2022 年度
中国手机安全状况报告

2023 年 02 月

前言

当前，电信网络诈骗犯罪已成为发案最多、上升最快、涉及面最广、人民群众反映最强烈的犯罪类型。诈骗手法紧跟社会热点持续演变升级，与当下流行的网络购物、物流递送、直播打赏等相结合，多环节包装实施连环诈骗。于此同时，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重要推手。

从 2022 年 360 安全大脑捕获到的黑产情报来看，在电销引流产业上，诈骗电话从“多卡宝”转向简易组网 GOIP，同时一些不法固话业务代理商、民众受利益驱使，将其开办的固话线路转接给境外电信网络诈骗分子，号码伪装性、迷惑性、欺骗性更强，群众难以辨别，极易上当受骗；在身份伪装产业上，从传统固网 IP 秒拨、服务器 IP 转向基站 IP、软路由等具备“反侦察”功能的 IP 类产品；在洗钱手法上，黑产一方面通过伪界面增加洗钱类应用的识别难度，一方面开发出高仿网银、“尾号跟随”等应用进行“黑吃黑”；在黑产链条上，盘踞在境内外的黑产供应商、团伙为占据更多的市场份额，获得更高的价值利润，增强了攻防能力，提高了攻击范围，如传统短信 ETC 钓鱼团伙，将攻击目标从普通群众增加至互联网企业业务系统及员工，影响更加恶劣。

为坚决遏制电信网络诈骗犯罪快速上升势头，公安部部署全国公安机关始终保持严打高压态势，全链条打击电信网络诈骗及关联犯罪，深入开展“斩链”“清源”“利剑”三大战役，抓获了一大批违法犯罪人员，破获了一大批诈骗案件；会同最高法、最高检等相关部门联合部署开展“拔钉”行动，成功将 240 名电信网络诈骗犯罪集团重大头目和骨干缉捕归案；针对华东、华南、京津冀等 3 个片区重点城市，组织开展区域会战，共捣毁诈骗窝点 1800 余个，实现规模打击效能最大化；针对涉诈黑灰产链条，组织发起打击涉诈固话语音专线、简易组网 GOIP、跑分洗钱等各类集群战役 80 余起，取得显著战果。

《2022 年度中国手机安全状况报告》基于 360 海量的安全大数据和 360 手机卫士黑灰产研判、分析、溯源能力，对 2022 年出现的电信网络诈骗及关联的重点黑灰产业链进行深度剖析，对相关反制手段、思路予以探讨，望能起到抛砖引玉的目的，集思广益。打击“黑灰产”是一项长期且艰巨的任务，需要政府、企业和个人一同努力，让“黑灰产”无缝可钻。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

第一篇 电信网络诈骗-黑灰产攻防技术.....1

第一章、电话引流技术，人机分离、远程操控.....1
一、 诈骗电话从“多卡宝”转向简易组网 GOIP.....1
二、 涉诈的“境外来电”穿上“本地来电”的外衣.....2
第二章、基站 IP、软路由成诈骗团伙热门网络环境隐藏手段.....3
一、 移动网络 IP 秒拨技术.....3
二、 固网代理 IP 软路由技术.....5
第三章、中文域名+自研客服系统成为征信类诈骗关键手段.....6
第四章、计算器成“跑分”产业新工具.....7

第二篇 电信网络诈骗-黑灰产业链现状.....10

第一章、利用靓号生成器进行虚拟货币盗刷.....10
第二章、利用定制化银行 APP，进行洗钱产业“黑吃黑”.....10

第三篇 电信网络诈骗-黑产技术供应商、团伙.....12

第一章、以 B**N 集团为攻防技术核心的东南亚博彩产业链.....12
一、 黑灰产攻防浏览器背后的开发者 B**N.....12
二、 B**N 开发应用关联产业.....13
第二章、钓鱼邮件攻击背后的“缅北魔方 G”组织.....14
一、 “缅北魔方 G”攻防特点.....14
二、 钓鱼邮件攻击路径分析.....15

第四篇 电信网络诈骗案例.....17

第一章、最新消息！暴雷 P2P 可以退款了？.....17
第二章、小心！网络代买“冰墩墩”骗局：有人花上百元收到的竟是“耳环”.....17
第三章、那一晚我们赤诚相见，你却用我的照片敲诈我.....18
第四章、注销贷款变成“申请贷款”.....19
第五章、 “杀猪盘”里没有爱情，只有诈骗.....21

第五篇 反电信网络诈骗行业动态.....22

第一章、政策法规颁布.....22
一、 中共中央办公厅 国务院办公厅印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》.....22
二、 反电信网络诈骗法表决通过.....23
第二章、政府重拳出击.....24
一、 公安机关打击治理电信网络诈骗违法犯罪取得显著成效.....24
二、 公安部深入推进打击电信网络诈骗“拔钉”行动.....25
第三章、行业服务建设.....26

一、 工业和信息化部再出反诈利器 正式推出“反诈名片”服务.....26

第六篇 电信网络诈骗趋势预测与反制建议.....27

第一章、新型网络犯罪趋势预测.....27

一、 引流、身份伪造等电诈产业出现全链条技术升级.....27

二、 洗钱手法更加隐秘，同时其产业内部出现大量“黑吃黑”现象.....27

第二章、黑产攻防对抗应对手段.....28

一、 开拓挖掘思路，提升黑产识别能力.....28

二、 构建电信网络诈骗防范和打击治理体系.....28

参考文献.....29

附录-2022 中国手机安全数据报告.....30

第一篇 电信网络诈骗-黑灰产攻防技术

第一章、电话引流技术，人机分离、远程操控

近年来，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“电销”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。

一、 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易暴露自身的位置。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。

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。

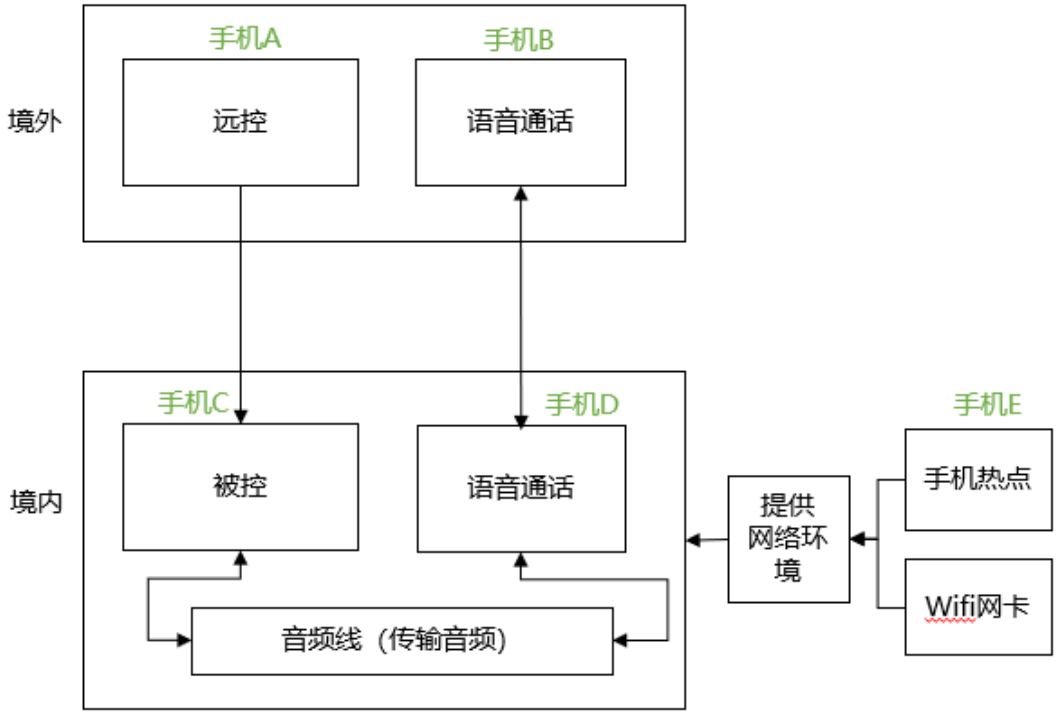

图 1 简易组网 GOIP 原理

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。

二、 涉诈的“境外来电”穿上“本地来电”的外衣

2022 年第二季度，我们发现诈骗使用的号码中，固定电话开始“冒头”，同期在黑产交易市场，我们也发现了大量的固话渠道商的踪影。由于诈骗分子来电号码显示为本地企业固定电话，极具伪装性、迷惑性和欺骗性，群众难以辨别，极易上当受骗。

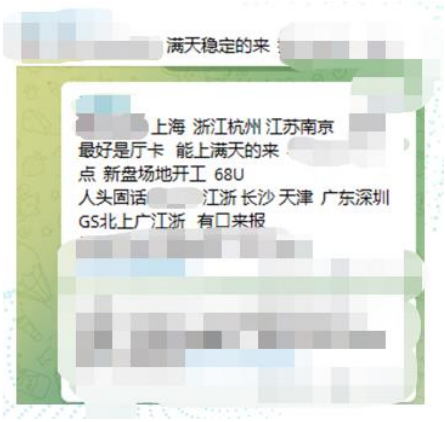

图 2 黑产群售卖固话线路

从掌握到的情报来看，一些不法固话业务代理商、民众受利益驱使，将其开办的固话线路转接给境外电信网络诈骗分子，从而使诈骗分子能够通过远程操控的方式拨打电话进行诈骗。境内固话线路人员，办理固定线路后，上线黑产提供或自费购买语音网关设备，将设备对接固定电话线路，上线黑产通过远程软件进行语音网关调试，对接相应的 SIP 服务器，实现固话线路的远程语音功能，诈骗人员使用具有 SIP 协议的语音类应用，远程调用固话线路拨打诈骗电话。

第二章、基站 IP、软路由成诈骗团伙热门网络环境隐藏手段

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 手机卫士在长期对黑灰产的溯源分析时，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，移动网络 IP 秒拨技术和固网代理 IP 软路由技术。

一、 移动网络 IP 秒拨技术

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。

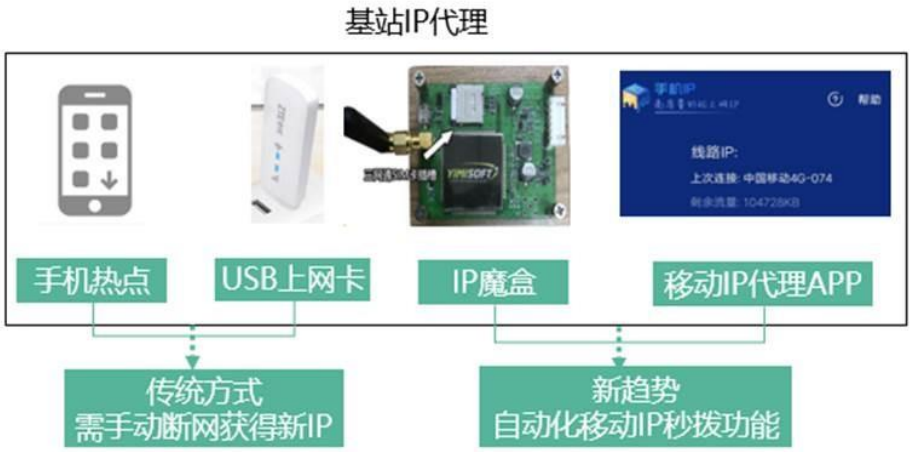

图 3 代理 IP 方式

USB 上网卡即便携式网络热点，插入手机卡，供电即可共享网络。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，分包卖给下线用户。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 4 移动网络秒拨 APP

二、 固网代理 IP 软路由技术

传统的 VPN 代理软件，针对的是使用该代理软件的设备，该设备的数据流量通过 VPN 软件进行转发，即设备需要先联网（内网/互联网），再连接进入 VPN 网络，当设备自身网络出现问题时，VPN 网络会中断，此时本机的 IP 便会暴露，于是一类针对全局网络，防止本机 IP 暴露的全局软路由器产品在黑产中出现。

此类软路由主要包含国内 IP 代理池、wifi 分发(一个路由器可分发出多个 wifi 信号，实现机机独立 ip，一键换 ip，断网保护，数据分流不串线)功能。目前黑产售卖的产品包括以下 2 类：①提供路由器固件及 IP 池，将市面上已发售的路由器进行刷机进而修改成可控的 VPN 类路由器。②集成 VPN 功能，支持多 IP 线路定制，多 wifi 分发（单设备可发出 1-100 个 WiFi，且机机 IP 独立）、IP 线路断网保护、wifi 伪装，修改 mac、ssid 于一身的路由器。

图 5 黑产渠道售卖的软路由产品效果展示

第三章、中文域名+自研客服系统成为征信类诈骗关键手段

冒充电商平台以用户账号征信存在问题需要注销为由，实施金融诈骗的手段是近年来高发的诈骗类型。随着反诈宣称力度和攻防对抗的加强，此类诈骗发生了一些攻防变化，诈骗人员伪造用于“身份认证”、“话术洗脑”的网站，从原先英文域名+第三方在线客服 API 搭建虚假的客服认证网站，转向使用中文域名+二次开发第三方在线客服系统搭建，效果更加逼真，用户及反制识别难度均增加。

此类冒充电商平台客服类诈骗，首先通过境内外号码联系受害人，引导受害者访问高仿的网站（电商平台、征信查询），增加信任感后，再引导受害人与该仿冒网站内的在线客服人员进行沟通，在客服的引导下安装会议、投屏类应用。在诈骗人员的远程协助下，进行“征信”处理，将自有资金或网贷资金转向指定账户。因此，在整个诈骗环节，仿冒的诈骗网站是诈骗成功的关键因素。为了提高迷惑性，诈骗团伙使用中文域名，且域名中使用了含特点电商平台、银监会相关的关键词，如*在线对接.com、*认证中心.me、银监会*中心.me 等。由于 com、cn 等传统域名注册人群较多，可用于注册的资源较少，诈骗团伙转而使用比较小众的域名，如 shop、me、lol、art、co、life、pics、club 等。从发现的部分黑产域名时间来看，最早时间为 2022 年 8 月，说明已有多个团伙使用中文域名进行攻防对抗。

图 6 虚假征信网站客服界面

以往发现的诈骗网站中，我们发现诈骗人员会通过第三方在线客服接口的方式实现网站的在线客服功能，近期发现的征信类诈骗网站使用的客服系统均非已知的客服接口，推测其“二次开发”了客服系统。从该客服页面中，我们发现了系统的备注说明（独立开发者）、相应的接口字段参数，根据这些参数我们发现该系统与市面上一款商业化客服系统界面、参数相似。该公司售卖的产品为源码授权模式，以此猜测黑产购买此套源码后进行二次修改，增加自有系统标识，在互联网出售给诈骗团伙。

第四章、计算器成“跑分”产业新工具

早前，我们发现博彩产业为方便博彩代理人员管理下线人员，为其定制开发博彩代理 APP，该应用伪装成一个可正常使用的计算器应用，当在该计算器中输入特定指令时，页面会展示真正的博彩代理登录界面。此类伪界面手段近期也在一款跑分应用中出现，通过同源追溯，发现该应用衍生产业链存活至今已达 2 年，且应用仍在不断进行版本迭代。

以跑分客的视角，来看看这个跑分应用到底是怎么“跑起来”的。首先，跑分客需要访

问指定的网址，获得本地 ip，并将 ip 提供给上线进行加白。紧接着登录指定的卡商网站，将跑分客的银行信息（银行卡号、所属省市、所属支行、取款密码、U 盾密码、登录密码、身份证号码）录入至平台，选择类型（U 盾、跑分-银行卡、手机短信-纯收款等）。完成账户信息录入后，手机安装界面伪装成计算器的应用，并授予短信权限，后期应用将实时将手机收到的短信同步给跑分云端服务器。

图 7 跑分客录入信息界面

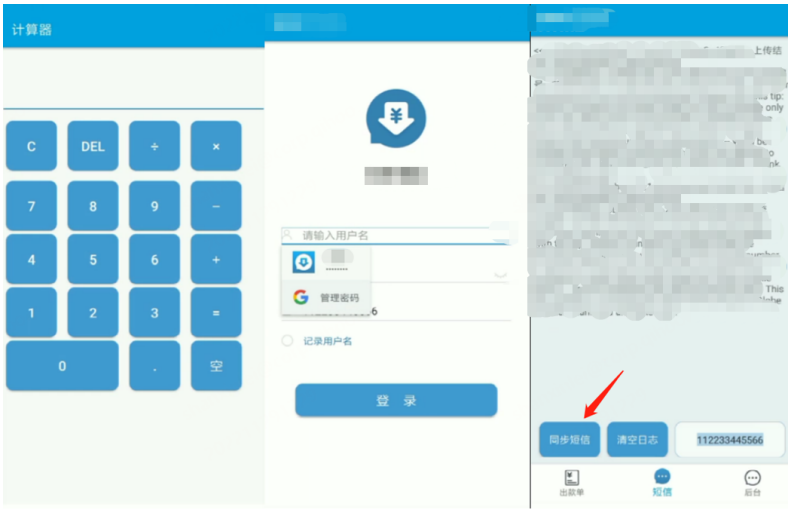

图 8 跑分客录入信息界面

根据其使用的样本特征，我们发现该应用运营者的运作模式主要包含使用多台境内外服务器做 APP 分发节点以及为不同的用户群控定制不同的子域名+不同的端口，例如子域名 shanghu（商户人员使用）、子域名 kashang（卡商人员使用）、sys（支付回调使用），故该产业涉及跑分客、支付通道运营商、黑灰产平台三个部分。支付通道运营商引导跑分客登录指定的卡商网站录入自己的银行卡信息，并在插入银行卡绑定手机号的卡的手机中安装指定的

计算器 APP，用于监控手机的银行卡短信，并转发至支付通道终端服务器。支付通道用户（博彩、诈骗等）开通该支付通道的 API 接入对应的诈骗平台，当用户在诈骗/博彩平台充值时，显示对应的充值入口（银行卡），用户在页面刷新后，重新调用接口。

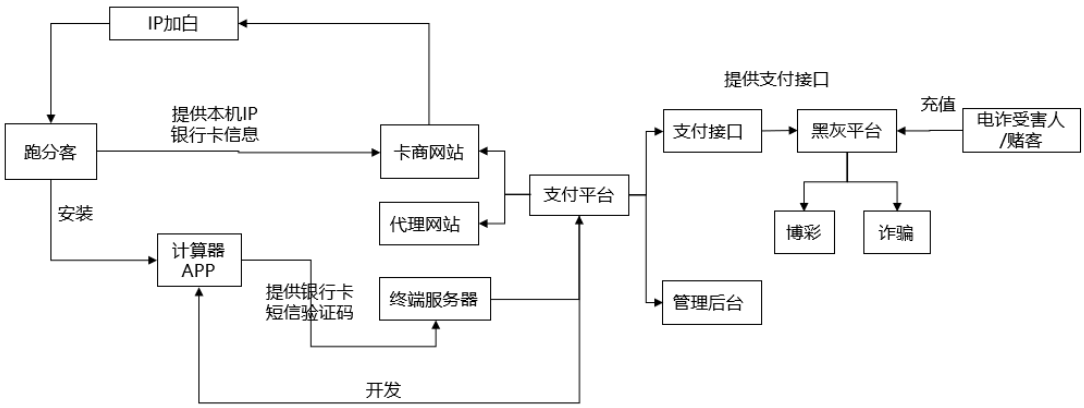

图 9 跑分产业流程

第二篇 电信网络诈骗-黑灰产业链现状

第一章、利用靓号生成器进行虚拟货币盗刷

相较于通过虚假虚拟货币网站、APP 此种高投入、低产出的资金盗刷方式，黑产开始针对有着大额流转的“洗钱”产业进行定向攻击，快速进行资产“掠夺”，其攻击方式是仿造出与“洗钱”产业中用于资金流转的相似账户，误导对方向伪装的账户转账。

在日常使用网银转账的过程中，部分网银会将过往交易记录中的账号展示出来，方便快速转账，例如 A 经常给 A1 频繁转账，A1 的账号就会频繁出现在最近转账的名单中。同样的道理，虚拟货币钱包也有类似的功能，此时若 B 生成了一个和 A1 账号尾号相同的账号，且出现在 A 的经常交易名单中，A 给 A1 转账的时候，就有可能误转给 B 。但想要实现这种骗局，涉及到两个重要的环节，需知道谁频繁转账，且知道收款人的账号信息，同时伪造出与收款人相同尾号的账号。这两个环节在传统的网银交易上基本上很难实现，但由于“虚拟货币网络”类似一个“记账本”，通过区块链浏览器即可查询虚拟货币网络中的交易情况，同时结合靓号生成器的地址伪造功能即可实现上述的过程。

靓号生成器其主要作用是批量生成指定规则的虚拟币收款地址，目前多个主流的虚拟货币网络均发现相关的靓号生成器，包括网页版、软件版。部分根据软件使用周期收费、部分根据号码规则（指定尾数 4 位，5 位，6 位）收费。其原理是随机生成一个私钥，然后由该私钥通过加密算法计算出地址，然后再根据靓号的规则去判断这个地址是不是符合要求，然后重复执行以上过程，根据机器的硬件性能不同，生成周期不同，约每秒可生成 1000 个地址，每天可生成 8000 万个地址。

第二章、利用定制化银行 APP，进行洗钱产业“黑吃黑”

在日常生活中，常见到“微商”们“晒的”各种收款截图，营造一种轻轻松松赚大钱的迷惑氛围，但熟悉微商套路的我们，深知那只是用于收割下线制作的“一眼假”收款截图。相较于微商通过转账生成器或图片生成网站生成银行转账截图，洗钱黑产们使用的工具则高深了很多。通过 360 黑产识别平台，捕获到黑产针对农业、平安、交通、浦发、招商、邮政、工商等银行制作的银行仿冒类应用，其作用原理是通过云端配置+仿冒银行 APP 上下游配合，实现定制化的虚假转账过程，再录制转账视频，其效果远比转账生成器或图片生成网站更加逼真。如下图黑产售卖的演示视频截图，在管理后台，针对账号的余额、信息、转账结果进行设置，如转账成功、转账失败、账户已冻结，在对应的高仿 APP 进行任意账号转账操作时，

页面即会显示已设置的内容。

图 10 黑产售卖的“银行仿冒类应用管理后台生成网银余额界面”教程截图

图 11 黑产售卖的“银行仿冒类应用转账效果界面”教程截图

针对此批高仿银行 APP 进行溯源分析，发现其从 2022 年 3 月开始上线，开发者通过多台境内外服务器充当存储及云控节点，使用不同的域名、不同的服务器进行应用迭代，约每 2 个月进行一次服务器替换。从该 APP 用户画像来看，其主要用户群体涉及博彩、诈骗、洗钱等。APP 在投放的过程中，我们发现其捆绑了 PC 远控木马，病毒名称包括*接码用户端平台.rar、代付流程.rar、吊大思路.txz 等，为接码、洗钱、诈骗产业相关的话术，即向黑产“投毒”，与此类 APP 的目标用户类型相同，据此推测此类样本为黑产人员用户资金诱骗，并以此进行黑产间黑吃黑。

第三篇 电信网络诈骗-黑产技术供应商、团伙

第一章、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 2022 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，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 12 诈骗网站提供的网址不能访问解决方案

一、 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 13 博彩网站推荐使用专属浏览器引流页面

二、 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。

第二章、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。2022 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。

一、 “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。

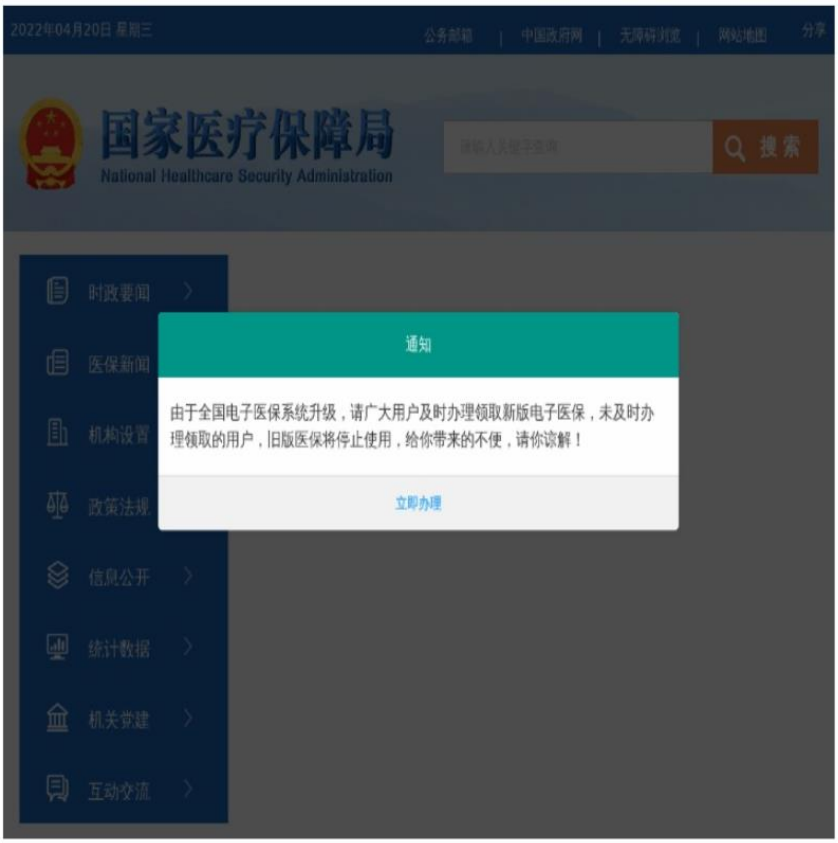

图 14 冒充国家医疗保障局钓鱼网站界面

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。

二、 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。

第四篇 电信网络诈骗案例

第一章、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。

第二章、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 15 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。

第三章、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 16 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。

第四章、注销贷款变成“申请贷款”

用户收到冒充某电商平台人员的固定电话，对方描述“用户的电商平台账户涉嫌绑定多

个网贷信息，违反国家的政策，需要解除相关贷款信息，恢复用户的征信”，随后引导用户使用指定的账号、密码登录指定的会议类应用进行解除操作，用户通过会议应用的屏幕共享功能，按照对方的要求，在多个贷款平台申请贷款，将所贷资金依次转入转账描述的“回款”账号，对方描述该账户收到资金后，进行校验后会自动返还原付款账户完成征信恢复，用户累计转账达 8 万余元，后发现受骗。

图 17 云会议界面截图

专家解读

在诈骗场景中，诈骗分子首先通过固话与受害人沟通，相较于传统的国际来电，固定电话的迷惑性较高，不易引起警觉，随后报出用户的信息取得初步信任。取得用户信任后，通过影响征信等话术，“恐吓”用户，进而引导用户在紧张的情绪下进入对方设定的陷进，同时通过会议类、远程协助类应用观察用户的手机屏幕，引导用户一步一步进行转账操纵，若用户不进行转账操作，则通过共享的屏幕窃取用户的转账交易密钥，实现资金盗刷。

安全提示

诈骗分子通常冒充电商客服人员，以“影响征信”“注销账户”“调整利率”为由，威胁与诱导并举，引导受害人进行操作，最终以套取受害者网贷和现金为目的。凡遇到此类来电，务必通过官方渠道核实，如对方要求视频通话或共享屏幕，应提高警惕。

第五章、 “杀猪盘”里没有爱情，只有诈骗

用户通过某聊天软件认识对方，随后对方以婚恋为由骗取用户信任，并称对方的亲戚在某头部互联网公司上班，有内部名额，可以投资赚钱。起初用户未参与该项目，但收到对方责怪“用户不为对方考虑”，随后用户安装对方指定的投资应用，并在该应用中购买理财项目，投资后却发现无法提现，联系该投资平台的客服，客服以“用户不是开发区域用户，被关闭取款通道和房间收益”为由，要求用户继续充值投资，用户发觉受骗。

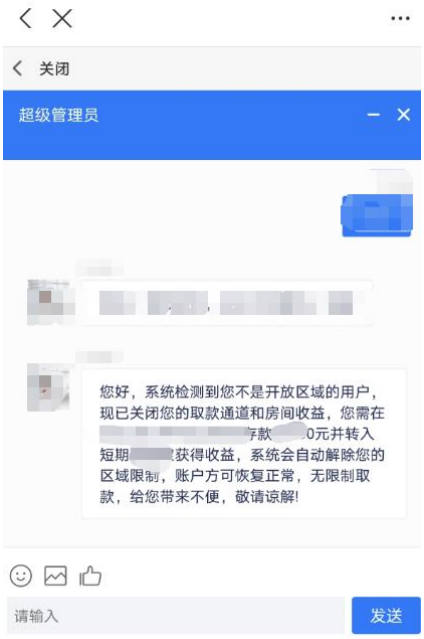

图 18 诈骗人员诱导受害人继续转账话术

专家解读

在诈骗场景中，诈骗分子通过交友的方式，以掌握快速赚钱秘籍为由，引导用户在指定的平台的进行投注，前期为增加用户信任度，给予小额返现，随着投注金额的增大，拒绝用户提现，并持续要求用户继续投注。

安全提示

网络世界虚虚实实、真真假假，网络交友一定要有戒心，不要过度透漏自己信息，以免给对方留有可乘之机，落入对方圈套。在网聊交友中一旦触及投资、购物、借钱、转账等关键词就要立即进行自我警示，在没有真正确定对方身份及用意时，切勿进行钱款操作。

第五篇 反电信网络诈骗行业动态

第一章、政策法规颁布

一、 中共中央办公厅 国务院办公厅印发《关于加强打击治理电信网络诈骗违法犯罪工作的意见》

近日，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》（以下简称《意见》），对加强打击治理电信网络诈骗违法犯罪工作作出安排部署。

《意见》强调，要坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的十九大和十九届历次全会精神，坚持以人民为中心，统筹发展和安全，强化系统观念、法治思维，坚持严厉打击、依法办案，实现法律效果与社会效果有机统一，坚持打防结合、防范为先，强化预警劝阻，加强宣传教育，坚持科技支撑、强化反制，运用科技信息化手段提升技术反制能力，坚持源头治理、综合治理，加强行业监管，强化属地管控，坚持广泛动员、群防群治，发动群众力量，汇聚群众智慧，坚决遏制电信网络诈骗违法犯罪多发高发态势，提升社会治理水平，使人民获得感、幸福感、安全感更加充实、更有保障、更可持续，为建设更高水平的平安中国、法治中国作出贡献。

《意见》要求，要依法严厉打击电信网络诈骗违法犯罪。坚持依法从严惩处，形成打击合力，提升打击效能；坚持全链条纵深打击，依法打击电信网络诈骗以及上下游关联违法犯罪；健全涉诈资金查处机制，最大限度追赃挽损；进一步强化法律支撑，为实现全链条打击、一体化治理提供法治保障；加强国际执法司法合作，积极推动涉诈在逃人员通缉、引渡、遣返工作。

《意见》要求，要构建严密防范体系。强化技术反制，建立对涉诈网站、APP 及诈骗电话、诈骗短消息处置机制；强化预警劝阻，不断提升预警信息监测发现能力，及时发现潜在受害群众，采取劝阻措施；强化宣传教育，建立全方位、广覆盖的反诈宣传教育体系，开展防范电信网络诈骗违法犯罪知识进社区、进农村、进家庭、进学校、进企业活动，形成全社会反诈的浓厚氛围。

《意见》要求，要加强行业监管源头治理。建立健全行业安全评估和准入制度；加强金融行业监管，及时发现、管控新型洗钱通道；加强电信行业监管，严格落实电话用户实名制；

加强互联网行业监管；完善责任追究制度，建立健全行业主管部门、企业、用户三级责任制；建立健全信用惩戒制度，将电信网络诈骗及关联违法犯罪人员纳入严重失信主体名单。《意见》还要求，要强化属地管控综合治理，加强犯罪源头地综合整治。

《意见》强调，各级党委和政府要加强对打击治理电信网络诈骗违法犯罪工作的组织领导，统筹力量资源，建立职责清晰、协同联动、衔接紧密、运转高效的打击治理体系。金融、电信、互联网等行业主管部门要全面落实行业监管主体责任，各地要强化落实属地责任，全面提升打击治理电信网络诈骗违法犯罪的能力水平[1]。

二、 反电信网络诈骗法表决通过

十三届全国人大常委会第三十六次会议 9 月 2 日表决通过《中华人民共和国反电信网络诈骗法》。专家普遍认为，反电信网络诈骗法坚持以人民为中心，统筹发展和安全，立足各环节、全链条防范治理电信网络诈骗，精准发力，为反电信网络诈骗工作提供有力法律支撑。

反电信网络诈骗法共七章 50 条，包括总则、电信治理、金融治理、互联网治理、综合措施、法律责任、附则等。这部法律自 2022 年 12 月 1 日起施行。

作为一部“小切口”的专门立法，反电信网络诈骗法在总结反诈工作经验基础上，着力加强预防性法律制度构建，加强协同联动工作机制建设，加大对违法犯罪人员的处罚，推动形成全链条反诈、全行业阻诈、全社会防诈的打防管控格局。

加强部门协同，是反诈工作的重要经验。反电信网络诈骗法规定了各部门职责、企业职责和地方政府职责，明确有关部门、单位在反电信网络诈骗工作中应当密切协作，实现跨行业、跨地域协同配合、快速联动，加强专业队伍建设，有效打击治理电信网络诈骗活动。

一段时期以来，手机卡、银行卡大量非法开办、随意买卖，成为电诈犯罪分子的重要工具。反电信网络诈骗法明确，电信业务经营者应当依法全面落实电话用户真实身份信息登记制度。银行业金融机构、非银行支付机构为客户开立银行账户、支付账户及提供支付结算服务，和与客户业务关系存续期间，应当建立客户尽职调查制度，依法识别受益所有人，采取相应风险管理措施，防范银行账户、支付账户等被用于电信网络诈骗活动。

反电信网络诈骗法还规定，办理电话卡不得超出国家有关规定限制的数量。对经识别存在异常办卡情形的，电信业务经营者有权加强核查或者拒绝办卡。开立银行账户、支付账户，不得超出国家有关规定限制的数量。对经识别存在异常开户情形的，银行业金融机构、非银行支付机构有权加强核查或者拒绝开户[2]。

第二章、政府重拳出击

一、 公安机关打击治理电信网络诈骗违法犯罪取得显著成效

2022 年，全国公安机关认真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，落实中共中央办公厅、国务院办公厅《关于加强打击治理电信网络诈骗违法犯罪工作的意见》部署要求，按照“四专两合力”总体工作思路，持续向电信网络诈骗犯罪发起凌厉攻势，截至 11 月底，全国共破获电信网络诈骗案件 39.1 万起，同比上升 5.7%，抓获犯罪嫌疑人数同比上升 64.4%，立案数同比下降 17.3%，造成财产损失数额同比下降 1.3%，实现了“两升两降”工作目标，打击治理电信网络诈骗犯罪取得显著成效。

为坚决遏制电信网络诈骗犯罪快速上升势头，公安部部署全国公安机关始终保持严打高压态势，全链条打击电信网络诈骗及关联犯罪，深入开展“斩链”“清源”“利剑”三大战役，抓获了一大批违法犯罪人员，破获了一大批诈骗案件；会同最高法、最高检等相关部门联合部署开展“拔钉”行动，成功将 240 名电信网络诈骗犯罪集团重大头目和骨干缉捕归案；针对华东、华南、京津冀等 3 个片区重点城市，组织开展区域会战，共捣毁诈骗窝点 1800 余个，实现规模打击效能最大化；针对涉诈黑灰产链条，组织发起打击涉诈固话语音专线、简易组网 GOIP、跑分洗钱等各类集群战役 80 余起，取得显著战果。在依法严厉打击的同时，结合《中华人民共和国反电信网络诈骗法》于 12 月 1 日正式施行有利契机，公安部部署全国公安机关统筹抓好反电信网络诈骗法的贯彻实施工作，联合最高法、最高检进一步完善“两卡”犯罪法律适用标准，用足用好法律武器，持续加大打击力度，全面提升打击质效，形成有力震慑。

为纵深推进打击治理电信网络诈骗犯罪工作，依托国务院部际联席会议机制，公安部积极会同相关成员单位加强科技支撑、强化预警防范，坚持系统观念、深入推进行业监管源头治理，努力构建更加严密的防范治理体系。公安部指导各地公安机关建立分级分类预警劝阻机制，推动“厦门经验”在全国落地生效，截至 11 月底，累计向各地推送预警指令 2 亿条，各地自主产出预警信息 1 亿条；会同工信部建成 12381 涉诈预警劝阻短信系统，累计发送预警提示短信、闪信 4.7 亿条；会同中央网信办建设推广国家反诈中心 APP，预警提示 2.4 亿次。人民银行深入推进“资金链”治理，支付行业常态化治理格局持续完善，组织商业银行、支付机构、清算机构协助公安机关阻断大量涉诈资金转移，挽回大量人民群众损失。工信部持续推进“断卡行动 2.0”，开展“不良 APP 安全治理”，严格落实实名制，全力整治虚商卡，对短信端口、语音专线、云服务等重点业务加大清理整治力度，不断提升全流程及时反制能力，累计处置涉诈高风险电话卡 1.1 亿张，拦截诈骗电话 18.2 亿次、短信 21.5 亿条。中央网信办集中整治互联网接入、域名注册、服务器托管、APP 制作开发、网络直播、引流

推广等涉诈重点领域，约谈曝光问题突出企业，网络生态环境不断净化。坚持广泛宣传和精准宣传相结合，加强对易受骗群体、案件高发行业和重点地区的精准宣传，联合中央宣传部组织开展“全民反诈在行动”集中宣传月活动，组织各类反诈宣传“进社区、进农村、进家庭、进学校、进企业”活动 2 万余场次，发送反诈宣传短信 30.7 亿条，国家反诈中心官方政务号发布短视频 9330 余条、播放量超 50 亿次，形成全社会反诈的浓厚氛围。

公安机关将全面贯彻落实党的二十大精神，认真贯彻落实反电信网络诈骗法，按照“四专两合力”部署安排，始终保持对电信网络诈骗犯罪的严打高压态势，深入开展“云剑”“断卡”“拔钉”等专项行动，持续强化区域会战、专案攻坚、集群战役，密切与各部门协作配合，坚决遏制电信网络诈骗犯罪高发态势，切实维护人民群众财产安全和合法权益[3]。

二、 公安部深入推进打击电信网络诈骗“拔钉”行动

2022 年 6 月以来，最高法、最高检、公安部等有关部门联合部署开展“拔钉”行动，严厉打击惩处电信网络诈骗集团重大头目和骨干。近日，中国公安机关与柬埔寨警方积极开展警务合作，成功抓获 9 名电信网络诈骗犯罪集团幕后组织者，查明涉案金额上亿元，“拔钉”行动取得重要成果。

近年来，电信网络诈骗犯罪多发高发，电信网络诈骗分子在境外搭建窝点，大肆对我国内民众实施诈骗。公安机关侦查发现，多起被骗损失超过千万元案件的诈骗窝点设在柬埔寨，公安部将其幕后组织者列为“拔钉”行动缉捕对象，牵头成立专案组，组织河北、山西、福建、河南、贵州等地公安机关加大侦查力度。在中柬执法合作协调办公室和驻柬使馆警务联络官的指导下，积极发挥国际刑警组织优势作用，我公安机关与柬埔寨警方通力合作，掌握了该诈骗犯罪集团的大量犯罪证据，柬警方先后将 9 名目标对象成功抓获，并于近日移交我方。另有 10 余名犯罪嫌疑人主动回国投案自首，目前已成功到案 24 名犯罪嫌疑人。

据悉，自“拔钉”行动部署以来，公安部先后将 490 余名电信网络诈骗集团重大头目和骨干列为“拔钉”缉捕对象。全国公安机关持续强化侦查研判，积极开展国际警务合作，已成功到案 240 余名缉捕对象，取得显著战果。部分犯罪嫌疑人已被提起公诉，等待他们的将是严厉的法律制裁。

全国公安机关将深入贯彻《反电信网络诈骗法》，继续严厉打击电信网络诈骗犯罪，深入推进“云剑”“拔钉”“断流”“断卡”等专项行动，依法高效开展国际警务合作，坚决遏制此类犯罪高发态势，切实维护人民群众的财产安全和合法权益[4]。

第三章、行业服务建设

一、 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[5]。

第六篇 电信网络诈骗趋势预测与反制建议

第一章、新型网络犯罪趋势预测

一、 引流、身份伪造等电诈产业出现全链条技术升级

在引流手段上，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“电销”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。在手机号码层面，从“多卡宝”类硬件转向简易组网 GOIP 设备，该设备本质上是成对出现的手机，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。在固话层面上，诱导他人将自有电话线索通过语音网关进行转接，实现远程操控固话线路拨打诈骗电话，由于诈骗分子来电号码显示为本地固定电话，极具伪装性、迷惑性和欺骗性，群众难以辨别，极易上当受骗。

在隐匿身份手段上，早期使用各类秒拨 IP 躲避风控的识别，为解决 IP 代理稳定性差产生的真实信息暴露，针对现有线路、设备进行全局改造，产出了包含全局代理、多 wifi 分发、专机专网、IP 伪造、设备伪造等功能的产品。

二、 洗钱手法更加隐秘，同时其产业内部出现大量“黑吃黑”现象

洗钱黑产与上游犯罪呈链条式发展，存在明显的相互依存关系，伴随着网络更新迭代，给传统的侦查理念、经验带来巨大冲击。在手段上，一方面洗钱团伙对于新会员的发展有着严格的审核制度，包括熟人介绍、邀请码机制，试图打造自有封闭生态；一方面使用反侦察手段进行攻防，包括带口令的伪界面应用，不断更替的 APP 存储、云控服务器、分发链接；同时与黑产平台紧密合作，在黑灰产平台投放广告，吸引跑分客入场，并为黑灰产平台提供源源不断的支付通道流转渠道，双方互利共生。

传统的洗钱方式，其本质是将资金通过银行卡、支付宝、微信等渠道进行多渠道流转，增加追溯的难度，但随着风控手段以及经侦建模能力的增强，传统洗钱方式易被快速冻结，而虚拟货币去中心化的特点，导致无法对全量交易进行风控及监管，而盗刷来源的虚拟货币相较于新生成的虚拟货币又增加了很多的干扰因素，进一步增加了监管难度，从历年来虚拟货币相关的资金盗刷情况来看，盗刷的金额越来越高，“受害人群”也从普通虚拟货币用户向大型虚拟货币交易所、职业洗钱团伙转移。大多数虚拟货币需通过传统的资金手段交易变

现，但由于不同国家对于虚拟货币有着不同的政策，传统金融行业与虚拟货币交易之间仍存在隔离屏障，无法通过传统的经侦手段关联现实资金与虚拟货币，虚拟货币。

随着黑产资金的大量聚合，各类针对洗钱产业黑吃黑手法涌现，例如通过高仿网银类 APP 伪造网银转账、利用靓号生成器进行虚拟货币资金盗刷。

第二章、黑产攻防对抗应对手段

一、 开拓挖掘思路，提升黑产识别能力

黑产的攻防对抗有个天然的不利条件，防守方需要针对所有的可能攻击行为制定风控模型，但过多的防守策略，间接的增加了业务的对接成本，防守策略是一个动态调节的过程，而攻击者仅需针对薄弱的环节进攻即可获得“胜利”，会持久的处于一种被动“挨打”的局面。

以 360 手机卫士在日常的黑产治理中所积累的经验来看，从“感知风险”和“控制风险”两个角度来对抗黑产，成功率相对较高。即谁、在什么时候、通过什么方式、对什么对象、做了什么，以及通过攻击者的思维来思考业务场景，攻击者关注的内容，能够获得的利益。以上文中的提及的各类黑产 APP 为例，这些 APP 并不是突然出现的，而是依托于相应的产业链出现的。通过对黑产产业链的分析，梳理其上下游，即可及时发现相应的攻防手段、关联工具，当拿到线报信息后，对线报进行拓线关联，识别对攻防手段的全链条封锁。此种场景下攻防对抗手段从单一的黑产环节识别转向监控黑产动向，实现全局封堵的难度降低。

二、 构建电信网络诈骗防范和打击治理体系

电信网络诈骗犯罪在世界各地遍地开花，成为全球性的打击治理难题。一是诈骗手法不断演变，逐渐使用的白+黑的手段导致风控识别模型出现误判，发现和识别难度增加；二是黑产使用的技术手段更加专业复杂化，通过新兴技术生成新的对抗工具；三是境内外团伙勾结，取证环节存在客观挑战。面对严峻的电信网络诈骗现象，需构建电信网络诈骗防范和打击治理体系，实现全链条电信网络诈骗惩治。一方面加大对黑灰产各黑产链条的打击力度，通过联合社会力量，对引流、技术支撑、信息买卖环节进行打击严惩，提升黑产环节的投入成本，；另一方面通过预警反制手段，发现潜在受害群众及时进行诈骗劝阻，降低案发率。

参考文献

[1] 中华人民共和国中央人民政府.中共中央办公厅 国务院办公厅印发《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.gov.cn/zhengce/2022-04/18/content_5685895.htm，2022/04/18

[2] 新华网. 反电信网络诈骗法表决通过 [EB/OL] http://www.news.cn/politics/2022-09/02/c_1128972095.htm，2022/09/02

[3] 中华人民共和国公安部. 公安机关打击治理电信网络诈骗违法犯罪取得显著成效 [EB/OL]. https://app.mps.gov.cn/gdnps/pc/content.jsp?id=8812495，2022/12/30

[4] 中华人民共和国公安部. 公安部深入推进打击电信网络诈骗“拔钉”行动 [EB/OL]. https://app.mps.gov.cn/gdnps/pc/content.jsp?id=8837670&mtype=，2023/01/11

[5] 中华人民共和国工业和信息化部. 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

附录-2022 中国手机安全数据报告

一、2022 年手机诈骗概况

1. 报案数量与类型

2022 年全年，360 反诈赔付保（原手机先赔）共接到 11 类手机诈骗举报，涉案总金额高达 2665.0 万元，人均损失 43761 元。在所有诈骗类型中，虚假兼职占比最高达 28.7%；其次是交友（26.1%）和身份冒充（13.0%）。从涉案总金额来看，交友类诈骗总金额最高，高达 908.1 万元，占比 34.1%；其次是虚假兼职诈骗，涉案总金额 610.0 万元，占比 22.9%；身份冒充排第三，涉案总金额为 588.0 万元，占比 22.1%。下图为 2022 年度手机诈骗的举报类型与涉案金额分布情况：

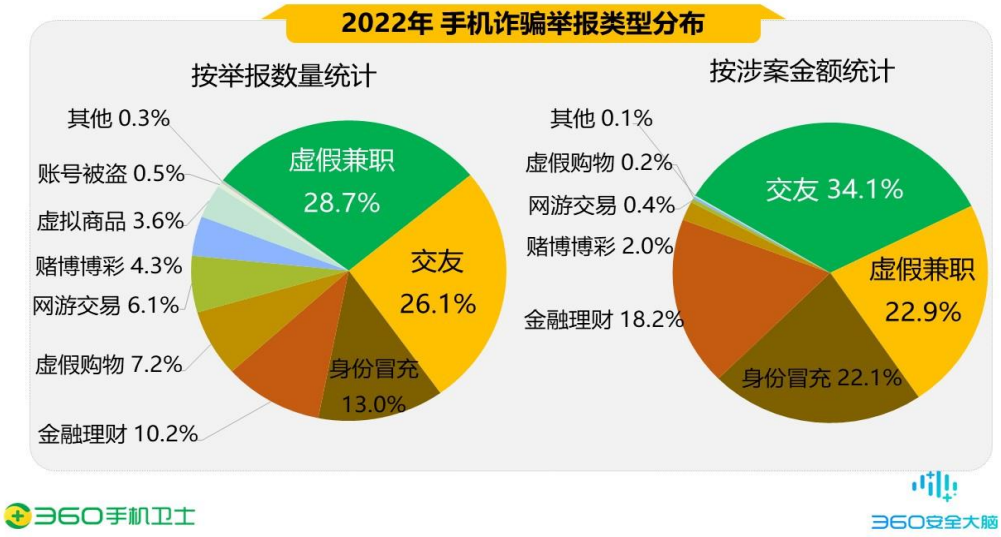

图 19 2022 年手机诈骗举报类型分布

2022 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，金融理财人均损失最高，约 7.8 万元；其次为身份冒充类，人均损失约为 7.4 万元。交友类诈骗由于其手法属于“敲诈勒索”，一旦受害人前期妥协向对方转账，后续诈骗人员会编造各种话术，逼迫受害人缴纳更多“保护费”，故此类诈骗的人均损失普遍较高。虚假兼职类诈骗在手法上，逐渐采用自研 IM+内嵌云控链接的应用，识别难度较原先的网页直接封装类应用有所提升。

2. 受害者性别与年龄

2022 年度，从举报用户的性别差异来看，男性受害者占 66.3%，女性占 33.7%，男性受害者占比高于女性。从人均损失来看，男性为 47100 元，女性为 37180 元，男性人均损失低

于女性。下图为 2022 年度手机诈骗受害者性别差异：

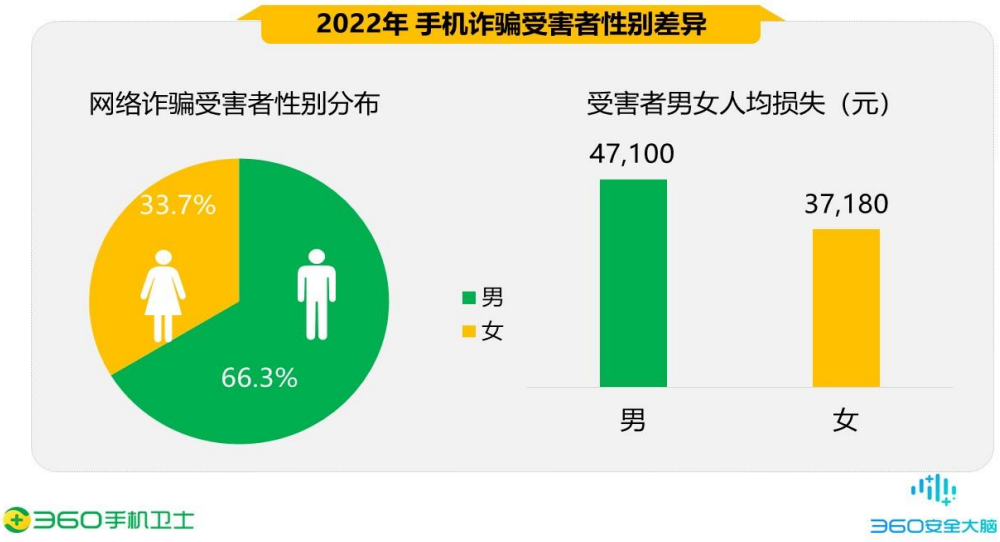

图 20 2022 年手机诈骗受害者性别差异

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 37.8%，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 27.4%；00 后占比为 24.0%；70 后占比为 8.0%、60 后占比 2.1%、50 后占比为 0.5%、40 后占比为 0.2%。下图为 2022 年度手机诈骗受害者年龄段分布：

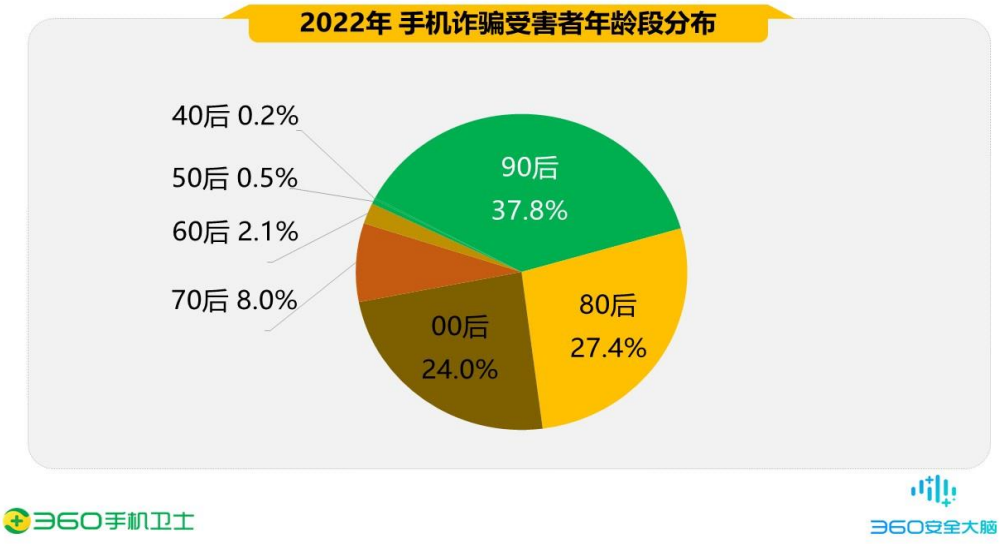

图 21 2022 年手机诈骗受害者年龄段分布

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。

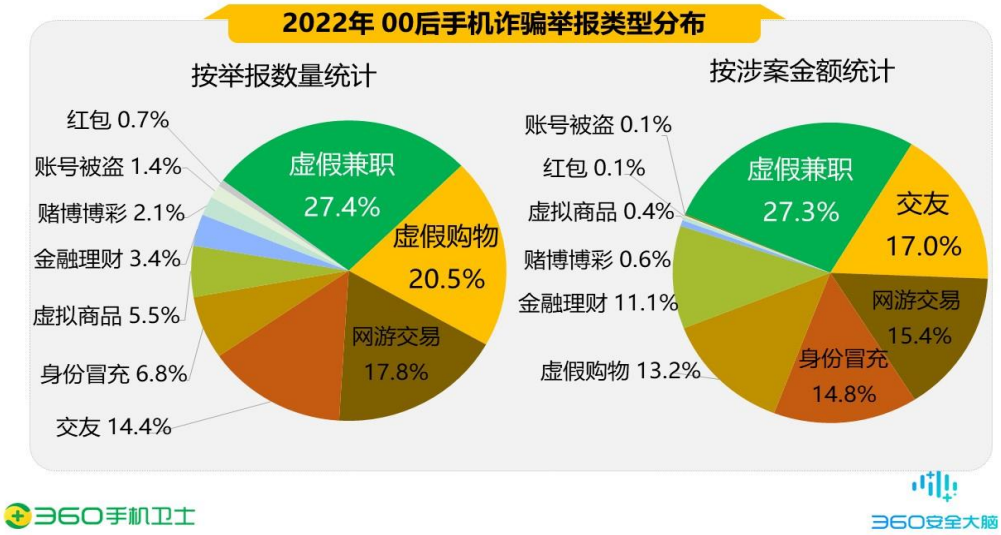

图 22 2022 年 00 后手机诈骗举报类型分布

从被骗网民的年龄段人数来看，2022 年度 90 后、80 后、00 后均为诈骗高发人群，90 后纷纷进入中年，成为家庭的顶梁柱，受到疫情、收入等客观影响，以及各类成功学、一夜暴富等信息洗脑，生活压力猛增，互联网成为其寻找感情寄托、增加额外收入的重要渠道。从数据上看，90 后中，男性为裸聊交友类的主要人群，女性为虚假兼职类的主要人群。

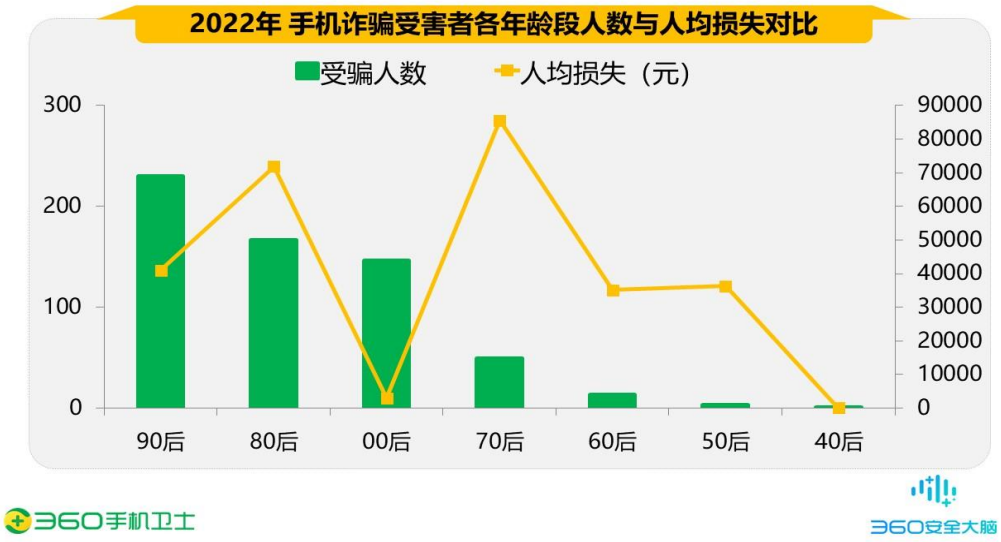

图 23 2022 年手机诈骗受害者各年龄段人数与人均损失对比

3. 受害者地域分布

2022 年度，从各地区手机诈骗的举报情况来看，山东（8.7%）、广东（8.5%）、河南（7.2%）、

江苏（6.6%）、河北（5.7%）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 36.8%。下图给出了 2022 年度手机诈骗举报数量最多的 10 个省份：

图 24 2022 年 手机诈骗举报数量 TOP10 省级分布

从各城市手机诈骗的举报情况来看，北京（4.9%）、西安（3.0%）、郑州（1.6%）、昆明（1.6%）、温州（1.5%）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 12.6%。下图给出了 2022 年度手机诈骗举报数量最多的 10 个城市：

图 25 2022 年 手机诈骗举报数量 TOP10 城市分布

二、场景识别

1. 移动端诈骗场景感染量与类型分布

2022 年全年，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 2245.4 万，下图为 2022 年度移动端各月诈骗场景感染量统计：

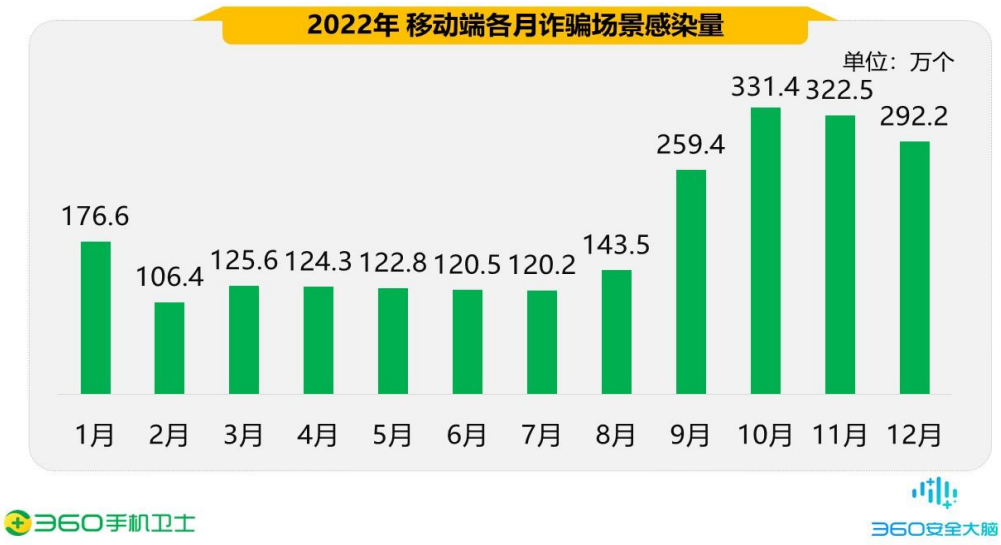

图 26 2022 年 移动端各月诈骗场景感染量

2022 年全年，移动端诈骗场景类型主要为刷单返利，占比 53.1%；其次为网络贷款（31.8%）、虚假投资理财（10.4%）、“杀猪盘”（2.6%）、裸聊敲诈（1.8%）和虚假招嫖（0.1%）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 通联应用增加了混淆、加固等攻防对抗手段，下半年在身份冒充类诈骗场景上，黑产逐渐采用电话引流+屏幕共享应用远程“操控”受害人进行转账或直接盗刷资金，360 安全大脑目前对此类场景、应用可以实现独家识别，下图为 2022 年度移动端诈骗场景类型分布：

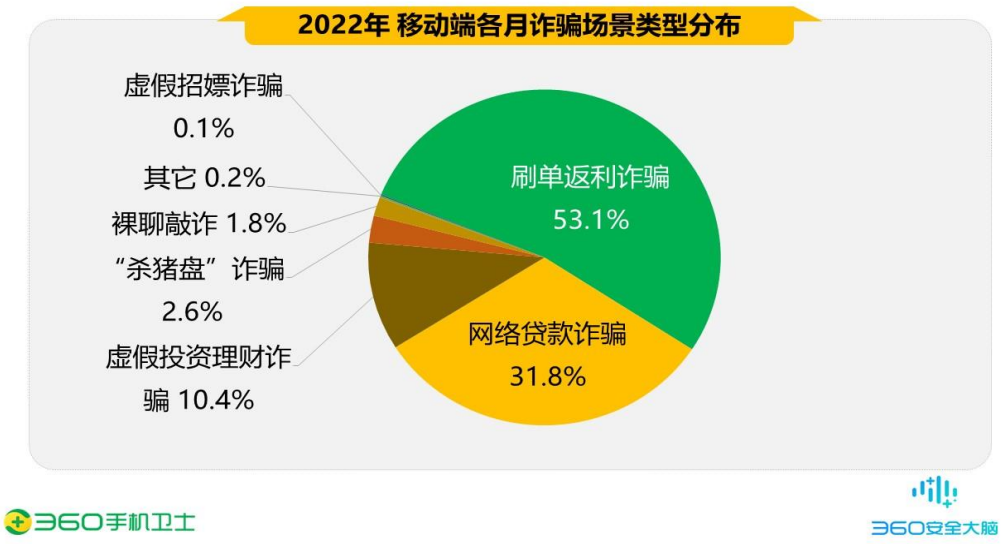

图 27 2022 年 移动端各月诈骗场景类型分布

2. 移动端诈骗场景感染量地域分布

2022 年全年，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 9.3%；其次为山东（6.8%）、河南（6.3%）、江苏（6.2%）、四川（6.1%），此外浙江、河北、湖南、云南、安徽的诈骗场景感染量也排在前列。

图 28 2022 年 移动端各月诈骗场景感染量 TOP10 省级分布

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 2.5%；其次为深圳（2.0%）、重庆（2.0%）、广州（1.9%）、西安（1.6%），此外郑州、苏州、武汉、昆明、杭州的诈骗场景感染量也排在前列。

图 29 2022 年 移动端各月诈骗场景感染量 TOP10 市级分布

三、恶意程序

1. 恶意程序新增样本量与类型分布

2022 年度，360 安全大脑共截获移动端新增恶意程序样本约 2407.9 万个，同比 2021 年度（943.1 个）上升了 155.3%，平均每天截获新增手机恶意程序样本约 6.6 万个。下图给出了 2013 年-2022 年移动端新增恶意程序样本量统计：

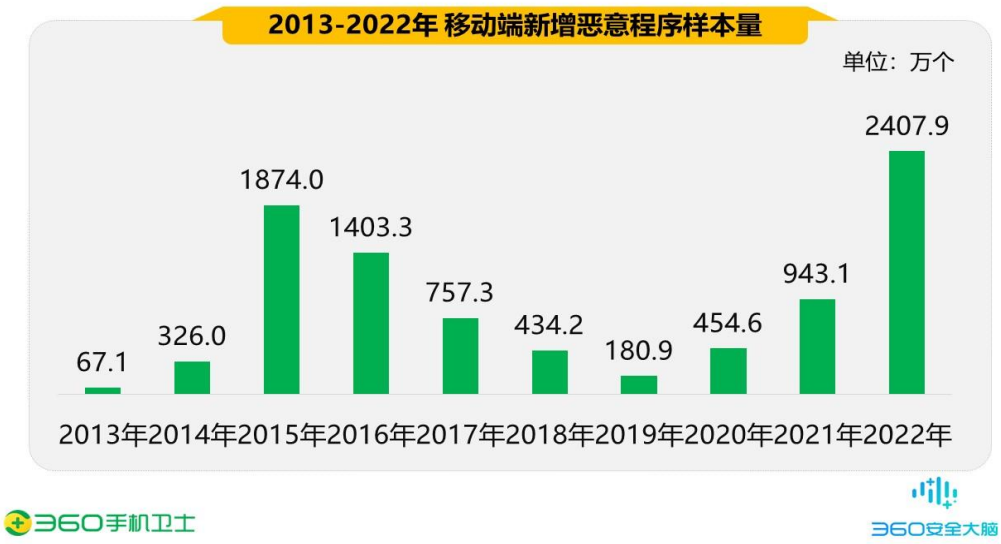

图 30 2013-2022 年 移动端新增恶意程序样本量

2022 年全年，从第三季度开始，新增样本量开始逐步增加，11 月达到峰值，具体分布如下图所示：

图 31 2022 年 移动端各月新增恶意程序样本量

2022 年度，移动端新增恶意程序类型主要为资费消耗，占比 97.2%；其次为隐私窃取

（1.4%）、违法违规（1.1%）、流氓行为（0.1%）、欺诈软件（0.1%）等。下图为 2022 年度移动端新增恶意程序类型分布：

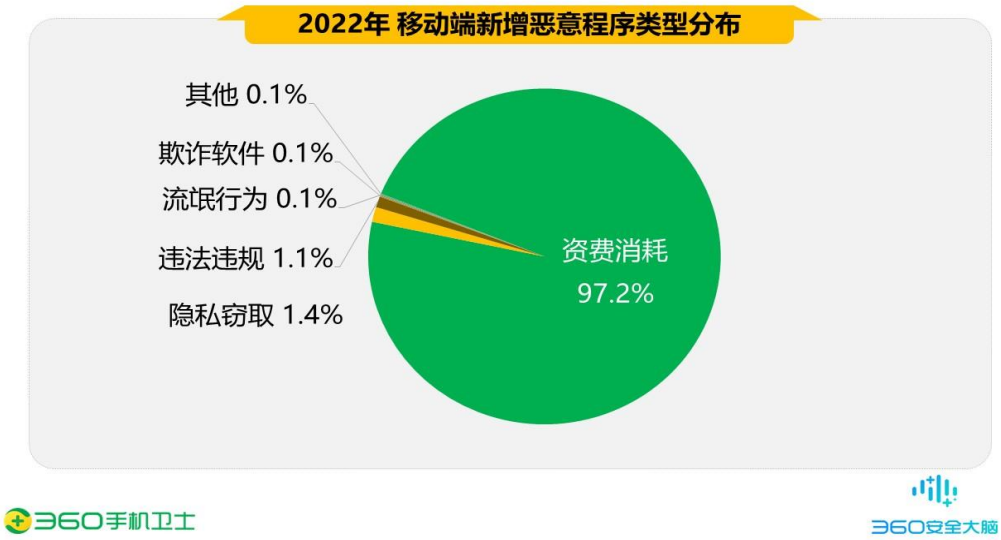

图 32 2022 年 移动端新增恶意程序类型分布

2. 恶意程序拦截量

2022 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 132.2 亿次，平均每天拦截手机恶意程序攻击约 3623.3 万次。下图为 2022 年度移动端各月恶意程序拦截量统计：

图 33 2022 年 移动端各月恶意程序拦截量

3. 恶意程序拦截量地域分布

2022 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 10.4%；其次为山东（7.7%）、河南（7.5%）、江苏（7.1%）、河北（5.6%），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。

图 34 2022 年 恶意程序拦截量 TOP10 省级分布

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（2.1%）、成都（2.0%）、北京（1.9%）、上海（1.8%），此外深圳、郑州、杭州、南京、苏州的恶意程序拦截量也排在前列。

图 35 2022 年 恶意程序拦截量 TOP10 市级分布

四、钓鱼网站

1. 移动端钓鱼网站拦截占比

2022 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 799.5 亿

次，同比 2021 年度（933.4 亿次）下降了 14.3%。其中，PC 端拦截量约为 795.2 亿次，占总拦截量的 99.5%，平均每日拦截量约 2.2 亿次；移动端拦截量约为 4.3 亿次，占总拦截量的 0.5%，平均每日拦截量约 117.4 万次。下图为 2022 年度钓鱼网站拦截占比分布：

图 36 2022 年 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 年度，360 安全大脑在移动端拦截钓鱼网站攻击约为 4.3 亿次，同比 2021 年度（5.6 亿次）下降 23.9%。下图为 2022 年度钓鱼网站各月拦截量分布：

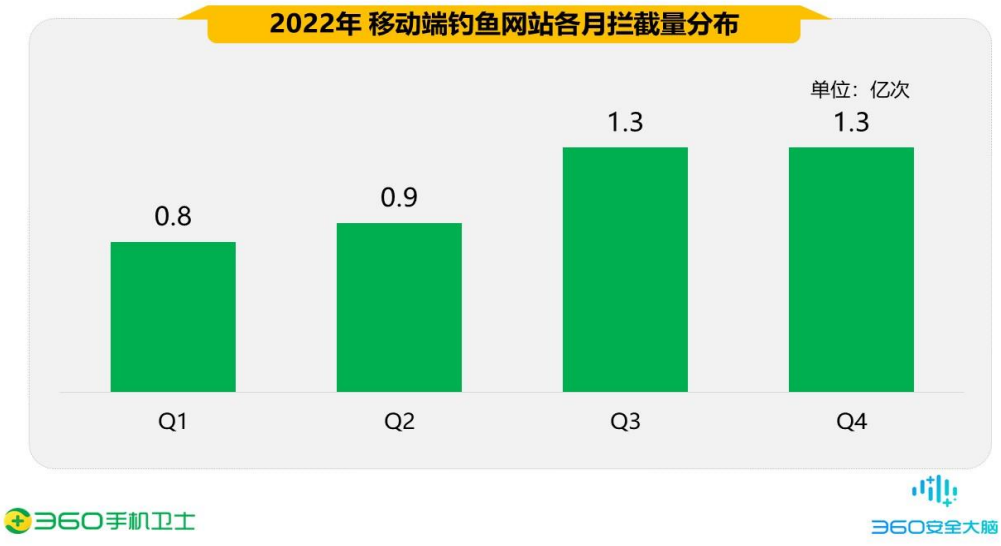

图 37 2022 年 移动端钓鱼网站各月拦截量分布

3. 移动端钓鱼网站类型分布

2022 年度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 65.1%；其次为色情

（26.7%）、金融证券（3.1%）、虚假购物（2.6%）、赌博（2.2%）等。下图为 2022 年度移动端拦截钓鱼网站类型分布：

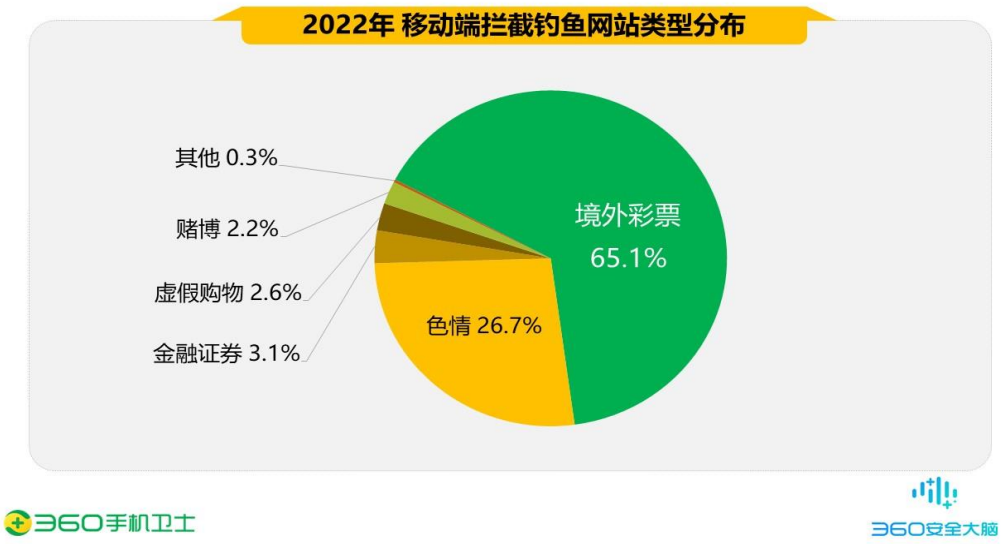

图 38 2022 年 移动端拦截钓鱼网站类型分布

4. 移动端钓鱼网站新增量

2022 年全年，360 安全大脑共截获各类新增钓鱼网站 1.9 亿个，同比 2021 年（1.6 亿个）上升了 23.0%，平均每天新增 52.7 万个。

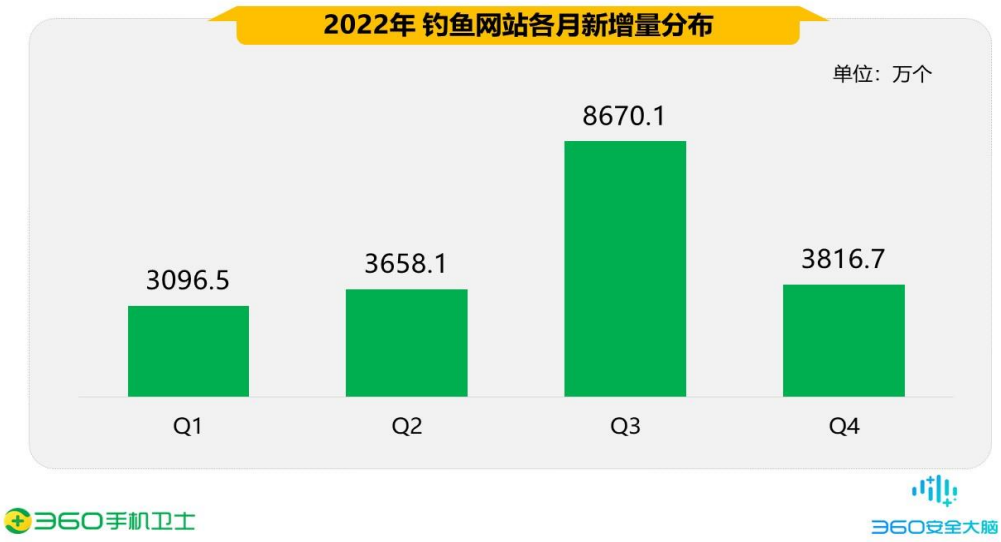

图 39 2022 年 钓鱼网站各月新增量分布

在钓鱼网站新增类型中，色情类占据首位，占比 54.5%；其次为赌博类，占比 39.7%。

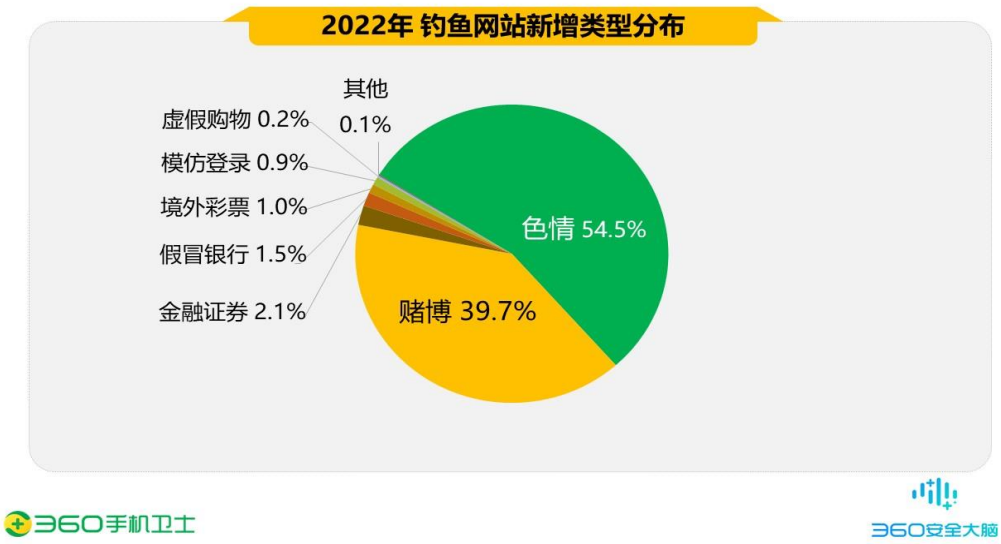

图 40 2022 年 钓鱼网站新增类型分布

5. 移动端钓鱼网站拦截量地域分布

2022 年全年，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 22.3%；其次为福建（8.6%）、广西（8.5%）、山东（5.0%）、湖南（4.8%），此外浙江、江苏、河南、河北、四川的钓鱼网站拦截量也排在前列。

图 41 2022 年 移动端钓鱼网站拦截量 TOP10 省级分布

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%；其次为深圳（3.3%）、南宁（2.7%）、北京（2.5%）、上海（2.3%），此外东莞、福州、佛山、泉州、重庆的钓鱼网站拦截量也排在前列。

图 42 2022 年 移动端钓鱼网站拦截量 TOP10 市级分布

五、骚扰电话

1. 骚扰电话拦截量

2022 年全年，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 233.9 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。环比 2021 年（228.0 亿次）上涨了 2.6%。下图给出了 2014 年-2022 年用户标记骚扰电话拦截号码次数统计：

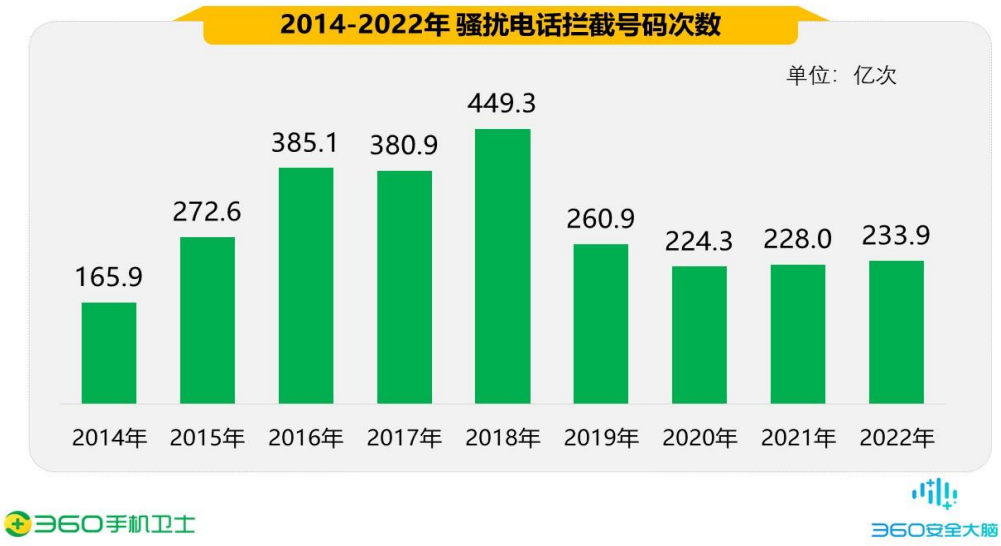

图 43 2014-2022 年 骚扰电话拦截号码次数

下图为 2022 年骚扰电话各月拦截号码次数分布：

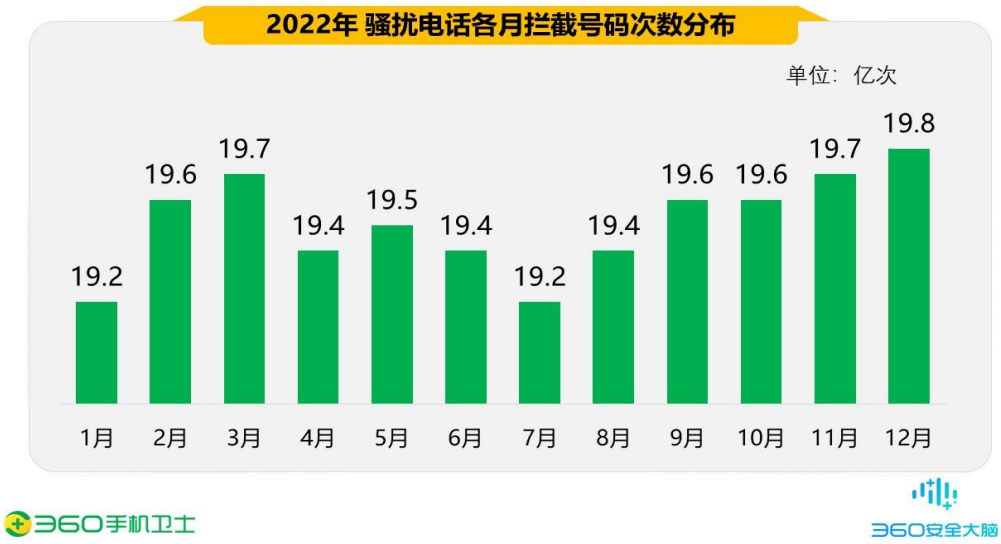

图 44 2022 年 骚扰电话各月拦截号码次数分布

下图为 2022 年识别与拦截骚扰电话趋势统计：

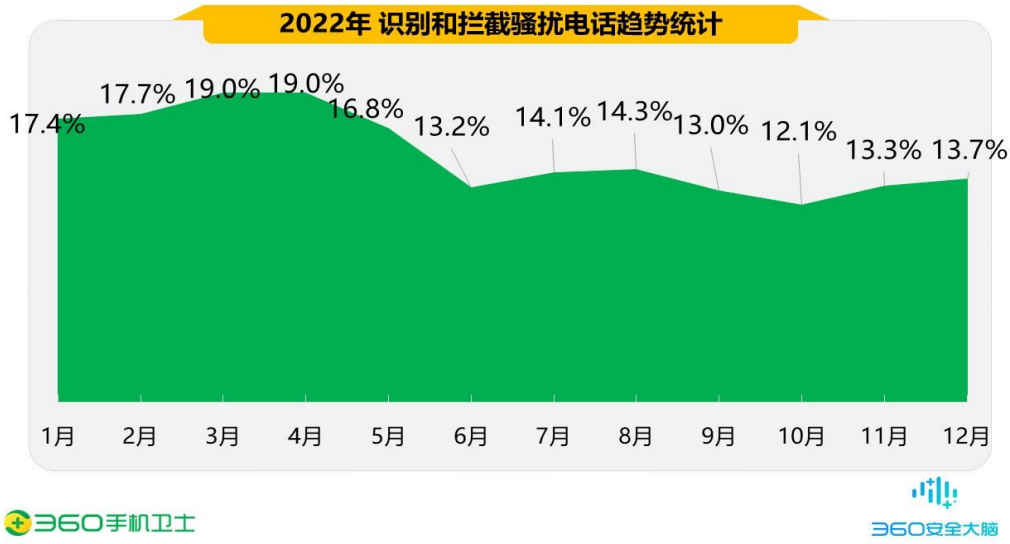

图 45 2022 年 识别和拦截骚扰电话趋势统计

2. 骚扰电话拦截类型分布

2022 年全年，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 89.6%的比例位高居首位；其次为广告推销（6.2%）、房产中介（2.7%）、疑似欺诈（1.0%）、保险理财（0.3%）、招聘猎头（0.1%）与响一声（0.1%）。下图为 2022 年骚扰电话拦截类型分布：

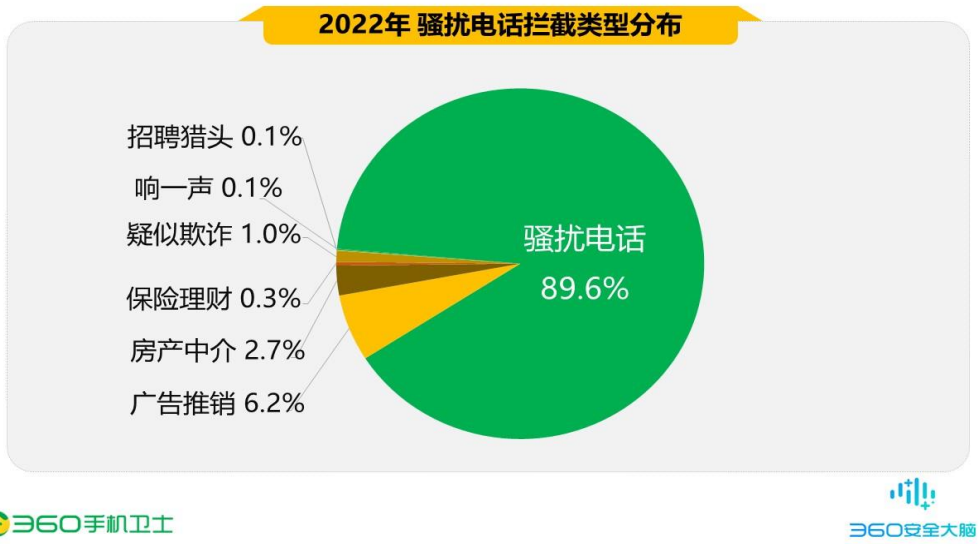

图 46 2022 年 骚扰电话拦截类型分布

3. 骚扰电话拦截号码号源分布

2022 年全年，从骚扰电话拦截号码个数分布来看，被拦截号码为固话最多，占比高达 41.3%；其次为运营商为中国联通的个人手机号（21.0%）、运营商为中国移动的个人手机号（19.1%）、虚拟运营商（10.1%）、运营商为中国电信的个人手机号（7.9%）与 95/96 开头号段（0.4%）等。下图为 2022 年骚扰电话拦截号码号源分布：

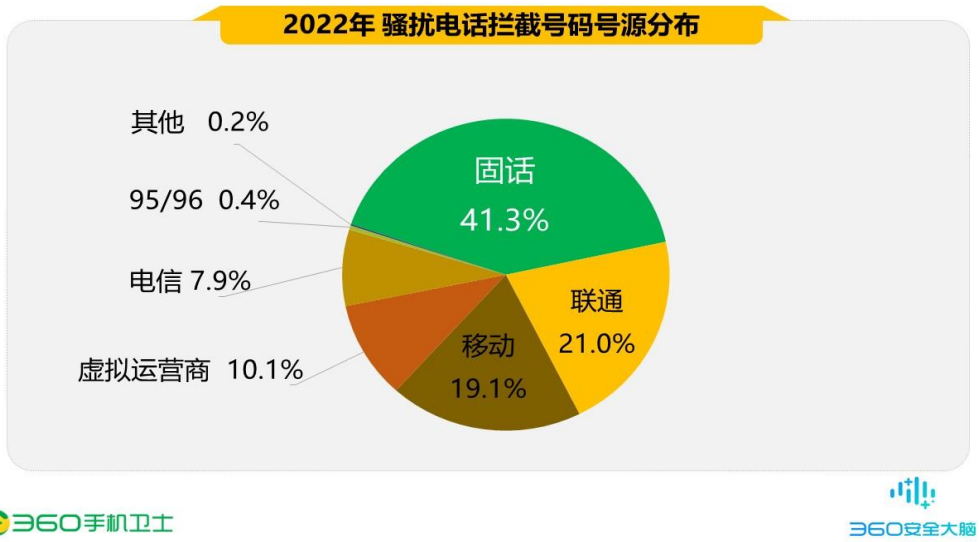

图 47 2022 年 骚扰电话拦截号码号源分布

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 88.3%；虚拟运营商也是骚扰电话类占据首位，占比 76.6%。95/96 号段与虚拟运营商号码遭不法分子利用，仍是不法分子从事非法行径的主要“工具”之一。

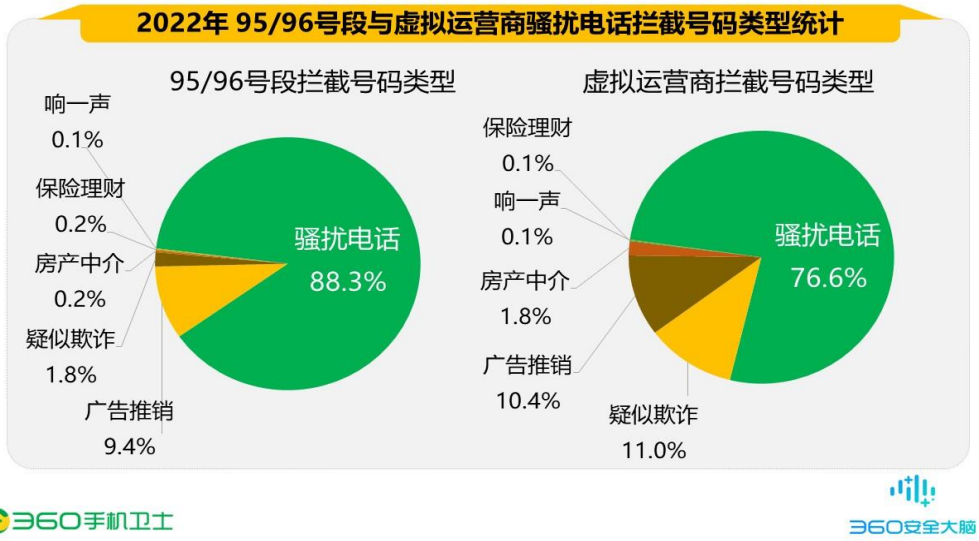

图 48 2022 年 95/96 号段与虚拟运营商骚扰电话拦截号码类型统计

4. 骚扰电话归属地分布

2022 年全年，从各地骚扰电话拦截量上分析，广东省用户标记骚扰电话拦截量最多，占全国骚扰电话拦截量的 13.6%；其次是山东（7.8%）、江苏（7.0%）、河南（5.6%）、浙江（4.9%），此外四川、河北、北京、湖南、湖北的骚扰电话拦截量也排在前列。

图 49 2022 年 骚扰电话拦截量 TOP10 省级分布

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 4.0%；其次是广州（3.9%）、上海（3.3%）、深圳（2.9%）、成都（2.7%），此外重庆、杭州、西安、郑州、武汉的骚扰电话拦截量也排在前列。

图 50 2022 年 骚扰电话拦截量 TOP10 城市分布

六、垃圾短信

1. 垃圾短信拦截量

2022 年全年，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 91.6 亿条，同比 2021 年（167.2 亿条）下降了 45.2%，平均每日拦截垃圾短信约 2510.6 万条。

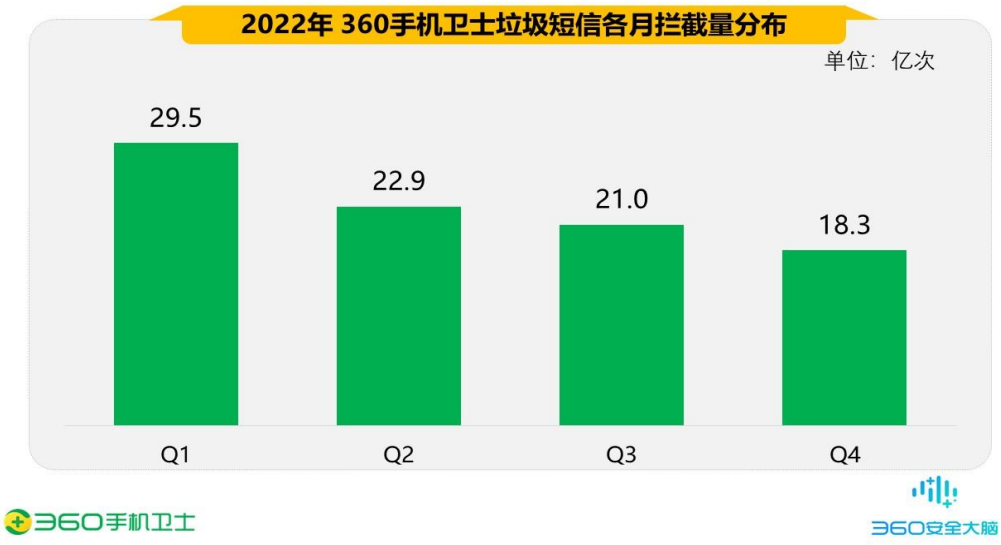

图 51 2022 年 360 手机卫士垃圾短信各月拦截量分布

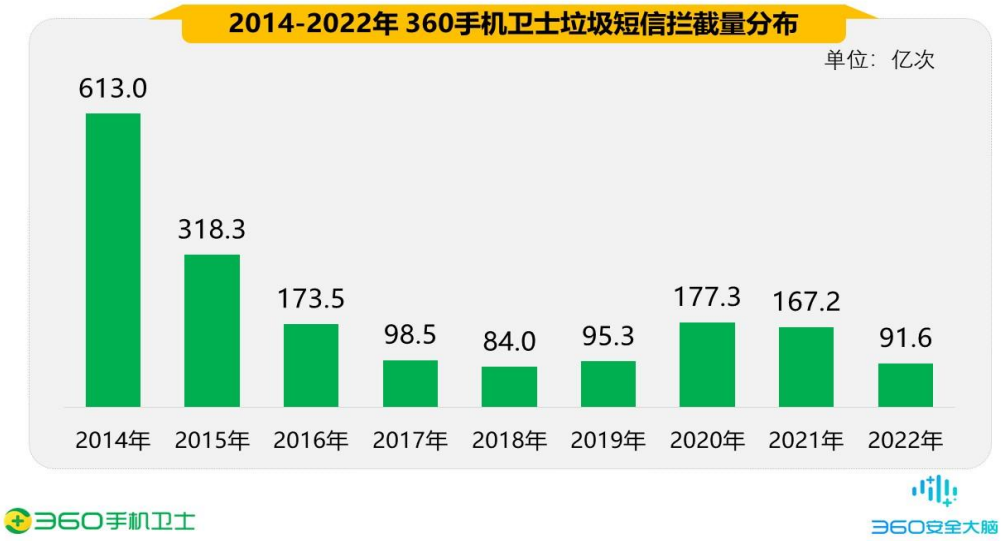

图 52 2014-2022 年 360 手机卫士垃圾短信拦截量分布

2. 垃圾短信类型分析

2022 年全年，垃圾短信的类型分布中广告推销短信最多，占比为 95.8%；诈骗短信占比 4.1%；违法短信占比 0.1%。

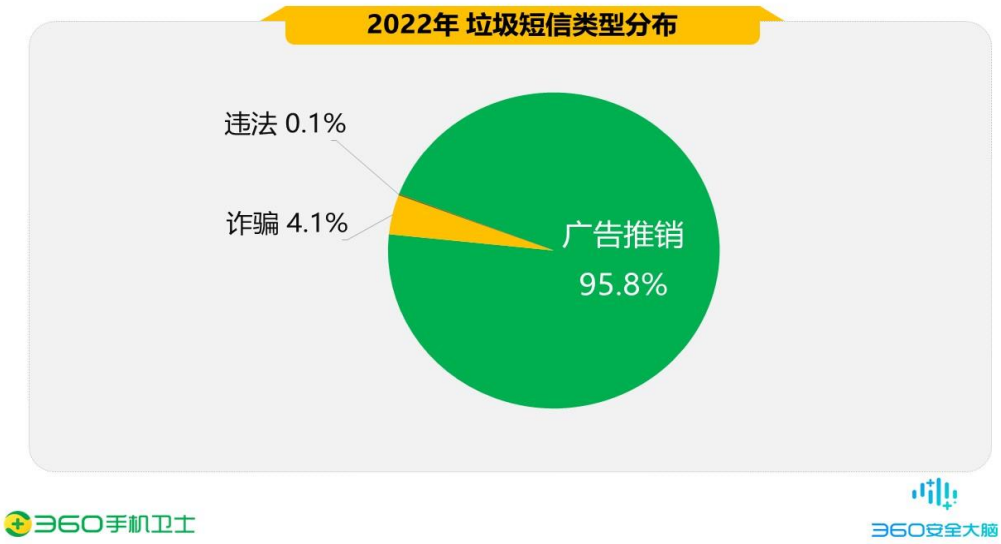

图 53 2022 年 垃圾短信类型分布

从诈骗短信拦截类型来看，诈骗短信以 69.1%的比例位居首位；其次为疑似伪装诈骗（19.0%）、赌博诈骗（9.9%）、兼职诈骗（0.9%）、股票诈骗（0.9%）等。下图为 2022 年诈骗短信子类型分布：

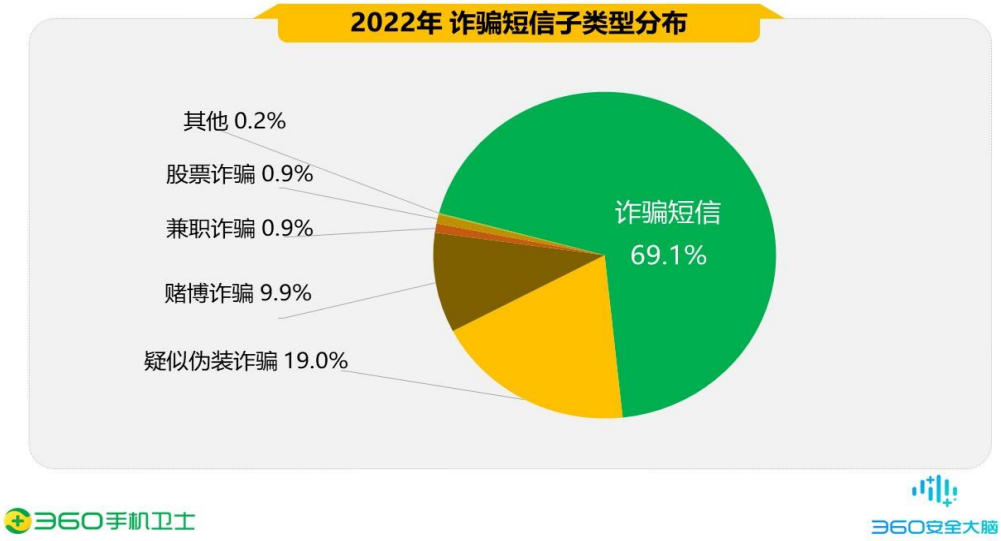

图 54 2022 年 诈骗短信子类型分布

从违法短信拦截类型来看，违法金融信贷短信以 85.2%的比例位居首位；其次为其他违法短信（11.8%）、疑似伪基站发送（1.3%）、售卖信息（0.9%）与色情短信（0.8%）。下图为 2022 年违法短信子类型分布：

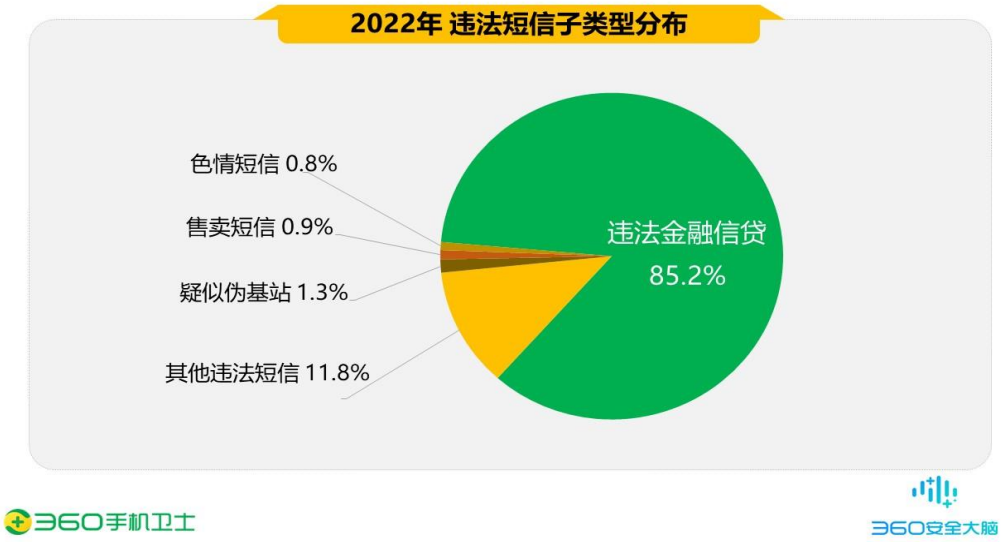

图 55 2022 年 违法短信子类型分布

3. 垃圾短信发送者运营商号源分布

2022年全年，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96.1%；利用其他号段传播垃圾短信占比约 3.9%。下图为 2022 年短信平台发送垃圾短信占比分布：

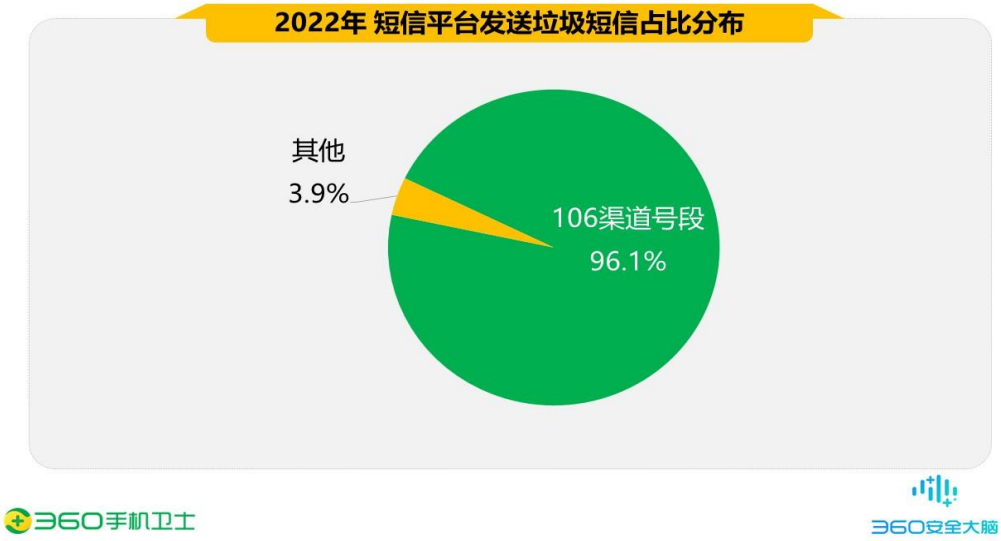

图 56 2022 年 短信平台发送垃圾短信占比分布

2022 年全年，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，利用虚拟运营商发送垃圾短信的最多，占比 33.3%；其次是 95/96 号段（28.9%）、固话（12.9%）、运营商为中国移动的个人手机号（11.5%）、运营商为中国电信的个人手机号（4.7%）、运营商为中国联通的个人手机号（4.3%）与 14 物联网卡（1.4%）等。

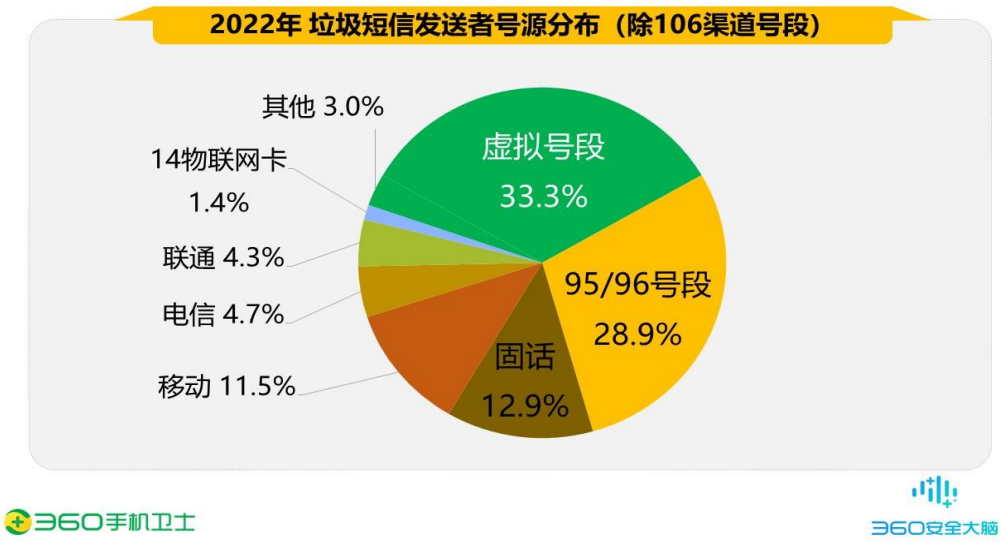

图 57 2022 年 垃圾短信发送者号源分布（除 106 渠道号段）

4. 垃圾短信拦截量地域分析

2022 年全年，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（10.0%）、江苏（8.2%）、山东（6.5%）、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。

图 58 2022 年 垃圾短信拦截量 TOP10 省级分布

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 11.3%；其次是广州（9.1%）、深圳（4.4%）、南京（4.3%）、上海（3.5%），此外重庆、成都、杭州、郑州、武汉的垃圾短信拦截量也排在前列。

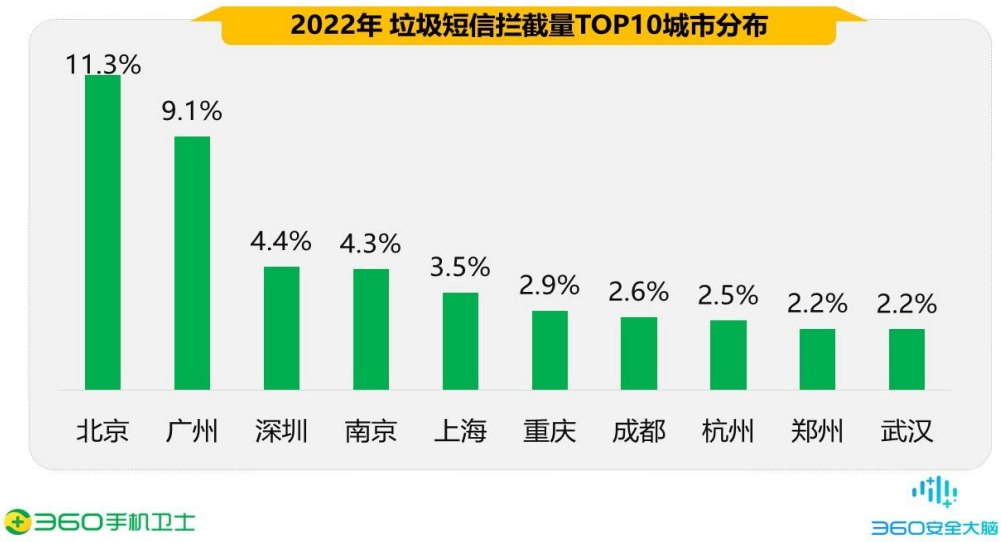

图 59 2022 年 垃圾短信拦截量 TOP10 城市分布