邮箱的登录页面都进不去，故黑产会优先选择公网类邮箱进行攻击。

从钓鱼邮件的攻防手段来看，网址是以二维码形式展示的，意味着大部分受害人会使用社交 APP、手机浏览器进行扫描访问，而目前除了主打浏览器安全防护拦截的厂商外，大多数厂商手机侧网址拦截能力均较弱。同时该二维码中的域名进行了 UA 检测，如果是非手机端访问，将不显示内容，并提示使用手机访问，增加了网址的识别及收录难度。若事前收录了某钓鱼页面，但由于其使用了多级跳转、子域名轮换、框架嵌套等技术，很难及时识别并拦截。

第四章　热门“诈骗剧本”

一、最新消息！暴雷 P2P 可以退款了？

近日，有不法网站假冒银保监会等金融监管部门，发布带有“银保监会认证”“中国银保监会”等不实信息内容，并以“官方回款”“清退回款”等名义实施诈骗。用户是某信贷平台的出借人员，但平台 3 年没回款，于是网上搜索“xx 信贷最新消息”的过程中，看到了相关公告类页面，该公告表示，鉴于用户是对方忠实的投资用户，邀请用户加群进行本息补偿服务。用户添加指定的 QQ 群后，向群管理员提供了“本息截图”、“平台注册手机号”，随后对方向用户介绍了回款方案，即在指定的 APP 内进行充值操作。用户在指定的 APP 内充值 3772 元后，对方引导其联系“规划师”进行回款操作。随即“规划师”表示，回款需要用户在回款周期内，在该款指定的 APP 内购买虚拟货币，用户购买首笔亏损 10 元后，申请退出被拒，发觉被骗。

专家解读

此类诈骗中，不法分子常常以“官方回款”“清退回款”名义欺骗群众，如 P2P 清退、教育清退，编造“成功案例”，利用消费者急于回款、挽回损失等心理，以达到骗取资金的最终目的。在 P2P 清退诈骗场景中，诈骗人员事前伪装了大量的 P2P 清退网页或信息，引导受害人主动关注，快速筛选目标用户。在自媒体时代，普通用户可以在媒体平台注册发帖，即诈骗分子可以在大量的媒体平台发布文章，由于平台的权威性，极易让用户误以为消息的真实性。

安全提示

针对 P2P 网贷机构出借人的“回款”诈骗、“官方回款”诈骗以及“虚假投资理财”“虚假网络贷款”“解债上岸”“代理退保”“白条代偿”“银行直存”等，均是利用消费者急于解困、急于挽回损失等心理特点，侵害消费者信息安全、财产安全，造成消费者财产损失，消费者要谨防“回款”类诈骗侵害。

二、这种二维码不能轻易扫，小心违规被封号！已有人被骗

骗子在 QQ 中冒充用户好友，谎称自己 QQ 账号异常，需要用户帮忙进行 QQ 辅助验证，给受害人发送 QQ 辅助认证二维码，用户扫码并辅助验证成功。

随后对方再次给受害人发送一个某信辅助二维码，希望用户帮助其进行某信辅助验证，但用户扫码后，某信被对方登录，对方冒充受害人，向其某信好友借钱。

图-某信异常登录提示

专家解读

被骗关键点在于，受害用户扫描的所谓的某信辅助二维码，其实是某信登录授权二维码，用户在不明真相的情况下“授权”骗子登录了某信，看似不算高明的手法背后，其实相当具有迷惑性。骗子第一次发送的是真实的 QQ 辅助验证，导致受害用户第二次扫描某信二维码时，会降低防范心理，骗子更容易得逞。目前，平板设备的普及，以及较为成熟的黑灰产业链背景下，变相降低了养号、诈骗等场景的成本。于此同时，某信从支持双端登录，升级到支持手机、平板、电脑三端登录，后续可能会演变出其他诈骗方式，要注意防范。

安全提示

不要轻易扫描陌生二维码，不要轻易帮助他人扫码进行辅助解封，谨慎使用需要授权登录某信、QQ 等绑定银行账户的第三方软件，建议选用 360 手机卫士 App 内的安全扫码功能，及时发现未知风险，防患未然。

三、提单需修复，请支付认购单

用户在短视频平台看到招收文具组装兼职广告，随后添加了“工作人员”的某信，在该工作人员的要求下，添加了“报名客服”的某信进行报名。报名后对方以公司准备发半成品组装笔原材料为由，索要了用户的姓名、收获地址、手机号，并以对接商家接待，领取材料、邮费为由，引导用户安装专属的聊天 APP。

在该聊天应用中，接待客服以物流发货需 5-7 天，在等待期间可以参与其他兼职活动为名，邀请用户参与刷单，即在指定的平台购买认购单。用户前期投入获得小额返利，后期用户完成认购任务后，却无法提现，对方以提单需修复为由，要求用户垫付认购单的 40%资金，用户发觉受骗。

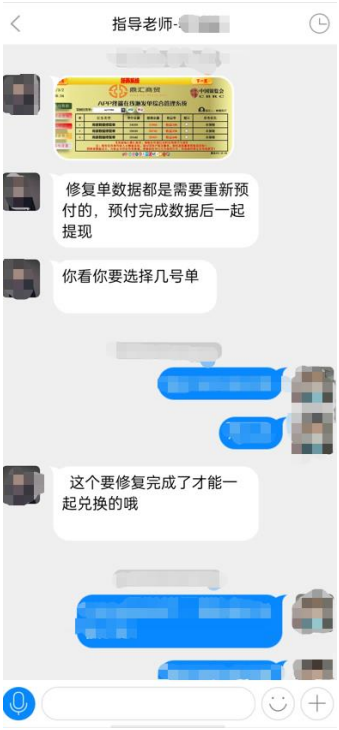


图-引导用户充值话术

专家解读

早期的刷单，是电商平台的商家以佣金的方式雇佣他人在其店铺购买商品，进行好评，提高其店铺在电商平台的权重，本质是商家围绕电商平台进行店铺数据造假。随着电信网络诈骗的兴起，不法分子脱离电商平台，假借刷单名义，诱导用户向其转账，骗取刷单商品费。

安全提示

网络刷单本身就是一种违法的行为，任何要求垫资的网络刷单都是诈骗，遇到“刷单”、“刷信誉”、“刷信用”的网络兼职广告时要提高警惕。

四、小心！网络代买“冰墩墩”骗局：有人花上百元收到的竟是“耳环”

被北京冬奥会带火的吉祥物“冰墩墩”，集万千宠爱于一身，成为“一墩难求”的爆款，线下店买不到，线上也售罄，这时有人告诉你，他手里有“冰墩墩”，想要吗？

2022 年 2 月，用户在短视频平台发现有用户售卖冰墩墩，与对方沟通后便添加对方的某信。双方确认商品价格、商品数量后，用户通过某信扫码的方式向对方支付商品费。对方收款后对方向用户提供了快递单号，但用户收到货后，发现商品并不是冰墩墩，而是一对耳环，准备询问对方原因时，发现已无法联系上对方，得知受骗。

图-引导用户转账界面

专家解读

“冰墩墩”的火热，吸引了大量买家的关注，但由于购买人数多，造成货源不足。不法分子便利用此种现状，以掌握货源为由，向用户兜售“冰墩墩”，但官方都缺货的商品，他却“有货”，这本身就是自相矛盾的事情。

安全提示

切勿从陌生人处购买“冰墩墩”谨防诈骗；此外，也不要从“黄牛”手中高价购买特许商品，不要相信价格炒作跟风盲目购买，要理性消费，不让骗子有机可乘。

五、那一晚我们赤诚相见，你却用我的照片敲诈我

2022 年 3 月，用户在境外某聊天软件中认识了好友，以为其是性情中人，在与其聊天的过程中，被对方诱导进行裸聊，裸聊之前对方要求用户安装名为“爱*”的 APP 进行远程操作。用户根据对方提供的网址下载安装了“爱*”，输入指定的邀请码完成了应用注册。双方裸聊后，对方以掌握用户的裸聊画面、手机通讯录为由，对用户进行敲诈勒索，用户按照对方的要求向对方转账 1.2 万元后，对方仍要求用户转账 11 万元，用户发觉即使转账也无法解决事情后，便不再向对方转账。

图-引导用户安装裸聊敲诈 APP

专家解读

用户被引导安装的“爱*”应用，其本质是一个窃取用户通讯录信息的恶意程序，不法分子通过色情诱惑的方式引导受害人安装，在双方裸聊后，以将受害人的裸照群发给通讯录好友为由进行敲诈勒索。

安全提示

网络交易需谨慎，主动提供色情视频聊天的，多半为诈骗分子的套路，不要随意点开陌生人发来的链接，更不要下载来源不明的 APP。

第五章　2022 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。

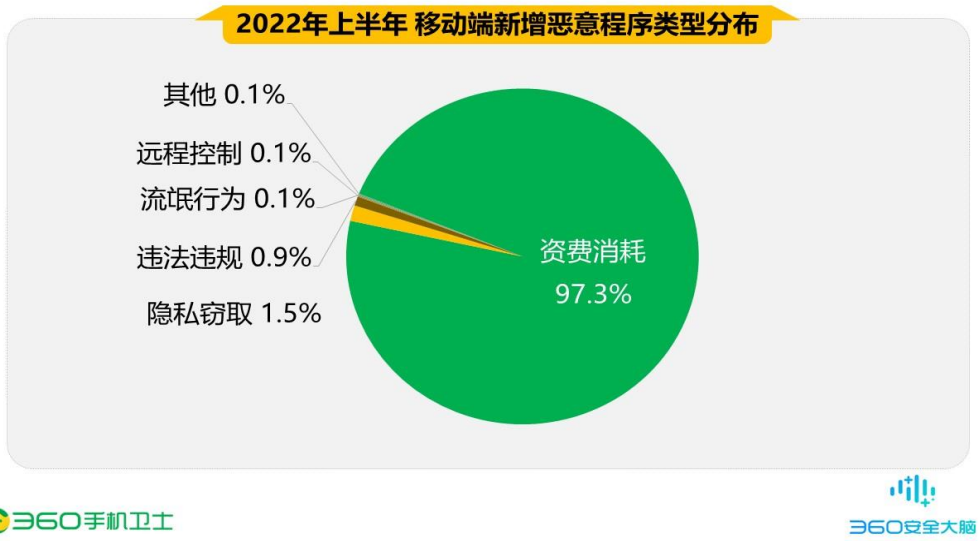
2022 年上半年 360 安全大脑不断提升针对移动互联网恶意程序的识别收录能力，截获的移动端新增恶意程序同比有显著提升。基于自身已有的海量数据进行实时研判，实现事前预警、事中阻断、事后溯源，不断提升黑灰产的诈骗成本，为移动互联网的健康有序发展提供强有力的技术支持。

一、 恶意程序

1. 恶意程序新增样本量与类型分布

2022 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 1079.7 万个，同比 2021 年上半年度（385.0 万个）上升了 180.5%，平均每天截获新增手机恶意程序样本约 6.0 万个。下图为 2022 年上半年度移动端各月新增恶意程序样本量统计：

2022 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 97.3%；其次为隐私窃取（1.5%）、违法违规（0.9%）、流氓行为（0.1%）、远程控制（0.1%）等。下图为 2022 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

2022 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 63.6 亿次，平均每天拦截手机恶意程序攻击约 3512.3 万次。下图为 2022 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

随着反诈反制力度的加强，传统的涉诈 APP、URL 遭到拦截、封停，生存空间被压制，诈骗产业逐步向色情直播+博彩综合类转型，恶意程序新增量逐渐增加，越来越多的诈骗集团增加此类投入，但由于头部应用效应，拦截量并未持续递增。同时，由于 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，恶意程序拦截量趋势，较去年也有明显增

长。

单位：万

4. 恶意程序拦截量地域分布

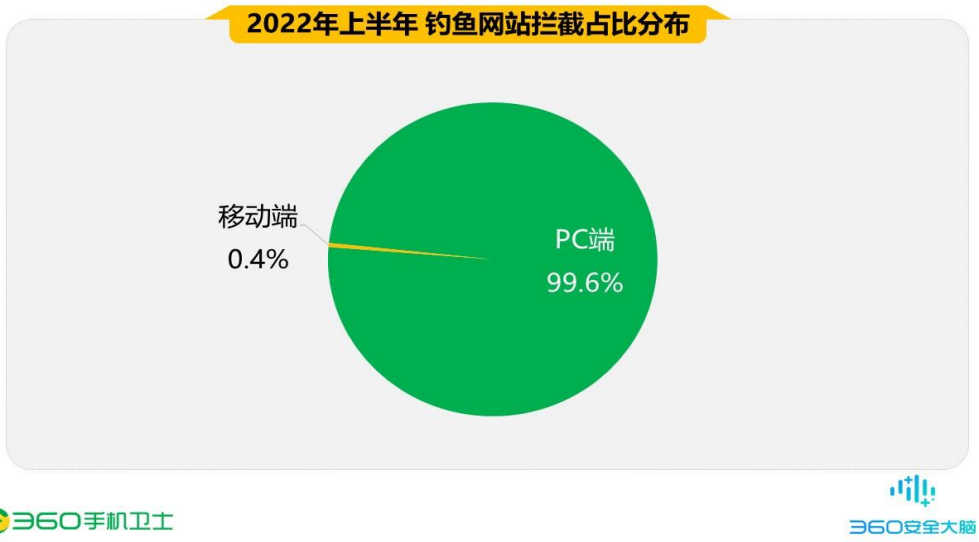
2022 年上半年度，从省级分布来看，遭受手机恶意程序攻击最多的地区为广东省，占全国拦截量的 10.3%；其次为山东（7.8%）、河南（7.4）、江苏（7.1%）、河北（5.5%），此外四川、浙江、安徽、湖南、广西的恶意程序拦截量也排在前列。

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，占全国拦截量的 2.3%；其次为重庆（2.0%）、成都（2.0%）、北京（1.9%）、上海（1.9%），此外深圳、郑州、杭州、天津、南京的恶意程序拦截量也排在前列。

二、 钓鱼网站

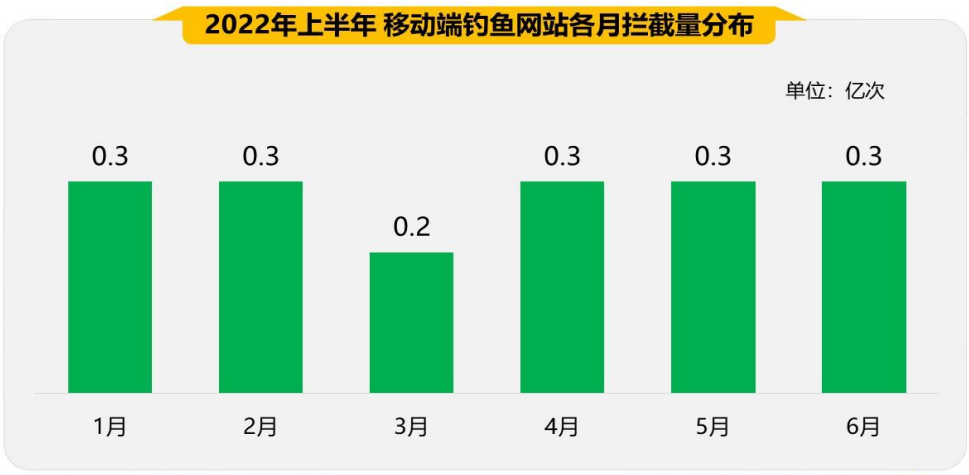
1. 移动端钓鱼网站拦截占比

2022 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 399.2 亿次，同比 2021 年上半年度（581.3 亿次）下降了 31.3%。其中，PC 端拦截量约为 397.5 亿次，占总拦截量的 99.6%，平均每日拦截量约 2.2 亿次；移动端拦截量约为 1.7 亿次，占总拦截量的 0.4%，平均每日拦截量约 95.1 万次。下图为 2022 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

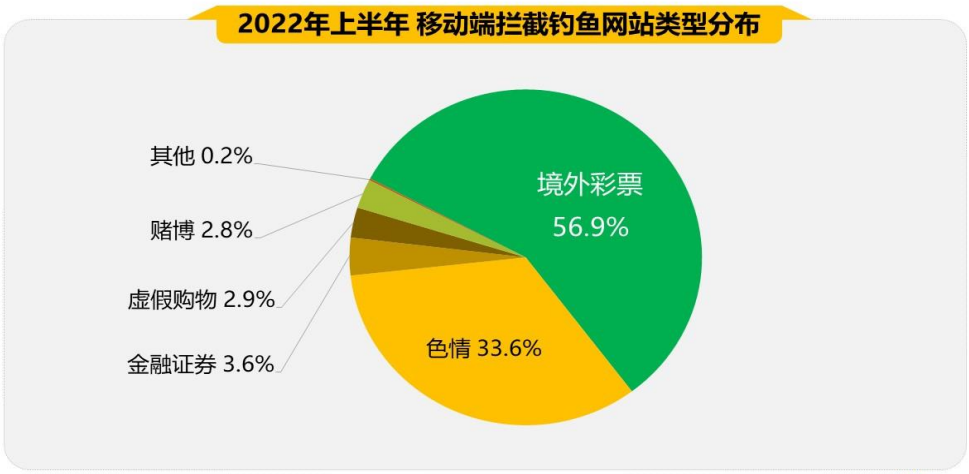
2022 年上半年度，360 安全大脑在移动端拦截钓鱼网站攻击约为 1.7 亿次，同比 2021 年上半年度（3.2 亿次）下降 45.8%。下图为 2022 年上半年度钓鱼网站各月拦截量分布：



360手机卫士　360安全大脑

3. 移动端钓鱼网站类型分布

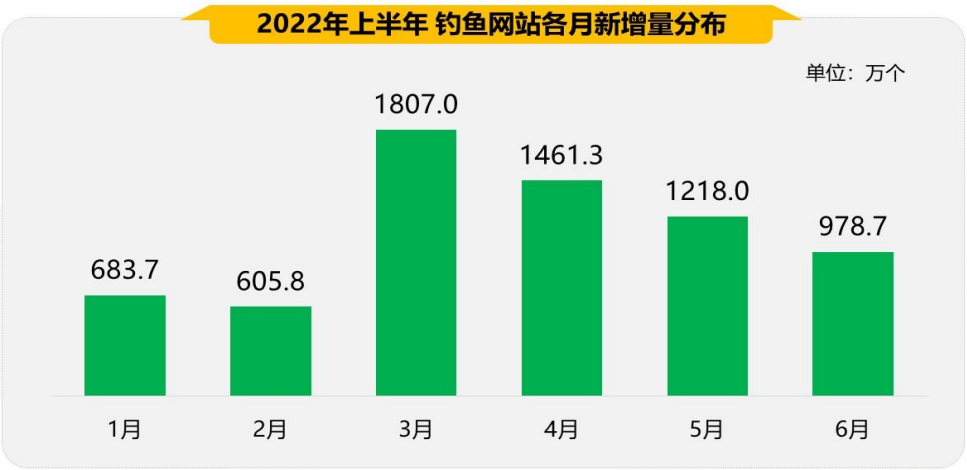
2022 年上半年度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 56.9%；其次为色情（33.6%）、金融证券（3.6%）、虚假购物（2.9%）、赌博（2.8%）等。下图为 2022 年上半年度移动端拦截钓鱼网站类型分布：



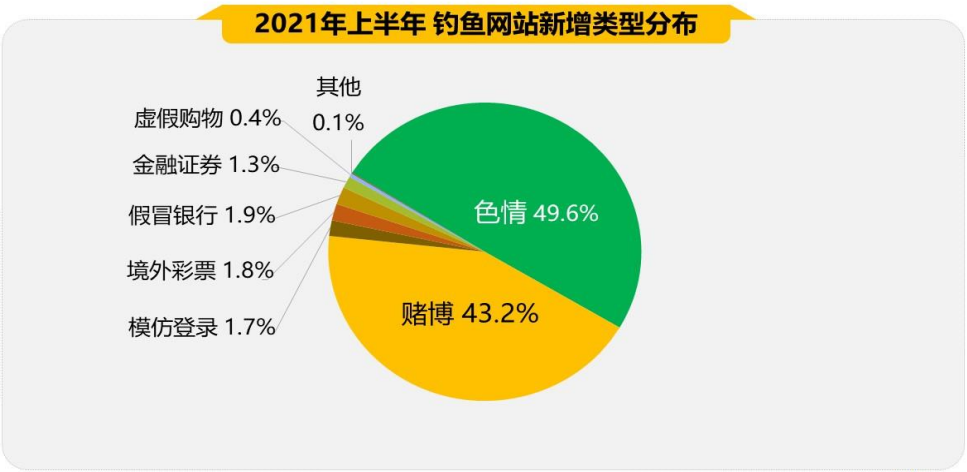
360手机卫士　360安全大脑

4. 移动端钓鱼网站新增量

2022 年上半年度，360 安全大脑共截获各类新增钓鱼网站 6754.5 万个，同比 2021 年上半年度（7833.9 万个）下降了 13.8%，平均每天新增 37.3 万个。下图为 2022 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 49.6%；其次为赌博类，占比 43.2%。下图为 2022 年上半年度移动端新增钓鱼网站类型分布：

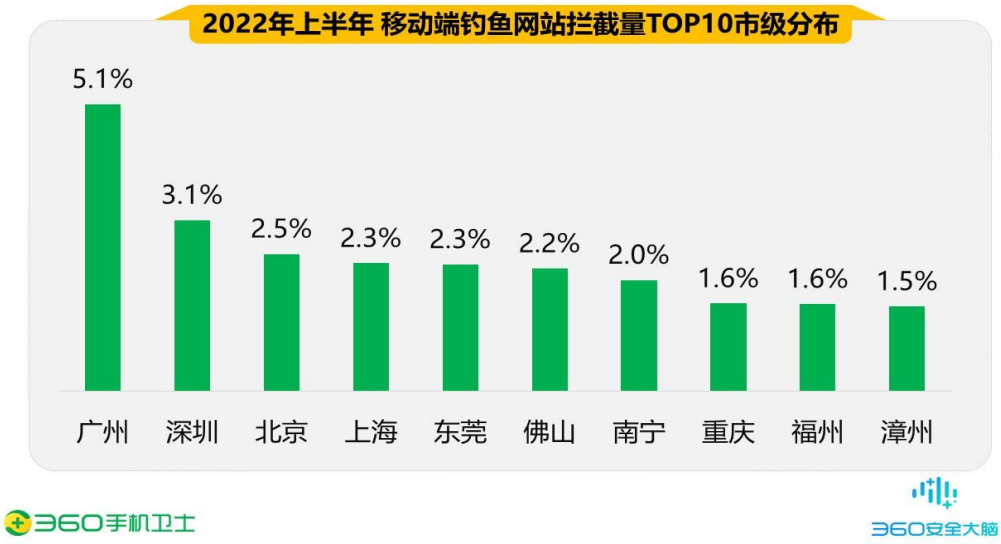


5. 移动端钓鱼网站拦截量地域分布

2022 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 23.7%；其次为广西（8.6%）、福建（8.1%）、山东（5.2%）、湖南（4.4%），此外

江苏、浙江、河南、河北、湖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 5.1%；其次为深圳（3.1%）、北京（2.5%）、上海（2.3%）、东莞（2.3%），此外佛山、南宁、重庆、福州、漳州的钓鱼网站拦截量也排在前列。



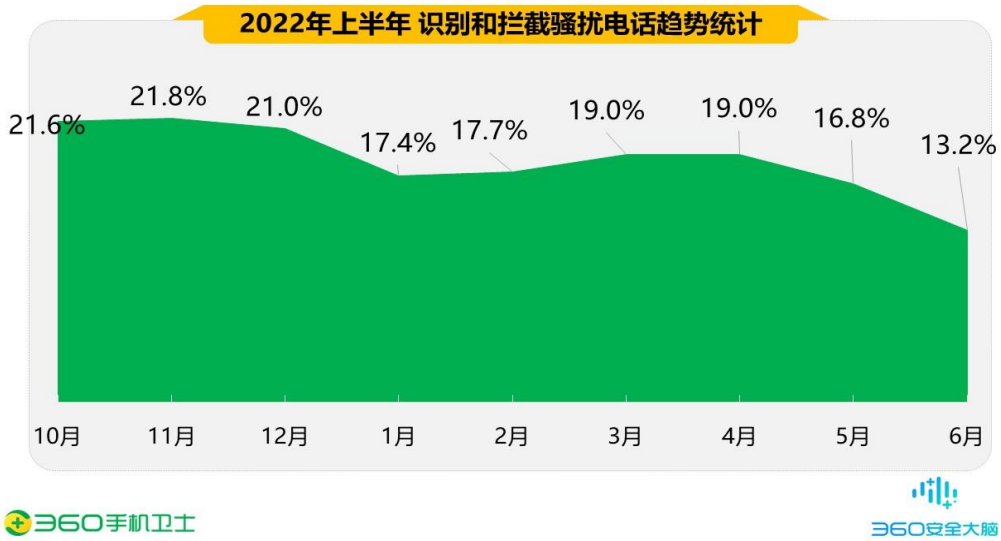
三、 骚扰电话

1. 骚扰电话标记拦截量

2022 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 116.7 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。同比 2021 年上半年度（111.0 亿次）上升了 5.1%。下图为 2022 年上半年度骚扰电话各月拦截号码次

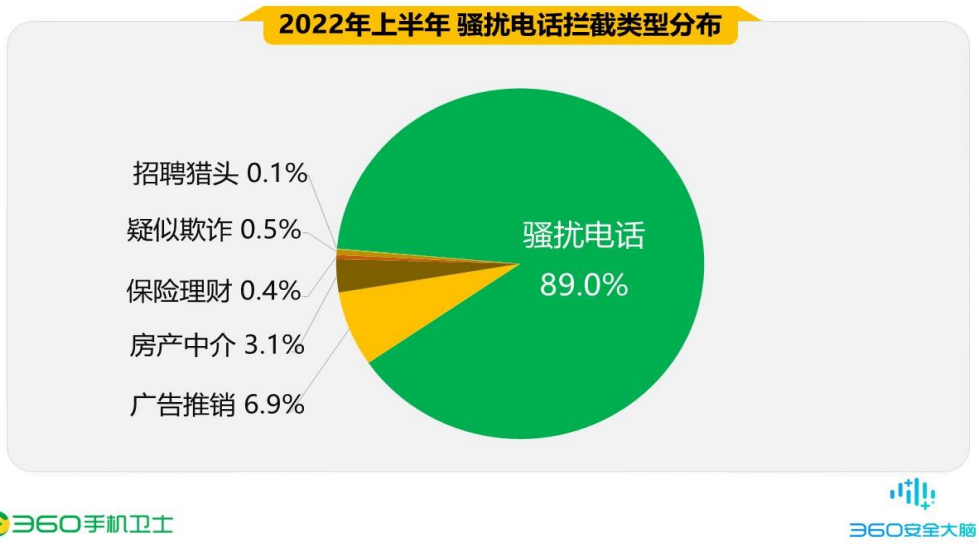
数分布：

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，2022 年 1 月底 2 月初正值春节假期，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。2022 年 3 月份起，骚扰电话拦截量回升，之后拦截量稳中有所下降。下图为 2022 年上半年度识别与拦截骚扰电话趋势统计：



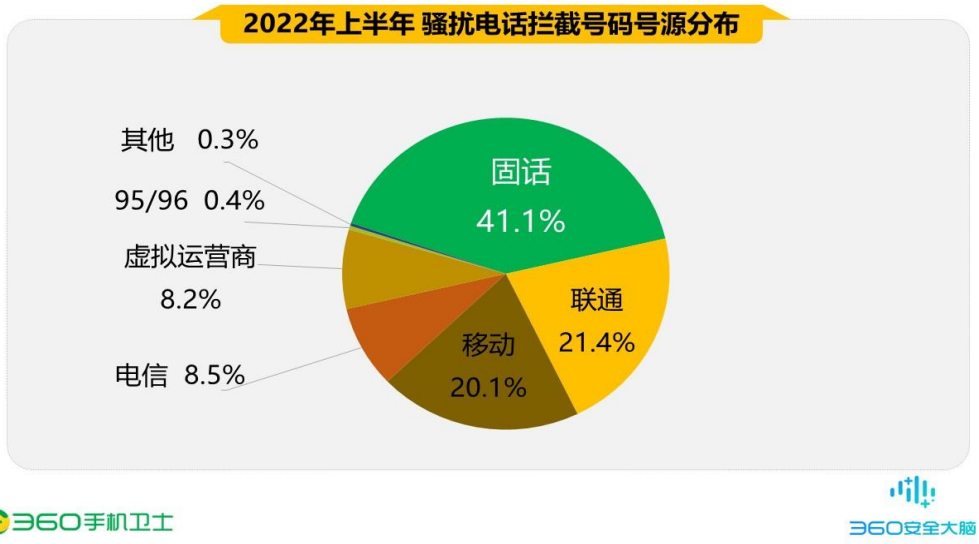
2. 骚扰电话拦截类型分布

2022 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 89.0%的比例位高居首位；其次为广告推销（6.9%）、房产中介（3.1%）、保险理财（0.4%）、疑似欺诈（0.5%）、招聘猎头（0.1%）。下图为 2022 年上半年度骚扰电话拦截类型分布：

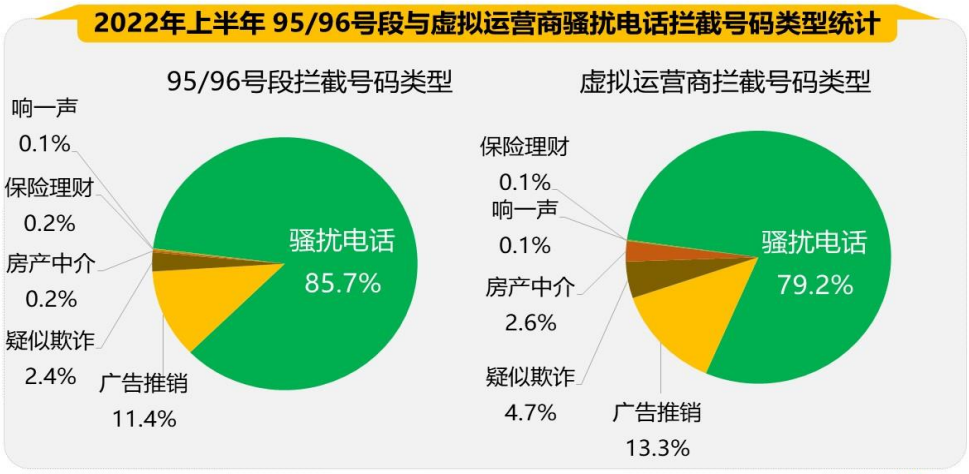


3. 骚扰电话拦截号码号源分布

2022 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 41.1%，其次为运营商为中国联通的个人手机号（21.4%）、运营商为中国移动的个人手机号（20.1%）、运营商为中国电信的个人手机号（8.5%）、虚拟运营商（8.2%）、95/96 开头号段（0.4%）等。下图为 2022 年上半年度骚扰电话拦截号码号源分布：



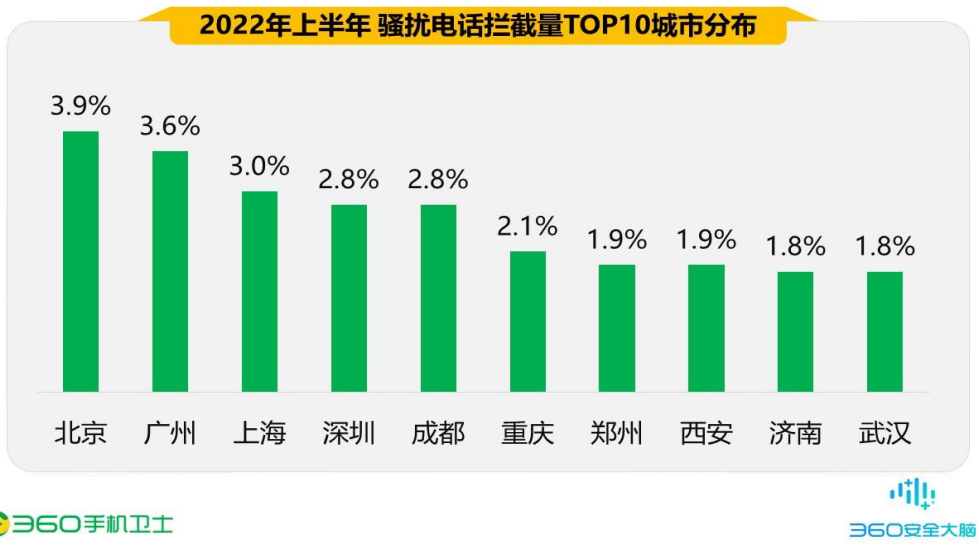
观察 95/96 号段与虚拟运营商骚扰电话拦截号码类型，95/96 号段骚扰电话类占据首位，占比 85.7%；虚拟运营商骚扰电话类占据首位，占比 79.2%；广告推销类分别占比 11.4%与 13.3%，类型比例占据前列。95/96 号段与虚拟运营商号码依然是不法分子从事非法行径的主要“工具”之一。



4. 骚扰电话归属地分布

2022 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 13.1%；其次是山东（7.9%）、江苏（6.7%）、河南（5.8%）、四川（4.9%），此外河北、浙江、湖南、北京、福建的骚扰电话拦截量也排在前列。

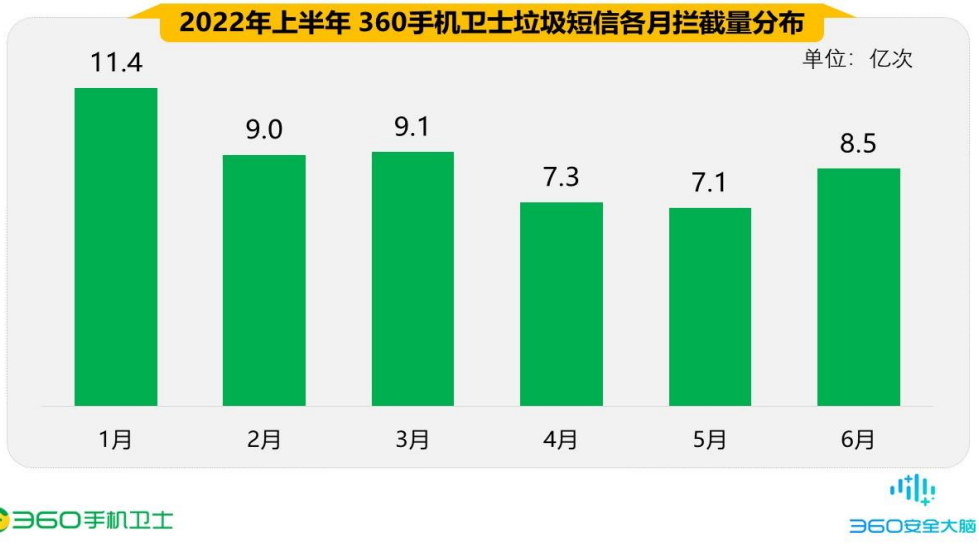
从城市分布来看，北京市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 3.9%；其次是广州（3.6%）、上海（3.0%）、深圳（2.8%）、成都（2.8%），此外重庆、郑州、西安、济南、武汉的骚扰电话拦截量也排在前列。



四、 垃圾短信

1. 垃圾短信拦截量

2022 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 52.3 亿条，同比 2021 年上半年度（93.4 亿条）下降了 44.0%，平均每日拦截垃圾短信约 2891.9 万条。下图为 2022 年上半年度 360 手机卫士垃圾短信各月拦截量分布：

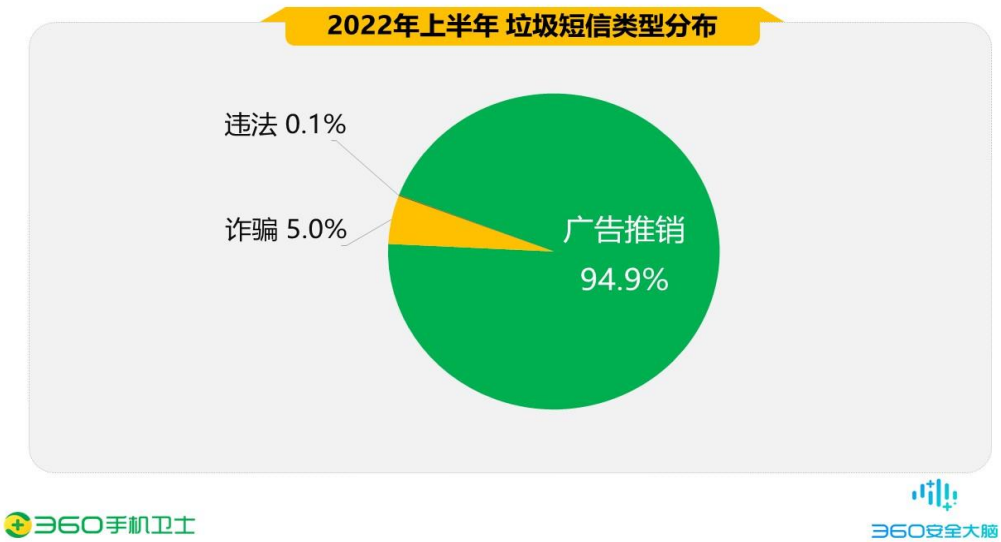


根据垃圾短信拦截量趋势分布，由于第一季度 2 月份春节期间各类发送垃圾短信的从业人员减少、企业放假休息，各类广告推销类型短信减少，导致 2 月份垃圾短信数量降低，3 月份开始逐步回升。但是由于短信治理力度加强，传统短信网关很难传输垃圾短信，引流渠道向短视频、小众聊天、加密聊天、招聘等渠道转移，垃圾短信拦截量还是有所下降。不

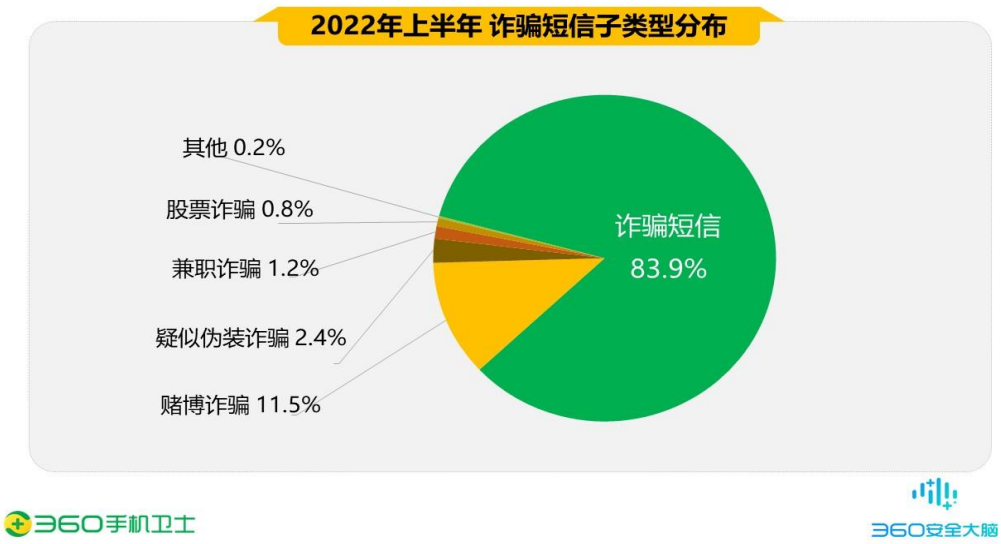
过在 6 月，由于电商活动，短信量有所回升。下图为垃圾短信拦截量趋势分布：

2. 垃圾短信类型分析

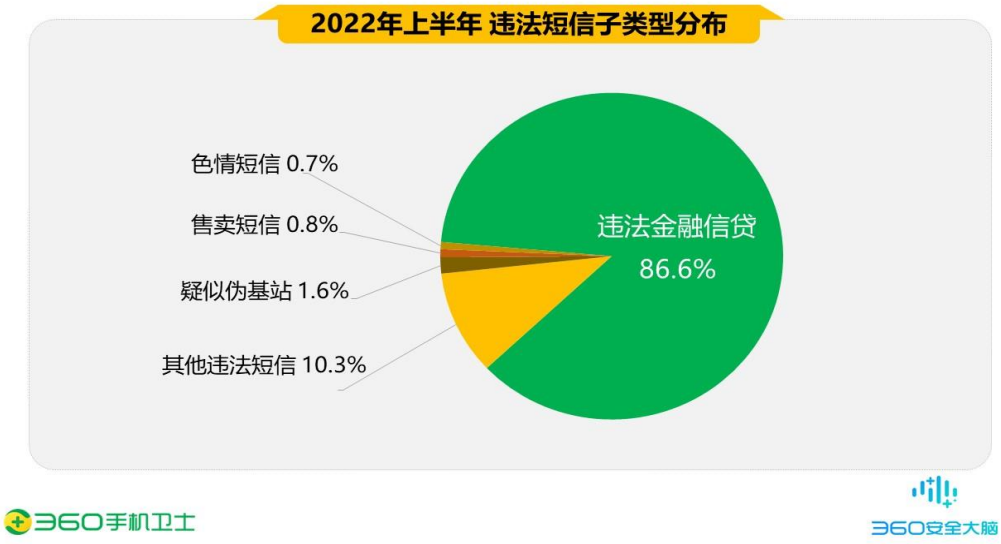
2022 年上半年度，垃圾短信的类型分布中广告推销短信最多，占比为 94.9%；诈骗短信占比 5.0%；违法短信占比 0.1%。



从诈骗短信拦截类型来看，诈骗短信以 83.9%的比例位居首位；其次为赌博诈骗（11.5%）、疑似伪装诈骗（2.4%）、兼职诈骗（1.2%）、股票诈骗（0.8%）等。现如今，越来越多的诈骗短信中包含文本字符少且仅有网址，如“可吃 www.******.rip”，此类短信内容晦涩难懂，仅通过内容难以判断其诈骗类型，360 安全大脑也在不断优化算法模型，提升实时研判诈骗短信新增与变种的能力，帮助用户抵制诈骗短信所带来的侵害。下图为 2022 年上半年度诈骗短信子类型分布：



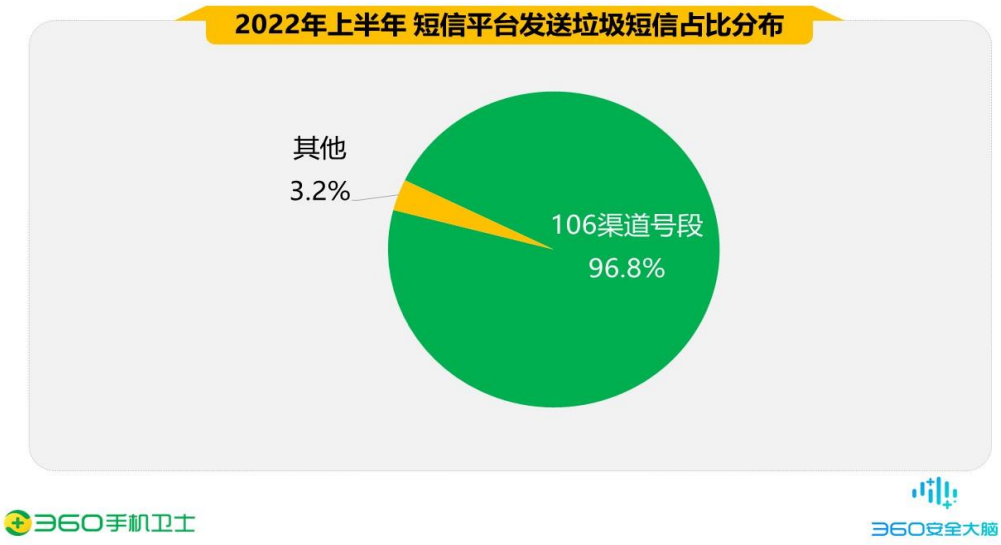
从违法短信拦截类型来看，违法金融信贷短信以 86.6%的比例位居首位；其次为疑似伪基站发送（1.6%）、售卖信息（0.8%）、色情短信（0.7%）等。下图为 2022 年上半年度违法短信子类型分布：



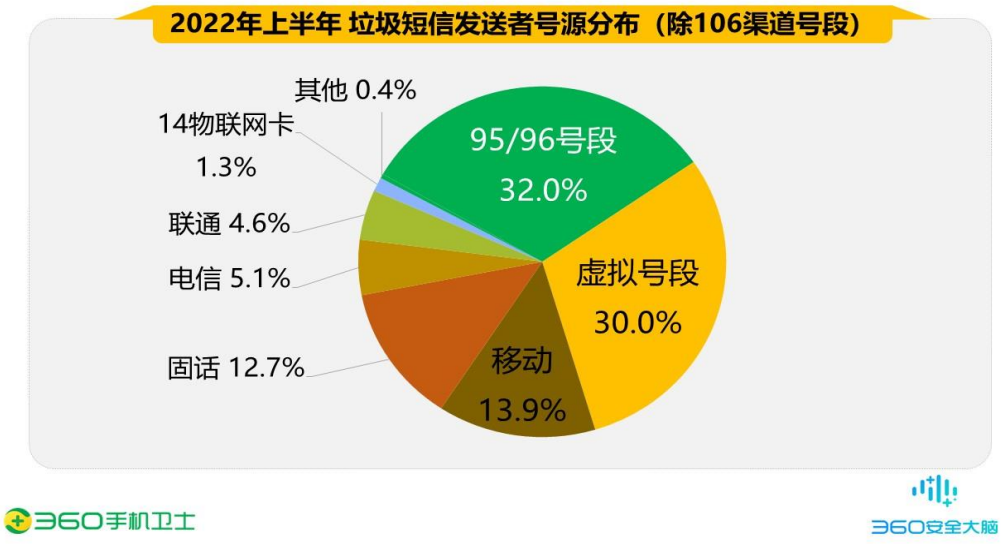
3. 垃圾短信发送者运营商号源分布

2022 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 96.8%；利用其他号段传播垃圾短信占比约 3.2%。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，从获取用户联系方式到群发短信已形成完整产业链条。其发送成本低、传播范围广的特点被黑灰产业利用，成为传播违法诈骗类短信的重要渠道。与此同时，在短信内容中利用关键词、变体字等实现“攻防”，而且越来越多的短信文本内容“短小精悍”，令人难以理解，无法仅从内容上辨别其本质，垃圾短信发展现状依然严峻，需要强而

有效的法规监管。下图为 2022 年上半年度短信平台发送垃圾短信占比分布：



2022 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 95/96 号段发送垃圾短信的最多，占比 32.0%；其次是虚拟运营商号段（30.0%）、运营商为中国移动的个人手机号（13.9%）、固话（12.7%）、运营商为中国电信的个人手机号（5.1%）、运营商为中国联通的个人手机号（4.6%）、与 14 物联网卡（1.3%）等。



4. 垃圾短信拦截量地域分析

2022 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 19.3%；其次是北京（9.5%）、江苏（7.5%）、山东（6.7%）、浙江（6.3%），此外河南、四川、河北、湖北、湖南的垃圾短信拦截量也排在前列。

从城市分布来看，北京市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 10.8%；其次是广州（9.1%）、深圳（4.3%）、南京（3.9%）、上海（3.4%），此外重庆、成都、杭州、武汉、西安的垃圾短信拦截量也排在前列。

第六章 2022 上半年度网络安全行业动态

一、 中宣部公安部联合启动“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和党中央决策部署，贯彻落实中办、国办印发的《关于加强打击治理电信网络诈骗违法犯罪工作的意见》，中宣部、公安部于 5 月 10 日联合启动“全民反诈在行动”集中宣传月活动，进一步加强宣传教育，发动群众力量，汇聚群众智慧，营造全民反诈、全社会反诈浓厚氛围。

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违法犯罪系列宣传教育，针对易受骗群体开展精准防范宣传，不断推动反诈防诈知识进社区、进农村、进家庭、进学校、进企业，着力构建全方位、广覆盖的反诈宣传教育体系。主要新闻媒体和新媒体平台将持续推出反诈报道，强化以案说法，普及防骗知识，切实增强群众防骗意识和识骗能力。中宣部、公安部将联合工信部、中国人民银行等有关行业主管部门，对金融机构、电信业务经营者、互联网服务提供者的从业人员及服务对象开展反诈宣传；联合教育部启动“反诈宣传进校园”活动，在全国高校推广建立校园反诈中心，组建大学生反诈志愿者队伍，开展反诈知识进教材、进课堂及反诈知识竞赛等教育宣传活动；联合全国老龄工作委员会开展“老年人防诈宣传”系列活动，编制《老年人防骗手册》，组织全国老年反诈知识竞赛等，持续掀起宣传教育热潮。

据了解，一年来，在以习近平同志为核心的党中央坚强领导下，各地区各部门各行业牢固树立以人民为中心的发展思想，狠抓打防管控各项措施和行业监管主体责任落实，推动打击治理电信网络诈骗违法犯罪工作取得明显成效。全国公安机关勇于担当作为、忠实履职尽责，持续开展“云剑”“长城”“断卡”“断流”等专项行动，先后组织全国集群战役 150 次，共侦破电信网络诈骗案件 39.4 万起，抓获违法犯罪嫌疑人 63.4 万名，同比分别上升 28.5%、76.6%。

在强有力的严打高压震慑下，全国电信网络诈骗案件快速上升的势头得到有效遏制，一年来公安机关立案数同比下降 18.7%。国家反诈中心会同有关部门全力构筑防止群众被骗的“防火墙”，直接推送预警指令 4060 余万条，各地推出预警线索 4170 万条，紧急止付涉案资金 3290 余亿元，成功避免 6170 余万名群众被骗。各地区各部门各行业将坚持打防结合、防范为先，切实形成齐抓共管、群防群治的整体合力，营造全民反诈、全社会反诈的强大声势，坚决遏制电信网络诈骗违法犯罪多发高发态势，有力维护人民群众财产安全和合法权益[2]。

二、 公安部集群战役打击为电诈提供新型“GOIP”通话服务的违法犯罪团伙

6 月，在公安部统一指挥下，31 个省区市公安机关同步开展集中收网行动，依法严厉打击为电信网络诈骗提供新型“GOIP”通话服务的违法犯罪团伙。截至目前，共抓获违法犯罪嫌疑人 870 余名，缴获“GOIP”设备 2390 余套、手机卡银行卡等作案工具 1.8 万张（台）。

近年来，由于“GOIP”设备具有人机分离、远程操控、异地拨号通话和支持多张电话卡等特点，大量藏匿在境外的电信网络诈骗团伙通过远程操控的方式，使用搭建在境内的“GOIP”设备向受害人拨打电话，从而实施诈骗，危害十分严重。

公安部对此高度重视，部署多地公安机关迅速捣毁一批违法犯罪窝点，同时拓展研判出相关线索 400 余条，发现相关案件 690 余起，涉案金额 4900 余万元，涉及全国多个省区市。在掌握相关犯罪事实和证据基础上，公安部决定组织全国公安机关开展集群战役进行集中收网。

公安部有关负责人表示，针对电信网络诈骗犯罪的新动向、新手法、新变化，公安机关将始终保持高压严打态势，确保打深打透打彻底，坚决从源头上遏制电信网络诈骗犯罪多发高发态势[3]。

三、 工业和信息化部再出反诈利器 正式推出“反诈名片”服务

为深入贯彻落实习近平总书记关于打击治理电信网络诈骗犯罪工作的重要指示精神，持续提升对电信网络诈骗的预警预防能力，继“12381 涉诈预警劝阻短信”和全国移动电话卡“一证通查”等服务之后，工业和信息化部再出反诈利器，面向公众推出了“反诈名片”服务。

近年来，各级公安机关投入大量警力，利用电话对正在遭受电信网络诈骗的群众进行预警劝阻，取得了显著成效。但在实际工作中，常常发生群众把公安机关的预警电话误认为诈骗或骚扰电话而拒接的情况，影响了预警劝阻成功率。为有效解决上述问题，工业和信息化部指导部反诈中心联合国家反诈中心，组织中国电信、中国移动、中国联通推出了“反诈名片”，对各级公安机关的反诈预警劝阻电话号码进行标记和来电提醒，帮助群众有效甄别电话来源，进一步提升预警电话的权威性和及时性。下一步，工业和信息化部将始终践行以人民为中心的发展思想，进一步加强与公安机关的协同配合，全力推进反诈各项工作，切实为群众办实事、做好事、解难事。

温馨提示，如果您收到带有“反诈名片”标记的预警劝阻电话，可以放心接听，如有疑问，请拨打 96110 进行咨询[4]。

参考文献

[1] 新华网. 国务院联席办有关负责人解读《关于加强打击治理电信网络诈骗违法犯罪工作的意见》[EB/OL].

http://www.news.cn/2022-04/18/c_1128571505.htm，2022/04/18

[2] 中国政府网. 中宣部公安部联合启动“全民反诈在行动”集中宣传月活动[EB/OL]

http://www.gov.cn/xinwen/2022-05/10/content_5689536.htm，2022/05/10

[3] 中国政府网. 公安部集群战役打击为电诈提供新型“GOIP”通话服务的违法犯罪团伙 [EB/OL].

http://www.gov.cn/xinwen/2022-06/13/content_5695512.htm，2022/06/13

[4] 工信部. 工业和信息化部再出反诈利器 正式推出“反诈名片”服务[EB/OL].

https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2022/art_416d5d2b670b4ff6ac32fd7a22857790.html，2022/06/23