2021 年上半年度
中国手机安全状况报告

2021 年 08 月 23 日

前言

在万物互联的大数据时代，传统犯罪不断向网络空间发展，呈现出传统犯罪网络化、网络犯罪常态化的犯罪大趋势。信息窃取、电信网络诈骗、网络洗钱等行为，以及隐藏在背后的工具、资源、平台、渠道已经形成了一系列稳定且生态化的黑灰产业链条。

近几年，移动安全领域的问题日趋复杂，网络生态环境日益恶劣。从涉案金额和诈骗手法上看，1600 万元、1.17 亿元、2.5 亿港元这些触目惊心的数字，是近几年全国各地群众被诈骗分子用冒充“公检法”手段诈骗的金额，甚至出现执法民警对正在遭受电信网络诈骗的受害人进行上门劝阻时，反被当作“假警察”闭门不见的报道。从黑产链条上看，发卡平台已成为了黑灰产资源供应中的重要一环，在整体黑灰产业链，承担中坚力量。发卡平台的便利，间接造就了黑灰产资源、羊毛党、诈骗团伙的泛滥。 从攻防技术上看，诈骗团伙为掌控整个诈骗环境，逐步将受害人引流至使用第三方聊天 SDK 搭建的聊天软件中，在聊天软件中内嵌诈骗平台，形成诈骗生态闭环。

现阶段，黑灰产犯罪行为更专业，职能更精细，诈骗分子不断迭代技术、升级话术、优化分工，采用更为“职业化”的方式实施诈骗。各类犯罪团伙间“亲密无间”的合作模式也日益显著，导致技术对抗性的难度加大，新技术将会带来新的挑战。

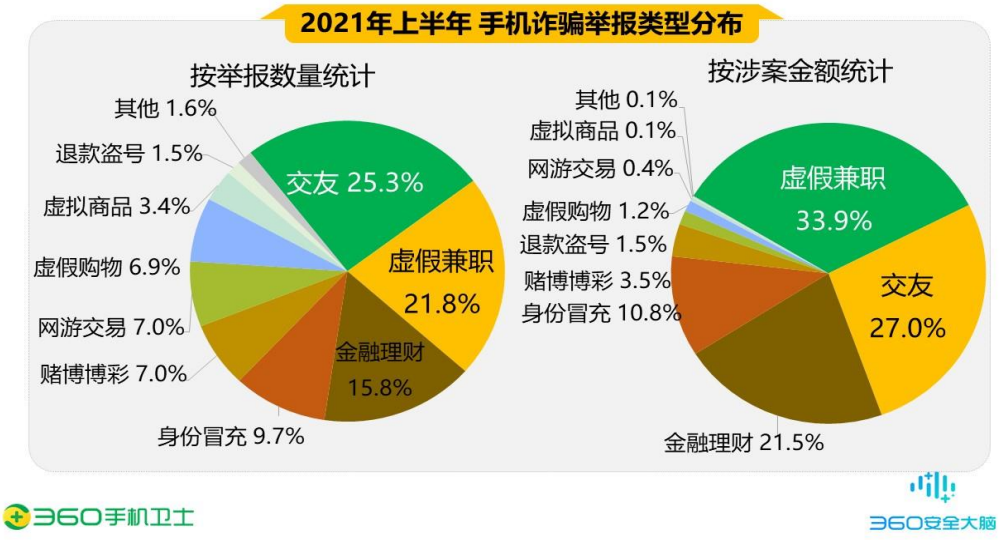
《2021 年上半年度中国手机安全报告》将从黑灰产业链、热门黑产项目、热门诈骗手法、最新攻防手段、各维度数据入手，深度剖析黑灰产业。360 将积极发挥自身技术优势，综合运用人工智能、大数据、云计算等技术手段有效打击涉诈产业链，维护用户移动信息安全。

目录

第一章 2021 年上半年度手机诈骗概况

一、 报案数量与类型

2021 上半年度 360 手机先赔共接到手机诈骗举报 1371 起。其中诈骗申请 669 起，涉案总金额高达 1425.2 万元，人均损失 21304 元。在所有诈骗申请中，交友占比最高达 25.3%；其次是虚假兼职（21.8%）、金融理财（15.8%）、身份冒充（9.7%）、赌博博彩（7.0%）等。从涉案总金额来看，虚假兼职类诈骗总金额最高，达 483.0 万元，占比 33.9%；其次是交友类诈骗，涉案总金额 385.5 万元，占比 27.0%；金融理财排第三，涉案总金额为 305.9 万元，占比 21.5%。下图为 2021 年上半年度手机诈骗的举报类型与涉案金额分布情况：



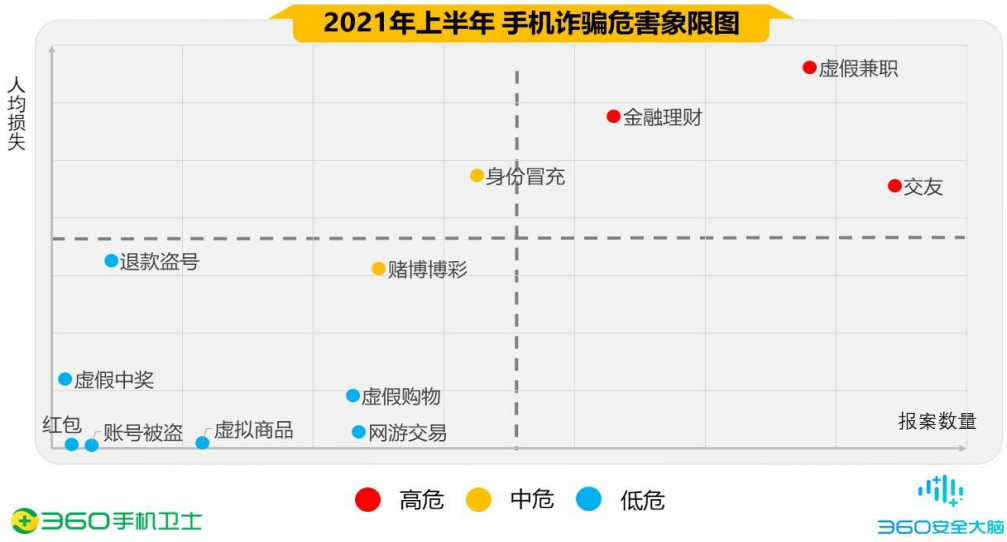
2021 年上半年度，手机诈骗中交友、虚假兼职、金融理财仍属于高危诈骗类型；身份冒充、赌博博彩属于中危诈骗类型。其中，虚假兼职类人均损失最高，约 3.3 万元；其次为金融理财类人均损失约为 2.9 万元。

1） 交友类诈骗仍以裸聊遭欺诈为主，从诈骗手法上看，不法分子仍是以视频裸聊为名，诱导受害人安装含有盗取用户通讯录信息的恶意应用。在录取受害人裸聊视频后，以将裸聊视频群发给受害人朋友为名进行敲诈勒索。从诈骗团伙话术上看，不法分子会针对不同心理的受害人群“定制化”诈骗话术，同时从长相、年龄等方面筛选目标受害者。

2） 上半年发现的虚假兼职类诈骗，在短信、电话、社交软件等传统渠道基础上，增加了短视频、新媒体等引流渠道。由于现在用户已经具有一定的防骗意识，在引流话术上，从之前的“日赚百元”的强感知刷单噱头转变为“购物好评送礼”的隐蔽话术，降低用户对于刷单

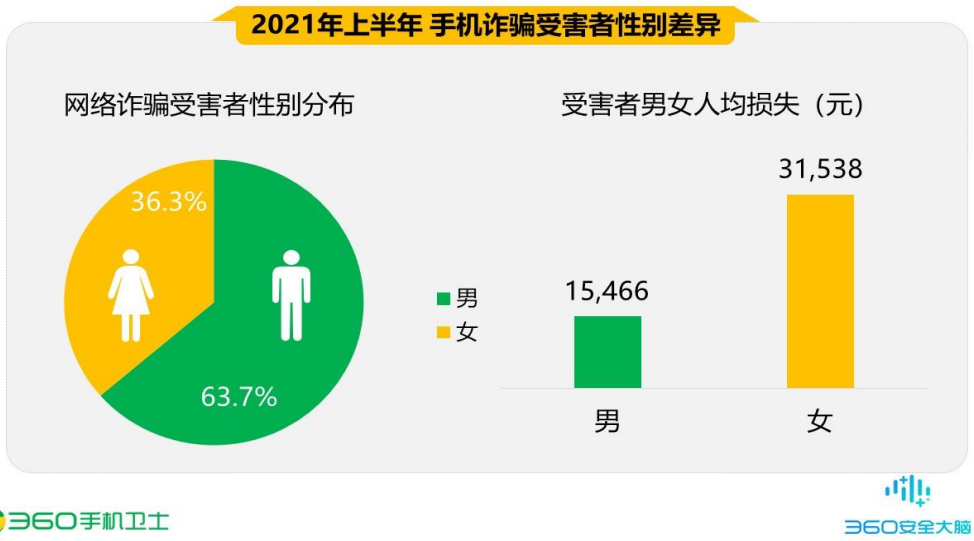
的抵触心理。在诈骗实施过程中，虚假兼职平台开始将自己嵌入到聊天软件中，作为一种新的引流方式诱导受害人付款。

3） 上半年度金融理财类诈骗仍以虚假网络贷款为主，一直呈现高发态势。但近期发现，仅次于虚假贷款的投资理财诈骗中，出现传统微盘诈骗的升级版。传统的微盘诈骗，以兼职赚钱或交友为名，引导用户至点位盘平台，对标的股票、贵金属、虚拟货币进行买涨或买跌的投机行为。而“升级版”诈骗，精心借助大量处于跑路阶段的 P2P 平台，出借人无法回本的背景，在一些新闻网站，以 P2P 平台收到国家要求进行回款为幌子进行引流。用户按照操作，初期会获得盈利，后期在平台进行大额充值后发现被骗。

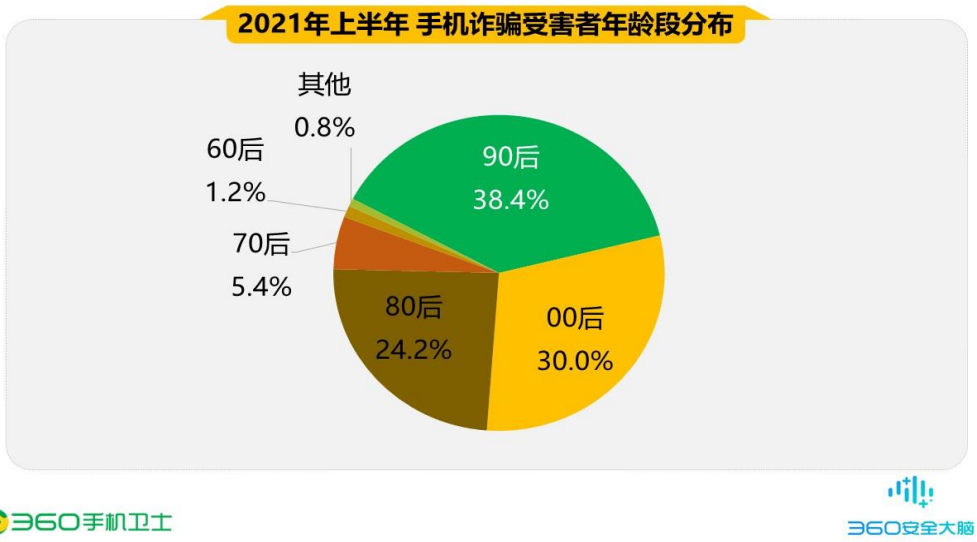


二、 受害者性别与年龄

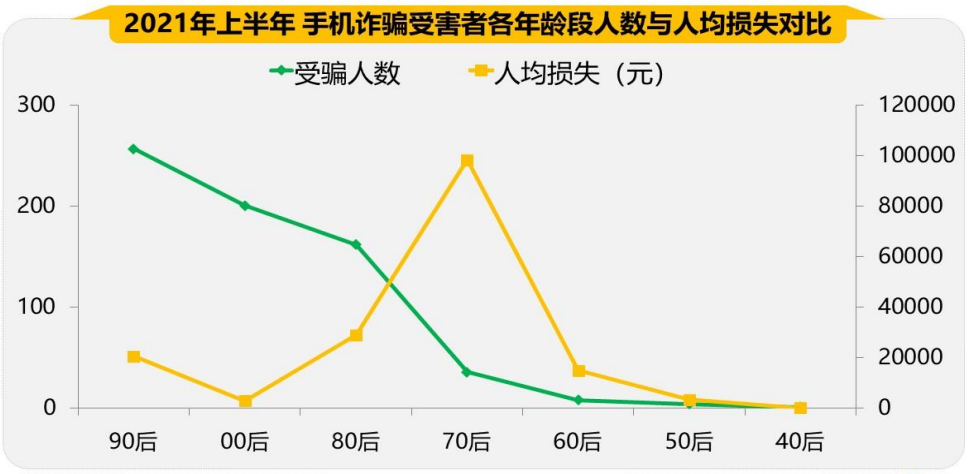
2021 年上半年度，从举报用户的性别差异来看，男性受害者占 63.7%，女性占 36.3%，男性受害者占比高于女性。从人均损失来看，男性为 15466 元，女性为 31538 元，男性人均损失低于女性。下图为 2021 年上半年度手机诈骗受害者性别差异：



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 38.4%，仍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 30.0%；80 后占比为 24.2%；70 后占比为 5.4%、60 后占比为 1.2%等。下图为 2021 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及人均损失来看，2021 年上半年，90 后受骗人数最多，但是 70 后人群人均损失最重。其中 90 后人群的受骗类型以裸聊交友为主，他们平时爱上网且心存猎奇，喜欢寻求视觉刺激，一不小心就成为裸聊诈骗团伙囊中“猎物”，一旦被入圈套，由于经验不足，被裸聊诈骗团伙几经“敲打”，就不得不“缴械投降”。而 70 后人均损失最高，主要原因在于其防范意识相对较为薄弱，易于点击欺诈短信中的钓鱼网址，填写个人信息以及银行卡信息，导致资金被盗刷。



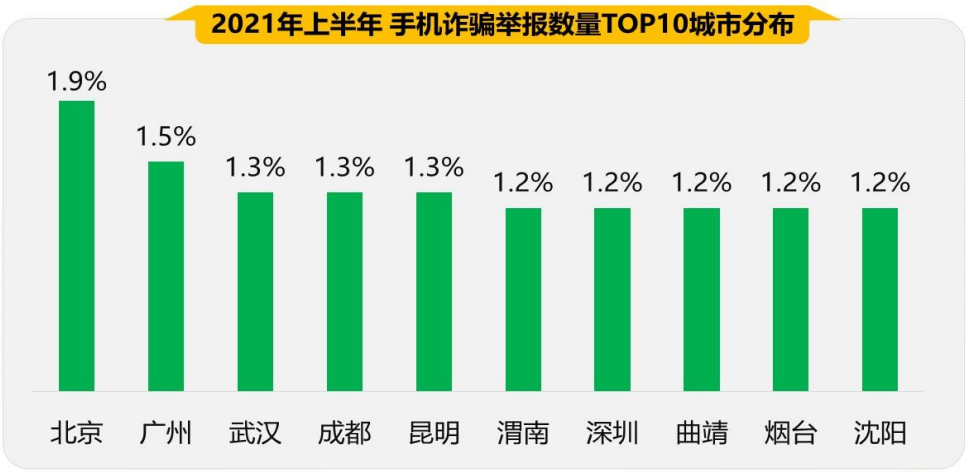
360手机卫士　360安全大脑

三、 受害者地域分布

2021 年上半年度，从各地区手机诈骗的举报情况来看，山东（9.9%）、广东（7.5%）、四川（6.0%）、河南（5.7%）、河北（4.9%）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 33.9%。下图给出了 2021 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（1.9%）、广州（1.5%）、武汉（1.3%）、成都（1.3%）、昆明（1.3%）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 7.5%。下图给出了 2021 年上半年度手机诈骗举报数量最多的 10 个城市：



360手机卫士　360安全大脑

第二章　黑灰产趋势及攻防技术原理分析

一、　冒充公检法诈骗背后的套路

1600 万元、1.17 亿元、2.5 亿港元这些触目惊心的数字，是近几年全国各地群众被诈骗分子用冒充“公检法”手段诈骗的金额。而冒充“公检法”类诈骗，也是诈骗案件中最常用、手段变化最多、金额损失最大的犯案手法之一。甚至出现执法民警对正在遭受电信网络诈骗的受害人进行上门劝阻时，反被当作“假警察”闭门不见的报道。如不有效打击该犯案手法，将后患无穷，故本报告将结合实际案件的真实过程，详细剖析冒充公检法诈骗手法、涉及的网站、APP 特点及识别方式。

1. 冒充“公检法”诈骗流程、话术

骗子通过非法渠道获取受害人身份等信息，冒充“公安局、通信管理局、国家安全局、中国香港国安局、互联网举报中心、社保局”等企事业单位工作人员给受害人打电话，编造受害人涉嫌洗钱/非法集资/出售假货/出售银行卡/出售手机卡/注册诈骗公司/发布传播违法违规信息/非法入境等理由，诱导受害人查看伪造的公检法网站、通缉令、财产冻结书等，对受害人进行威逼、恐吓。一旦受害人相信，就会诱导受害人去宾馆等独立空间进行深度“洗脑”，以帮助受害人洗脱罪名为由，要求受害人将名下账户所有钱款转账至所谓的“安全账户”，或使用钓鱼网址、恶意应用盗刷受害人的银行账户信息。由于冒充的身份不同，诈骗剧本会有所不同，以下为冒充不同身份涉及的话术。

（1）冒充 “法院”

自称是受害人所在地“法院”工作人员，法院办理洗钱案件中发现洗钱团伙使用的银行卡是用受害人身份信息办理的，需要受害人前往案件所在地法院（异地）澄清，此时受害人出于时间、路程等角度会表示去不了，诈骗团伙便开始引导添加“公安”QQ 或通过视频配合办案。

（2）冒充“公安局”

在该类案件中，受害人先接到自称是“公安局”民警来电，表示一名“嫌疑人”用受害人身份拐卖人口，称银行有大量资金流动。引导受害人添加“公安”QQ，查看资金冻结的证据，展示针对受害人的“通缉令”。

（3）冒充“通信管理局”

犯罪分子自称是“通信管理局”的工作人员，受害人其手机号码注册的微信，涉嫌在微信朋友圈发布违法犯罪信息，“腾讯”投诉后，已经被公安机关立案了，在受害人表示没有此事后，随即给用户转接“公安”电话、添加“公安”的 QQ。

为加强受害人的信任度，诈骗分子会在沟通期间开启视频通话，给用户播放“身着警服伪装警察”的合成视频。进而要求受害人访问指定网址，查看自己的通缉令、逮捕令。以保障受害人资产安全为幌子，要求受害人访问指定网站，下载“安全防护”程序，在网站、及安全程序中填写银行账户信息。当掌握到受害人的银行账户信息后，一方面盗刷银行卡里的资金，一方面引导受害人在多个贷款平台申请贷款，并提现至受害人的银行账户资金中再次盗刷。

2. 冒充“公检法”诈骗工具特点、作用

从上述诈骗过程中，骗子们花费最大精力为受害人营造的就是伪“公安”通告环节，受害者因此被骗子的“证据”洗脑进而误信。随着时间的推移，互联网技术的发展，冒充“公检法”类诈骗涉及的电话、网站、恶意应用等工具纷纷进行了技术手段升级。

冒充“公检法”诈骗中涉及的钓鱼网站、恶意应用，主要用于给用户展示通缉令及诱导受害人在页面内填写个人银行账户信息。常见的冒充“公检法”诈骗网页大同小异，特征也十分明显。目前存在以下 2 类，即验证码与服务端进行数据校验，当验证码不正确时，无法进入下级页面，这样即使收录到网址，也无法深入分析。

第一种网站标题为“login web”，页面内容要求输入“案件编号”，当填写的编号错误时，提示“编号不存在”，其中页面中的 “请输入编号”、“案件标号”为图片超链接。第二种网站标题为“安全检测”，页面内容要求输入“登录账号”，当输入 3 次错误时，会增加验证码校验。

当校验成功后，会跳转至下图展示的虚假公检法网站，其主要包含案件管理、网上清查、安全软件、手机安全软件四个用于诈骗的板块。

该系统中的案件管理（犯罪通缉追查系统），主要引导受害人在页面左侧，选择所犯罪行为（“危害公共安全罪”、“妨害社会管理秩序罪”、“贪污贿赂罪”、“毒品防治罪”、“走私罪”、“违反枪炮弹药管制罪”、“侵犯财产罪”、“恐吓勒索罪”、“金融洗钱罪”），使用“专案验证码”（受害人身份证号码），查询自己的通缉令。

网上清查（资金清查），主要是引导受害人输入自己的银行账户信息，包含开户银行、银行卡密码、U 盾密码。当受害人在页面填写信息后，会将此些信息提交至诈骗团伙服务器。

安全软件板块，Windows 版安全软件下载链，主要是对受害人的电脑进行监控。当受害人电脑安装并运行该程序后，该程序会释放 TeamViewer（远程控制类软件）进程，进而远程控制受害人的电脑。

手机安全软件板块，安全防护 APP 下载链。当受害人安装此安全防护 APP，输入特定的验证码、并授予该 APP 拨打电话、短信、通讯录、通话记录等权限后，安全防护 APP 会上传手机设备信息，接管并替代手机短信功能，备份并上传手机最近 50 条短信，配置呼叫转移逻辑完成呼叫转移号码设置，此时受害人手机无法接听外部呼入来电。当受害人在安全防护 APP，文号查询板块输入银行账户信息后，信息随即上传至诈骗团伙服务器。检测到受害人收到新的短信时，也立即上传至服务器，此时受害人的手机信息、银行卡账户信息完全掌握在诈骗团伙手中，可随时盗刷受害人银行账户资金。

二、 黑产聊天软件技术演变

1. 黑产使用的聊天软件演变过程

互联网发展早期，信息传播渠道较为单一，黑灰产主要通过短信、电话、交友软件、邮箱等传统渠道引流吸引用户关注，衍生出提供 QQ 信封、卡池等渠道商。手机号实名制、社交平台账号举报机制的完善，黑灰产人员使用的账号“存活期”遭到压缩。

伴随着互联网产业和技术的逐步发展，黑灰产从业人员得以技术迭代，衍生了云控产业，即通过电脑远程控制多个手机设备，实现批量账号管理；再借助一些养号策略，实现对批量社交账号的注册、养号，解决黑灰产社交号码短缺、号码被封、号码校验机制等问题。针对电信网络诈骗犯罪活动猖獗、严重侵害人民群众财产安全的情况，国家多部门重拳打击整治电信网络诈骗犯罪，诈骗使用的“获客引流”及与“受害人”联系的渠道空间受到打击。

API 技术的发展，黑灰产从业人员又挖空心思，开始将第三方在线客服系统集成到诈骗网站或 APP 中，以此规避传统社交软件账号易被封的问题。由于部分在线客服平台是网页形式，访客每次访问时系统会刷新页面，并不给访客展示之前的聊天记录，受害人很难保存受骗聊天资料。拥有技术能力的团伙甚至使用开源的客服系统搭建客服平台，相对于第三方在线客服平台而言，此种开源客户系统摆脱了第三方平台的“掣肘”，基本实现了在线客服平台完全可控，

并将聊天记录本地化。以下某诈骗平台内嵌的第三方在线客服平台网址。

2021 年第二季度，我们发现黑灰产为进一步增加识别难度，逐渐开始加强对内嵌的第三方在线客服链接进行保护。当用户在钓鱼网站内与客服进行交流时，原先是通过新窗口的形式，弹出在线客服页面，此种方式用户可以直接看到在线客服的网址，于是衍生出了原页面展示聊天界面的方式，即将聊天客服界面内嵌在网站内，用户看到的仍是原网址。同时对网站内容进行保护，无法通过技术手段查找内嵌的第三方在线客服链接。

部分诈骗团伙为掌控整个诈骗环境，开始将受害人引流至使用第三方聊天 SDK 搭建的聊天软件中，在聊天软件中内嵌诈骗平台，既可与受害人交流，也可快速安排受害人访问涉诈网站。为增加安全防护，还对诈骗平台加一层邀请码保护机制，这样即使样本被发现，也无法窥探其内部的数据，甚至压根儿都发现不了里面还内嵌一个诈骗平台，手段隐蔽性极高。

2. 内嵌诈骗平台的聊天软件剖析

2021 年 1 月，有用户通过 360 手机卫士反馈，其添加了网络兼职放单人员的微信后，对方描述“兼职需先使用指定的 MT 聊天软件，添加指定的接待员 MT 账户进行任务领取”。用户使用 MT 聊天软件，联系上该接待员后，对方进而告知此兼职活动是帮助商家推广数字货币交易量，该货币交易所目前需要上市，需要任务员帮忙刷交易数。随后接待员引导用户在 MT 软件中的发现板块，使用邀请码注册 MT 交易平台。用户完成注册后，接待员给用户发布刷交易量任务，用户首次获得收益并成功提现，后期任务金额越来越大，且无法提现，得知受骗。

通过分析发现，MT 聊天软件包含四个功能板块，分别为聊天、通讯录、发现、我的，仅从界面上看，这仅仅是个聊天软件，并没有涉嫌诈骗的内容，但点击应用首页的发现板块，填写指定的邀请码注册后可发现其隐藏的虚拟货币平台。

MT 聊天应用的主界面，调用的是域名 mt.50****.com；虚拟货币交易界面，调用的是域名 m.ava***.com，虚拟货币域名在浏览器中访问时其展示效果与在 MT 聊天软件的展示效果相同，意味着诈骗团伙先使用 mt.50****.com 搭建了聊天软件，然后将 m.ava***.com 诈骗平台对接到 MT 聊天软件的发现板块中。

通过分析 mt.50****.com 不同子域名的情况看，其子域名分别代表不同名称的通讯软件，如嗨呀即时通讯、信通即时通讯等。这些聊天软件，内嵌关联网站的首页路径均为/im/index.html，登录页路径均为/web/im/login.html，其中的 JS 文件，“暴露”了其背后的技术提供方“***易”IM。根据“***易”IM 的产品介绍，接入其 SDK 后，即刻拥有私聊、群聊、聊天室等通讯能力。诈骗团伙为了躲避监管和识别，将诈骗平台对接到了使用“***易”IM 的 SDK 制作的不同名字的聊天软件中。

2021 年 5 月，我们发现黑产又进行迭代升级，区别于以往利用子域名生成不同聊天软件的手法，此次域名调整为 API 形式，而非子域名形式，由于缺少参数，直接访问会显示“请求方式错误”，杜绝了逆向分析的可能。

通过对 APP 网络请求频繁出现的网址分析，推测诈骗团伙使用第三方 IM-SDK、境外服务器制作了 App server，当用户在应用登录时，首先与 APP 的服务器产生数据校验，再与第三方 IM-SDK 服务器产生数据校验。这里的 APP server 应用服务器，是诈骗团伙运部署运行业务代码的服务器，用来对接第三方 IM 服务，从 APP server 可以看出，诈骗团伙已逐渐增加对 APP 的开发的投入。

三、 境外电话、短信成黑产热门引流渠道

依托 360 安全大脑海量的网络安全威胁情报、360 手机卫士的用户举报数据，我们发现 2021 年上半年高发的诈骗案件中，境外电话、境外短信已成为诈骗团伙重要的引流工具。本报告将从实战角度出发，阐释境外电话、境外短信背后的原理。

1. 境外电话呼出渠道

在对诈骗案件分析的过程中，我们发现诈骗案件中的受害人，其接到的境外诈骗电话，存在多归属地的特点，即同一个诈骗团伙会使用不同国家的电话号码，向同一个受害人拨打电话，说明同一个窝点的诈骗团伙手里掌控大量不同国家的手机号码，在号码归属地国家搭建呼叫系统或使用号码漫游的方式控制此些号码。

这里就产生了一个问题，同一个诈骗窝点，是如何掌握不同国家的号码呢？这里以安卓端 W 应用为例进行原理解读。W 应用是一款网络电话 APP，使用手机号+短信/语音验证或邮箱账号完成注册后，如下图展示，即可按照国家、省份/州、区号等筛选条件，购买不同国家的电话号码，在服务有效期内，使用 W 软件拨打、接听电话。同时，由于 W 应用不安装手机卡也可以使用，注册成功后还赠送一部分话费，黑产从业人员在接码平台、一次性邮箱平台助力下，可批量注册免费境外号码和购买收费号码，拥有了海量的境外号码资源，在云控平台的支撑下，甚至可以实现批量外呼。

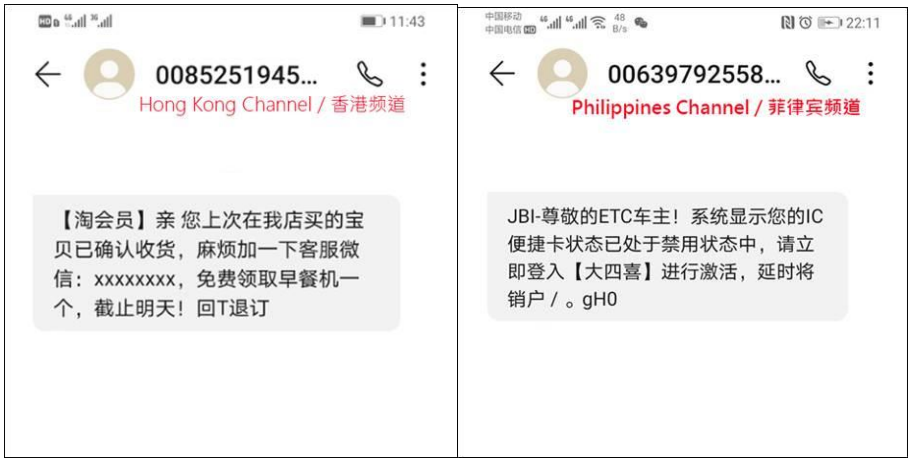
2. 境外短信群发平台

2021 年上半年高发的杀猪盘、虚假兼职、身份冒充等诈骗场景中，均出现国际通道短信的身影，在对产业挖掘的过程中，发现部分国际短信通道是由境内黑产人员搭建，通过境外通联 APP 售卖给从事博彩、虚假兼职、杀猪盘等诈骗团伙。

2.1 短信通道分类及推广渠道

根据短信通道的发送方种类，其包含国内通道和国际通道两种。国内通道指的是使用境内手机号、渠道号向境内手机发送短信；国际短信通道指的是能发送全球直达的短信，例如使用 852（中国香港）、856（老挝）、639（菲律宾）等号码发送短信。

目前在境内、境外社交软件群，均可发现国际短信推广的踪迹，其中境外社交软件群相较于其他渠道推广态度更加明确，推广客在推广过程中，大多都直接表明可为直播（ZB）、网贷(WD)、股票(GP)、博彩(BC)、网赚(WZ)等内容提供短信服务，为提高短信到达率，降低欺诈短信被拦截几率，还可提供短信内容模板。鉴于运营商、手机厂商、网络安全厂商各家拦截策略不同，不同类型诈骗短信，黑产会使用不同的短信渠道商、不同的国际渠道进行短信传播。例如虚假兼职使用中国香港短信通道、冒充 ETC 欺诈使用菲律宾短信通道。



2.2 短信发送方式

短信通道商提供短信管理后台和 API 接口 2 种短信发送方式，此些短信管理后台，其界面和功能大同小异，主要包含短信批量发送和模板设定功能。这里以某国际短信通道管理后台为例，使用短信通道商提供的账号登录短信通道平台后，在模板设定功能，填写需要发送的短信内容，批量上传短信接收方号码，单次上限 10000 个号码，选择菲律宾、土耳其等短信频道，即可使用此些国际号码发送指定短信内容给指定的收件人。

为提高短信的到达率，黑产人员除在短信内容上，使用黑话、简繁体字做拦截攻防外，还针对接收短信的号码进行了地址过滤，主动屏蔽例如北京、云南、内蒙古、重庆、新疆、江苏、山东等骚扰短信治理比较好的地方。

API 接口指的是使用国际短信通道提供的 api 接口、key 进行批量短信，例如某国际通道短信 API 接口格式为：https://api.g*****.com/send+ access_key+ mobile+ content+ callback_url，替换其中的内容即可批量发送短信。

第三章　热门黑产项目

一、 电商平台抢货的“正确姿势”

对于电商平台来讲，网络之上的购物盛宴有多狂欢，隐匿网络之下的黑色产业链就有多疯狂。研究中发现，黑产为了攻击电商平台，会购买大量电商平台账号，此些电商平台的账户与手机号进行了绑定，但由于黑产多通过接码平台进行注册，无法获得手机号的实际控制权，接码平台关闭后，便无法获得手机短信验证码，影响账号的正常使用。为解决这个问题，黑产账户卖家将电商平台的账号、密码、CK 一起出售，CK 是 Cookie 的简称，某些网站/应用为了辨别用户身份而储存在用户本地终端上的数据，这样下次再登录该平台就无需再次登录。由于 CK 账户免登录校验的优势，其已成为攻击电商平台的主要手段。

1. CK 账号分类

根据账号不同的登录方式，账号+密码登录、验证码登录、扫码登录；登录账号的客户端不同，M 端（手机网页）、APP 端、PC 端，产生的登录数据不同，Cookie 时效性不同，提取方式也不相同，因此即使是同一个电商平台的账号，其也存在多种不同的黑产账号，M 端-CK、PC 端-CK、APP 端-CK、直登账号、不能直登 CK 账号。下图为黑产渠道售卖的 CK 账号说明。

2. CK 账号提取方式

由于风控机制的存在，目前 Ck 账号分为手动版和自动化提取两种方式，手动版指的是在电商平台的 M 端（手机网页版）进行手动提取，登录电商平台后，通过浏览器抓包、解包获得

cookie 信息；自动版指的是利用 CK 提取软件，在 CK 提取软件中登录电商平台，由该提取软件自动提取 cookie 信息。为了满足黑产日益增长的 CK 账号需求，还存在浏览器插件提取 CK、脚本提取、APP 抓包等手段。

3. CK 账号的应用场景

黑产在掌握大量的 CK 账号后，即可以使用此些 CK 账号免登录校验的优势批量完成电商平台的任务，领取奖励。例如某电商平台的助力好友活动，黑产人员在购买大量的 CK 账号后，使用脚本软件导入大量 CK 账号批量完成任务，薅取平台的任务奖励。

CK 账号产业，本质是利用 CK 提取软件提取大量的 CK 账号，结合打码平台，云控等黑产手段躲过电商平台风控，获得电商平台的优惠券，再将优惠券进行贩卖牟利。在平台日益加强风控的趋势下，对于电商平台的普通用户而已，将自己的 CK 账号出售给他人，极易导致账号被风控，影响账号的正常使用；同时黑产间黑吃黑的现象仍很普及，CK 工具存在后门风险，一旦使用 CK 工具导致 CK 账号被盗，还存在资金被盗的风险。

二、 黑产低成本攻击方案

1. 钓鱼 WiFi

2021 年上半年，发现某视频平台出现钓鱼 WiFi 教程，不仅教程详细，作者更是将此钓鱼软件进行了开源操作，相较于传统借助 linux 破解 WiFi 手段，门槛更低，而更让人惊讶的是视频评论区，有不少用户分享着自己的破解心得。

钓鱼 WIFI 的原理是伪造信息，让路由器与连接 WIFI 的手机客户端以为双方需要断开连接，仿冒原路由器与客户端进行连接，从而盗取 WiFi 连接密码。

市面上提供的钓鱼 wifi 模块,主要是将钓鱼 wifi 固件，写入到单片机中，然后仿冒需要“偷取”的 wifi，诱导连接过该 WIFI 的手机主动连接，当该手机连接时，利用钓鱼网址页面，以“路由器固件升级，请输入 wifi 密码来确认升级，否则无法上网！”为由，诱导机主填写 wifi 登录密码，从而获得 wifi 登录密码。

钓鱼 wifi 固件的开源化，硬件成本的低廉化，导致钓鱼 wifi 门槛极低，在一些电商平台，甚至 10 元左右即可买到钓鱼 wifi 硬件。wifi 本质是连接设备与互联网的桥梁，通过桥梁的汽车，桥梁是可感知的，因此，在 WiFi 已成为用户生活中不可或缺的一部分的时代，WiFi 安全问题值得我们正视。

2. 短信轰炸

明明啥也没干，手机却无故收到大量骚扰短信，细看短信内容都是注册各平台接收的验证码，不少人可能都遇到过这种情况。在软件中输入手机号码，就可使对方手机不间断地接收短信，这便是黑产攻击工具“短信轰炸机”的威力。

在日常生活中，可能会遇到使用手机号+短信验证码登录 APP 的场景，输入手机号，选择短信验证码登录，手机便收到了登录使用的验证码。此手机号如果同一时间，在 100 个平台，选择手机号+短信验证码进行登录，该手机号短时间内便收到此 100 个平台发送的登录短信验证码，短信轰炸便是模拟该手机号短时间在大量的平台进行短信验证操作，实现该手机号短期收到大量的验证码的效果。

短信轰炸的本质是短时间内向同一个手机号发送大量的短信，阻碍机主正常使用手机，因此如何掌握大量的短信发送平台成为了关键。目前短信轰炸类应用，主要是批量“抓取”短信发送平台的接口，例如用于 APP 登录校验使用的短信验证码接口，将大量的接口通过脚本的方式集合在一起，生成一个短信轰炸脚本，当输入一个手机号后，该脚本自动模拟该手机号，在已爬取的接口平台批量进行短信验证操作。

短信接口被盗用于短信轰炸，一方面大量无辜用户收到短信骚扰；一方面短信通道不断发短信，造成短信资费浪费；若遭受用户投诉短信骚扰，短信通道可能被关停，导致正常业务短信无法下发，影响正常业务。在此建议，使用短信进行身份校验的平台方，通过同 IP、同 IP、图文验证等方式加强验证码风控策略，降低影响。

三、 低价包年视频会员账号

在对黑产链条分析的过程中，我们发现了大量出售影视会员卡密的源头发卡平台。发卡平台也称 24 小时自动发货平台或卡盟，提供一站式售卖虚拟商品，用户在平台下单，平台自动给用户发货（软件激活密钥），售卖的商品多以低价账号、黑产应用为主，如应用多开、爆粉人脉、通联 APP 辅助、虚拟定位、微商辅助、支付账号代点亮、营业执照代办等。下图为某发卡平台售卖的商品。

1. 发卡平台运作模式

发卡平台本质是一个对接上游黑灰产资源方、下游资源需求方，类似一个小型暗网平台的黑市，上游黑产团伙通过接码平台、群控、养号等方式掌握了大量的平台账号，在发卡平台，将账号卖给羊毛党、诈骗团伙，进行资金变现。发卡平台为了更快的进行资源变现，普遍具备分站代理功能，在此网站注册、付费成为代理后，可以获得对应的分站二级域名，他人通过此分站域名进入网站后进行的下单操作，分站站长可获得对应商品的佣金提成。

2. 分站运营方式

分站代理本质是发卡平台的代理商，因此无法掌控其售卖的商品资源，能做的仅是对已有的商品进行价格调整，做到“中间商赚差价”。分站代理后台主要包含“商品上架”、“商品发货”、“商品收款、提现”三个板块。商品上架主要是填写商品类型、名称、介绍、价格、发卡模式（自动发货、手动发货、邮寄发货）、上传商品图片完成商品上架；商品发货指的是在对应商品填写商品卡密，当用户下单后，自动给下单人员发送对应的商品卡密；商品收款、提现指的是将在第三方支付通道注册后，获得的商户 ID 和商户密钥与分站平台进行绑定， 实现当用户付款后，可在第三方支付通道进行提现。

目前，发卡平台已经成为了黑灰产资源供应中的重要一环，在整体黑灰产业链，承担中坚力量。也正是由于发卡平台的泛滥，间接造就了黑灰产资源、羊毛党、诈骗团伙的泛滥，其贩卖的商品，多具备“高嚎头”，“有效周期短”的黑产属性，用户在发卡平台购买的商品，往往有效期还没有结束，已经无法使用。同时，发卡平台提供给分站代理使用的多是些不正规的第

三方支付通道，分站站长存在间接被洗钱团伙利用的情况。

第四章　热门诈骗剧本

一、 开了个屏幕共享，钱没了

随着反诈骗知识的普及，全民反诈骗意识逐渐提升，不会轻易访问别人发送的钓鱼网站，更不会轻易向对方提供银行短信验证码。但被动式信息泄露的数据，出现了上升。2021 年上半年 360 手机卫士接到用户关于诈骗的举报案例中，有一个词频繁出现 “分享屏幕”，受害人曾都被骗子要求开启分享屏幕功能。

今年 5 月，用户反馈其收到商家电话，表示其购买的商品质量问题，为避免消费者投诉，愿意主动退款。在办理退款过程中，用户按照要求，进行了手机屏幕共享，随后发现自己的银行账户被盗刷。

通过分享屏幕功能，她的银行卡号、银行提现验证码、卡内余额等信息均被骗子尽收眼底，尽管她自己没有参与提现操作，可是钱还是被骗子转走。

专家解读

屏幕分享顾名思义就是将手机屏幕共享给他人，目前社交、会议等 APP 会具备此些功能，因此骗子会主动引导受害人安装此些 APP，以远程协议为名，查看受害人的手机界面，从而窥探受害人银行卡号、银行提现验证码等信息，进行资金盗刷。

安全课堂

屏幕分享功能开启后，他人可以看到手机上的内容，切勿向陌生人开启屏幕共享功能。即使开启屏幕功能，也切勿在分享过程中操作支付类、银行类产品，防止财产信息泄露。

二、 确认收货，加 V 免费送礼品

每逢电商大促，用户必收到大量促销短信，2021 年 4 月 360 手机卫士收到用户反馈，其因添加了陌生号码发来的短信中的微信，在领取所谓的“红包”过程中，被骗在博彩平台充值下注，被骗几千元。

2021 年 4 月，用户收到了 “确认收货，可以送早餐机”的短信，添加了短信内的微信账号，骗子确认用户是通过短信添加后，邀请用户进微信群领礼品。用户进群后，按照任务要求关注了公众号并回复截图，群主给用户发了红包佣金。随后，群主称该礼品赞助商的应用需要下载量和注册量，用户下载应用可再获得奖励金。用户下载该聊天应用后，在应用内添加了奖

励金结算员账号，在结算员的指引下，参与了新的佣金任务，即在该聊天软件内嵌的博彩平台进行充值投注。前几次按照对方提供的计划下注，对方进行了返金；后期多次下注上千元后，对方未返金而得知受骗。

专家解读

随着技术对抗的升级，诈骗团伙为降低自身资产的损失，会将受话人引导至专属的诈骗场景实施定向诈骗，本文中提及的虚假兼职，诈骗分子制作了内嵌博彩平台的通 APP，通过短信、微信多次引流跳转，最终将受话人落地至专属的 APP 中，既躲避了传统社交软件的围追堵截，也避免了钓鱼网址轻易被发现的风险。

安全提示

以“免费送”礼品为幌子，诱导添加微信的短信，切勿相信。特别是做任务，还需要安装存在风险行为的应用，更要提高警惕。

三、 再爱，也不要网络招嫖

上半年中，360 手机卫士有收到用户反馈，其在网络招嫖过程中被骗 5000 元。通过对诈骗手法的分析，其主要通过引流、切客、诱导支付三个环节实施诈骗。

首先在色情网站发布会所、服务项目等信息。通过 QQ、微信等聊天软件与用户初步沟通后，引导用户安装具体端对端加密的聊天 APP，在加密聊天 APP 中，向用户讲解“上门服务内容”，为方便用户的需求，给用户发送含“技师”信息的 APP 平台，供用户选择。当用户选择好“技师”后，以先付款再派技师出发、首次用户需预交套餐服务费、 转账时未备注“小姐”编号需再次转账等理由诱导用户转账，转账后，对方最终与用户断联。

专家解读

移动互联网的普及使用，个人信息蕴含了巨大的经济价值，促使黑灰产的滋生，个人信息成为黑灰产“抢夺”的目标。在对部分会所类 APP 分析时发现，部分 APP 暗地里窃取用户地理位置、通讯信息，窃取相册文件、有针对性地静默录像。即当受害人安装并使用招嫖团伙提供的上门服务 APP 后，其手机信息存在泄露的风险。

安全提示

任何诈骗最初都是具有强烈的迷惑性，应洁身自好，提供警惕，否则一不小心，就会掉进骗子的陷进。

四、 赌球下注总输钱？

欧洲杯正在如火如荼的进行中，而一些钓鱼网站大多通过短信、社交群、不良网站等形式传播扩散，引导用户到赌球网站/APP、或进群参赌。“提供每场比赛精准盘口，支持转账日结。”不少群里会放出每天比赛的盘口，用户可以根据需求来下单，球赛一结束，就可以马上结算。如此“便捷”的方式吸引了很多好赌人士。一些赌球 APP 通过鼓励消费者注册充值、竞猜比赛“胜平负”等方式开奖获利外，有的 APP 还以“公司入款单笔 10000 元以上赠 2.5%存款额”的方式来吸引用户进行大数额充值，但博彩平台具备控制利率、开奖结果，禁止用户登录等功能，用户最终只有全输的结局。

专家解读

从博彩诈骗的手法演变上看，博彩平台逐渐减少对 QQ、微信等社交平台的依赖，呈现出利用小众聊天软件作为渠道进行诈骗的趋势，试图降低账号被封风险。同时不断增加对平台攻防的成本投入，不断更换服务器与域名解析，躲避安全厂商识别。

安全课堂

“赢的还想赢，输的想翻盘”。网络赌球不管输赢，最后的赢家永远是游戏的掌局者。用户应该通过正规渠道购彩，通过合理下注，获得竞彩的乐趣。

第五章　2021 年上半年度安全数据

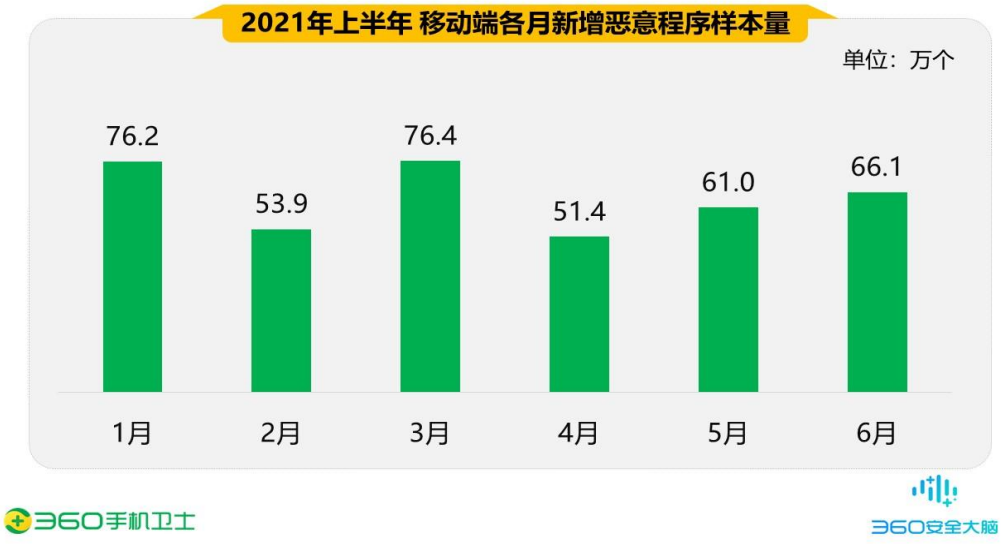
飞速发展的网络通信时代，互联网以及智能手机的普及给民众的生活和获取资讯带来了极大的便利，同时不法分子不断“更新迭代”的技术手段也带来了一定程度的安全风险，对人们的日常生活产生恶劣影响的同时，更造成了个人财产的损失和隐私泄露。

面对当前复杂而严峻的网络安全形势，针对不法分子恶意利用技术，360 安全大脑一直在持续履行作为安全厂商的职责。基于自身已有的海量数据进行实时研判，采用人工智能、多维模型等方式，提升移动互联网恶意程序的识别收录能力，预设钓鱼网站识别规则，提升实时研判垃圾短信新增与变种的能力，建立更为精准的号码识别拦截规则，持续抵制互联网不法信息传播，维护用户移动信息安全。

一、 恶意程序

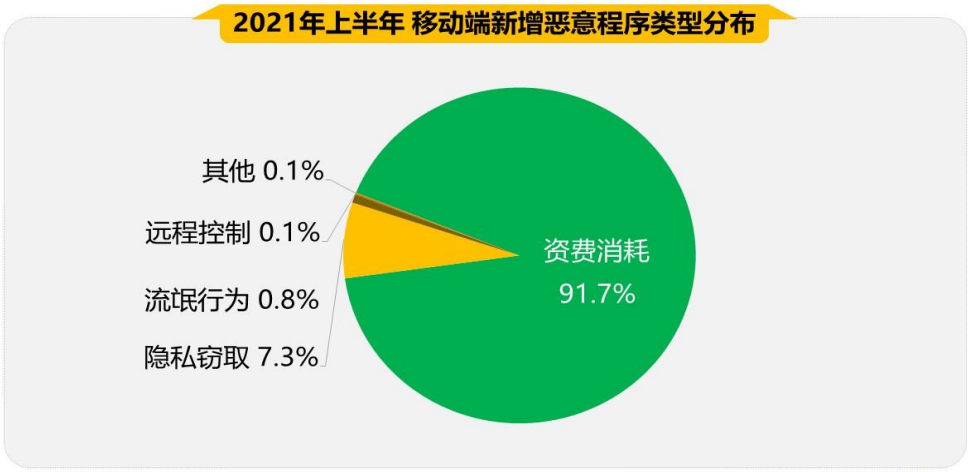
1. 恶意程序新增样本量与类型分布

2021 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 385.0 万个，同比 2020 年上半年度（104.8 万个）上升了 267.2%，平均每天截获新增手机恶意程序样本约 2.1 万个。下图为 2021 年上半年度移动端各月新增恶意程序样本量统计：



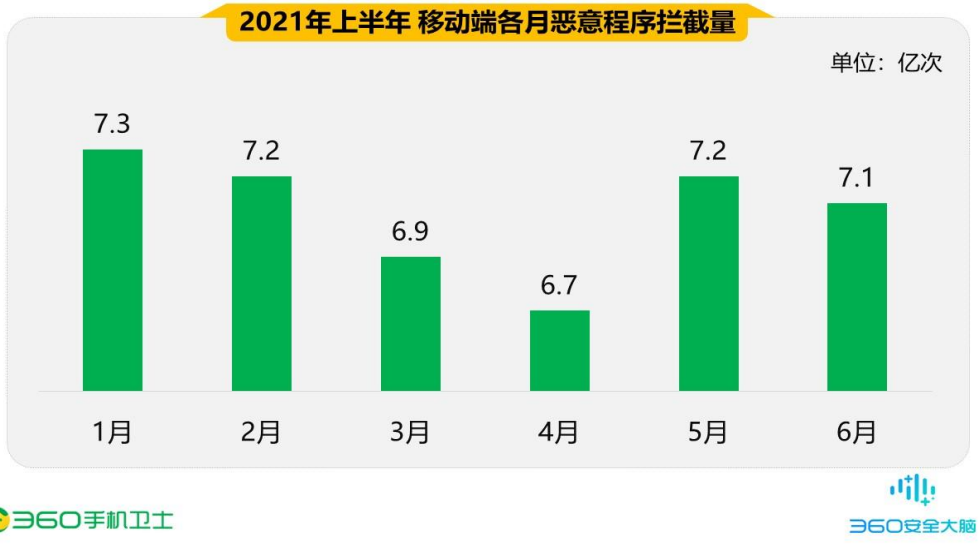
2021 年上半年度，移动端新增恶意程序类型主要为资费消耗，占比 91.7%；其次为隐私窃取（7.3%）、流氓行为（0.8%）、远程控制（0.1%）等。下图为 2021 年上半年度移动端新增恶

意程序类型分布：



2. 恶意程序拦截量

2021 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 42.3 亿次，平均每天拦截手机恶意程序攻击约 2338.6 万次。下图为 2021 年上半年度移动端各月恶意程序拦截量统计：

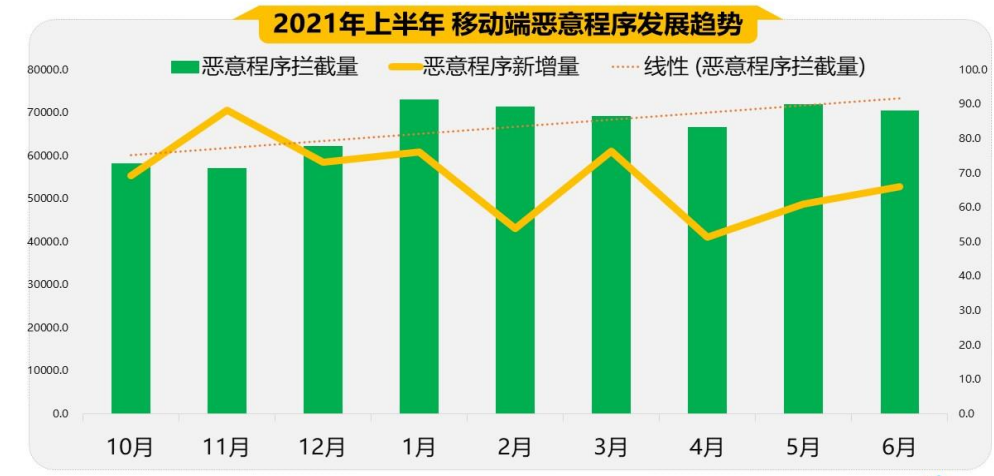


3. 恶意程序发展趋势分析

2021 年上半年，恶意程序新增量在 2021 年 3 月出现激增峰值，当月恶意程序新增量为

76.4 万，之后 4 月又重新恢复日常情况，稳步上涨。观察新增样本类型，主要体现在资费消耗类型。

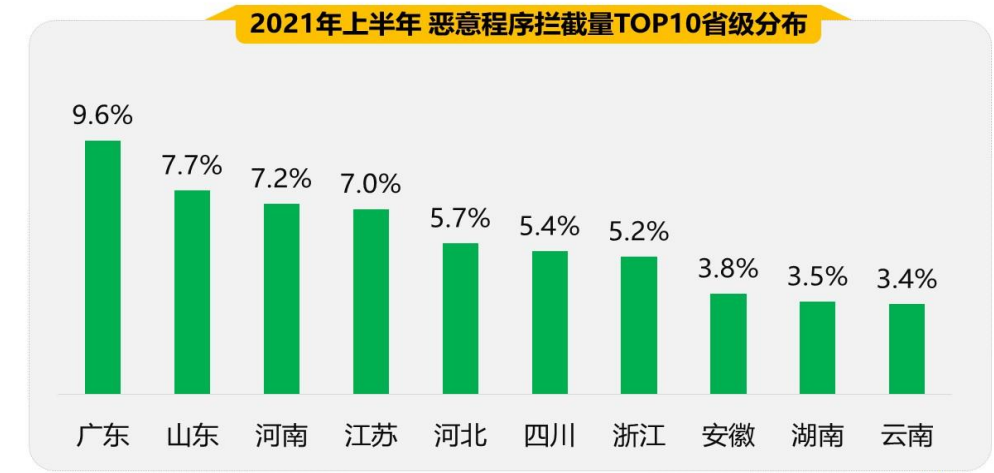
反观恶意程序拦截量趋势，较去年有明显增长，360 对恶意程序的拦截能力也在不断提升。广泛应用的线上场景，如网络授课、视频会议、远程办公等让大众对于移动网络的日常使用愈加频繁，360 对此不断提升拦截能力，以便尽可能多地减小用户隐私泄露或者财产损失的风险。



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

2021 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 9.6%；其次为山东（7.7%）、河南（7.2%）、江苏（7.0%）、河北（5.7%），此外四川、浙江、安徽、湖南、云南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上海市，占全国拦截量的 2.3%；其次为北京（2.2%）、广州（2.1%）、重庆（2.0%）、成都（1.9%），此外深圳、西安、天津、郑州、苏州的恶意程序拦截量也排在前列。

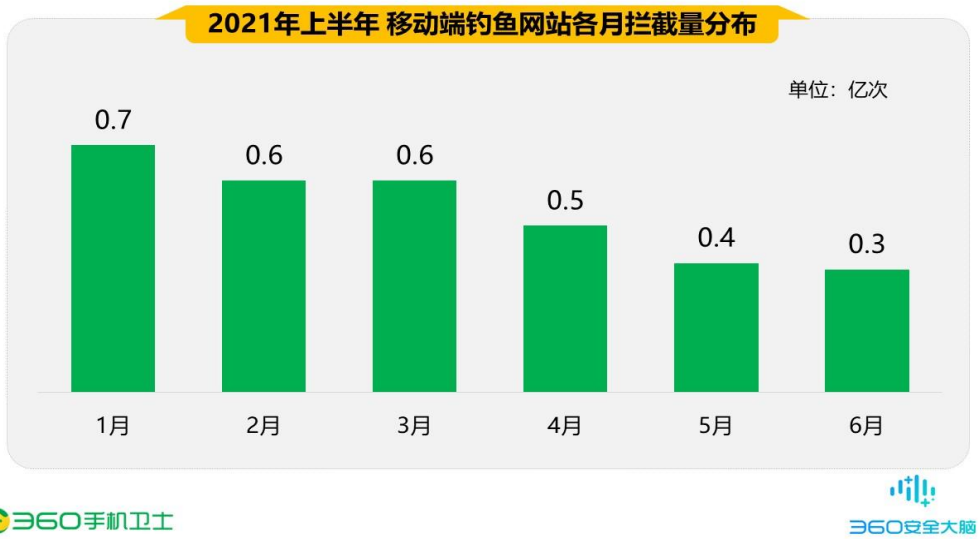
二、 钓鱼网站

1. 移动端钓鱼网站拦截占比

2021 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 581.3 亿次，同比 2020 年上半年度（435.8 亿次）上升了 33.4%。其中，PC 端拦截量约为 578.2 亿次，占总拦截量的 99.5%，平均每日拦截量约 3.2 亿次；移动端拦截量约为 3.2 亿次，占总拦截量的 0.5%，平均每日拦截量约 175.5 万次。下图为 2021 年上半年度钓鱼网站拦截占比分布：

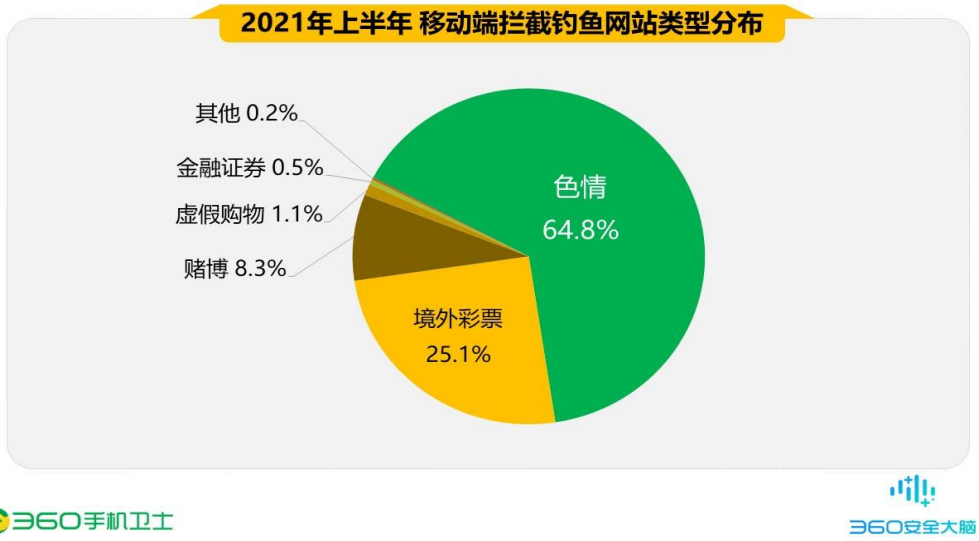
2. 移动端钓鱼网站各月拦截量分布

2021 年上半年度，360 安全大脑在移动端拦截钓鱼网站攻击约为 3.2 亿次，同比 2020 年上半年度（6.7 亿次）下降 52.8%。下图为 2021 年上半年度钓鱼网站各月拦截量分布：



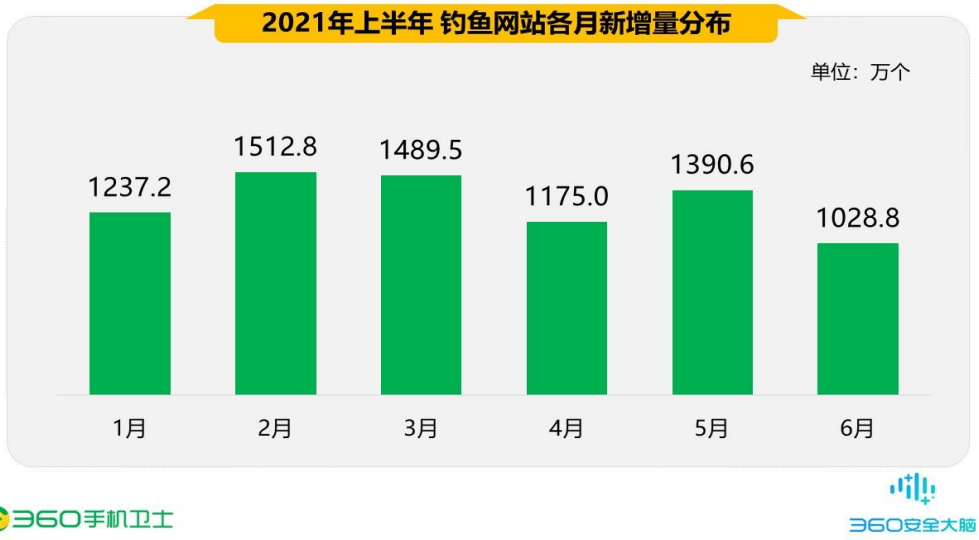
3. 移动端钓鱼网站类型分布

2021 年上半年度，移动端拦截钓鱼网站类型主要为色情，占比高达 64.8%；其次为境外彩票（25.1%）、赌博（8.3%）、虚假购物（1.1%）、金融证券（0.5%）等。下图为 2021 年上半年度移动端拦截钓鱼网站类型分布：

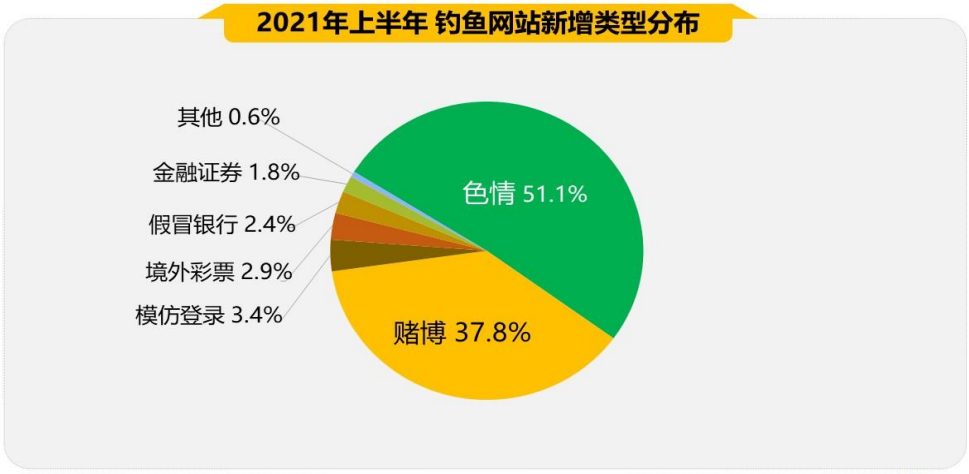


4. 移动端钓鱼网站新增量

2021 年上半年度，360 安全大脑共截获各类新增钓鱼网站 7833.9 万个，同比 2020 年上半年度（2416.3 万个）上升了 224.2%，平均每天新增 43.3 万个。

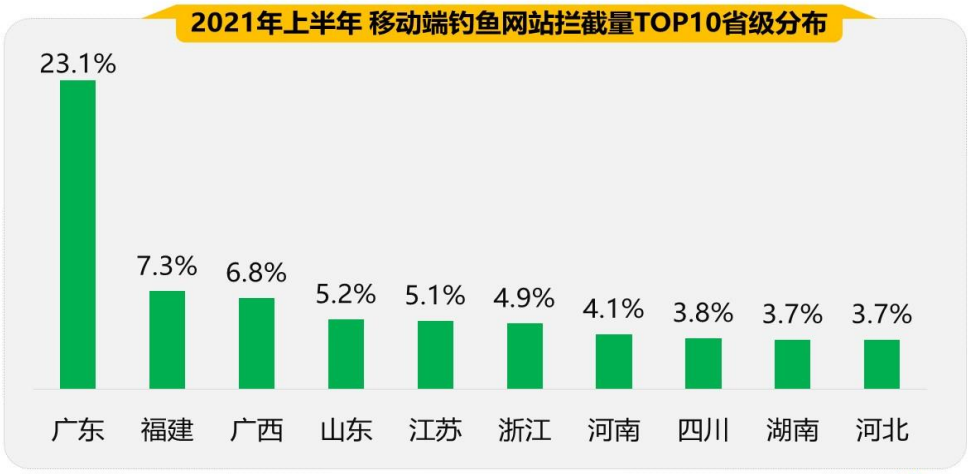


在钓鱼网站新增类型中，色情类占据首位，占比 51.1%；其次为赌博类（37.8%）、模仿登录（3.4%）、境外彩票（2.9%）、假冒银行（2.4%）、金融证券（1.8%）等。在过去的半年中，360 安全大脑持续对钓鱼网站的类型进行细分，提升样本检测量与样本拦截能力，及时识别各类黑灰产网站，尽可能全面地保证用户的信息安全与财产安全。下图为 2021 年上半年度移动端新增钓鱼网站类型分布：

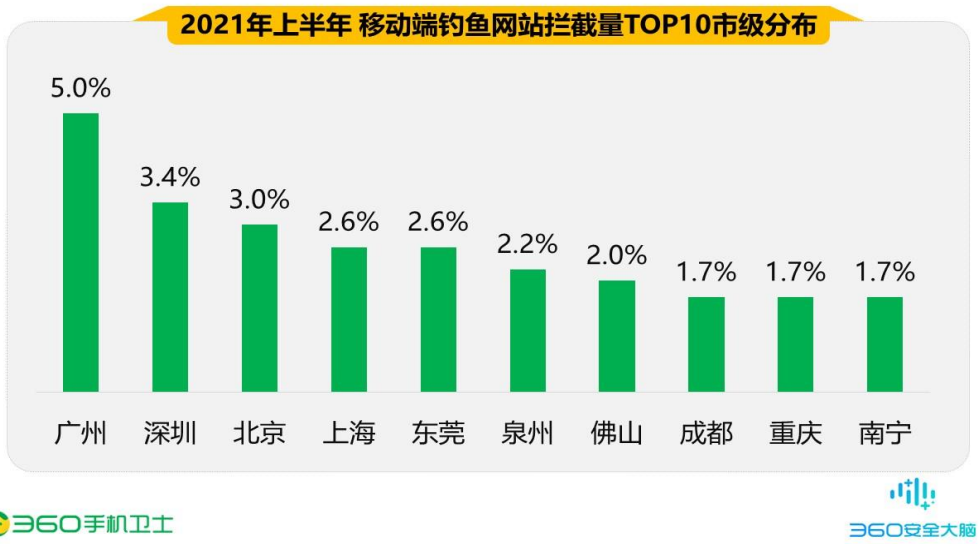


5. 移动端钓鱼网站拦截量地域分布

2021 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 23.1%；其次为福建（7.3%）、广西（6.8%）、山东（5.2%）、江苏（5.1%），此外浙江、河南、四川、湖南、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 5.0%；其次为深圳（3.4%）、北京（3.0%）、上海（2.6%）、东莞（2.6%），此外泉州、佛山、成都、重庆、南宁的钓鱼网站拦截量也排在前列。



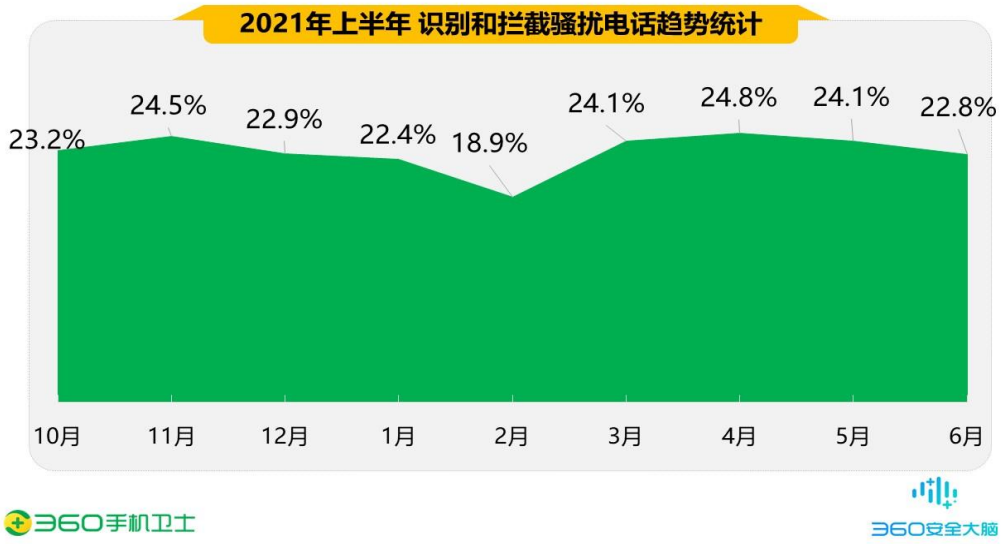
三、 骚扰电话

1. 骚扰电话标记拦截量

2021 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 111.0 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。同比 2020 年上半年度（112.3 亿次）下降了 1.1%。下图为 2021 年上半年度骚扰电话各月拦截号码次数分布：

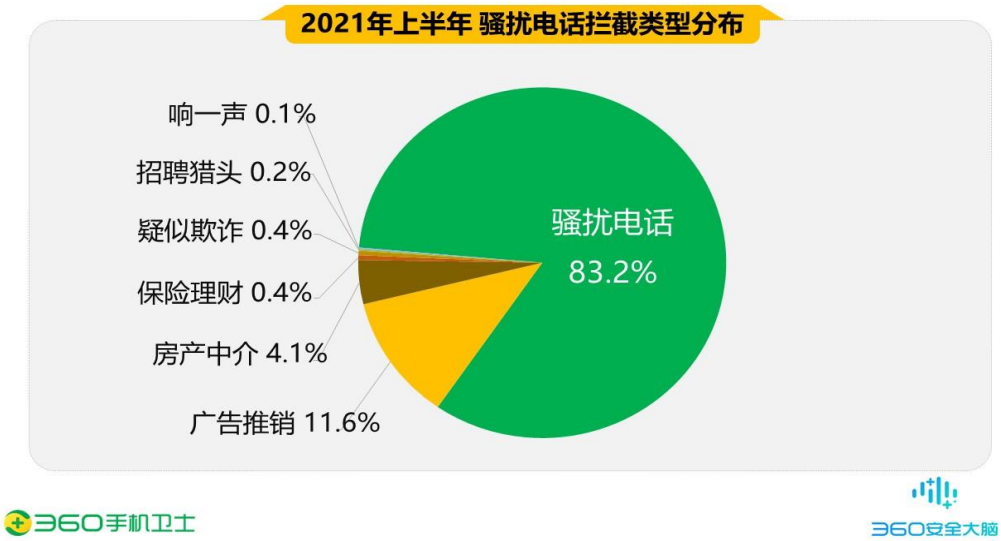
根据各月骚扰电话呼入占比分析，2021 年 2 月份期间正值春节假期，骚扰电话拦截量最低。通过往年趋势可知，春节期间从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入

量降低。2021 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 2021 年上半年度识别与拦截骚扰电话趋势统计：



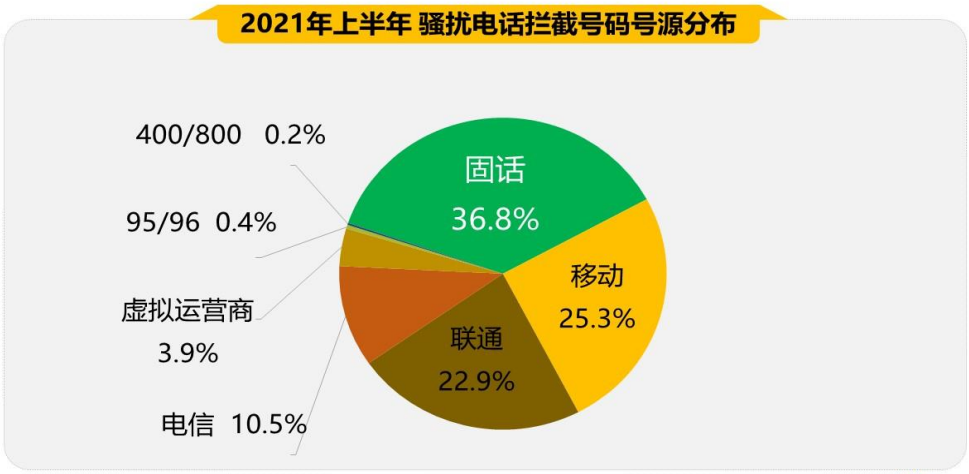
2. 骚扰电话拦截类型分布

2021 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 83.2%的比例位高居首位；其次为广告推销（11.6%）、房产中介（4.1%）、保险理财（0.4%）、疑似欺诈（0.4%）、招聘猎头（0.2%）与响一声（0.1%）。下图为 2021 年上半年度骚扰电话拦截类型分布：

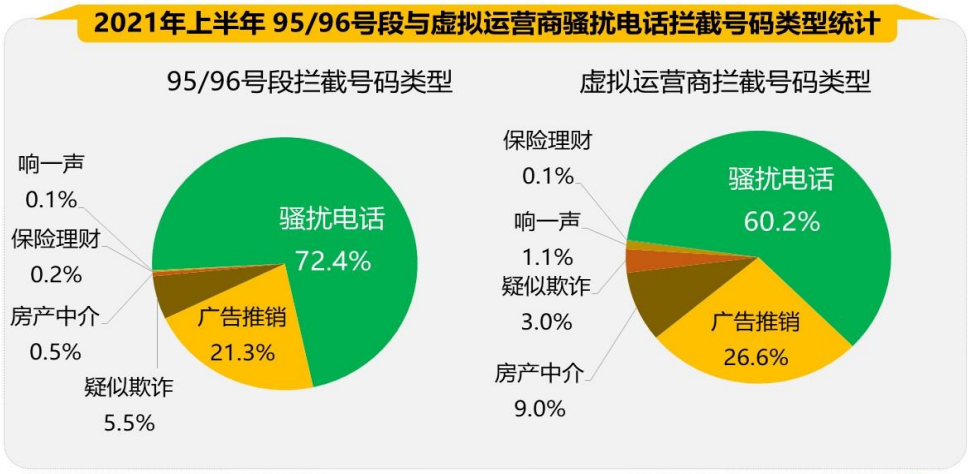


3. 骚扰电话拦截号码号源分布

2021 年上半年度，从骚扰电话拦截号码个数分布来看，被拦截号码为固话的占比最多，高达 36.8%，其次为运营商为中国移动的个人手机号（25.3%）、运营商为中国联通的个人手机号（22.9%）、运营商为中国电信的个人手机号（10.5%）、虚拟运营商（3.9%）、95/96 开头号段（0.4%）与 400/800 开头号段（0.2%）。下图为 2021 年上半年度骚扰电话拦截号码号源分布：

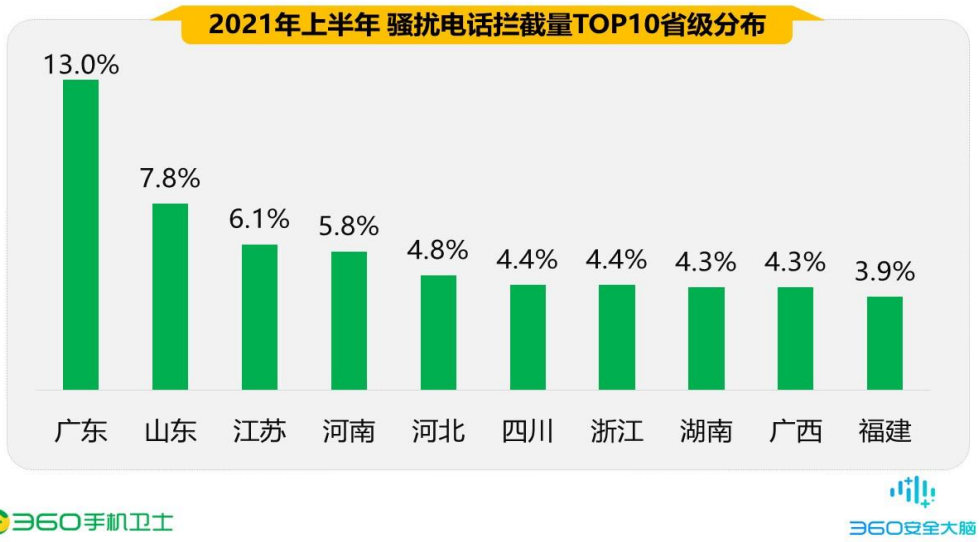


观察 95/96 号段与虚拟运营商骚扰电话拦截号码类型，95/96 号段骚扰电话类占据首位，占比 72.4%；虚拟运营商骚扰电话类占据首位，占比 60.2%；广告推销类分别占比 21.3%与 26.6%，类型比例占据前列。95/96 号段与虚拟运营商号码依然是不法分子从事非法行径的主要“工具”之一。

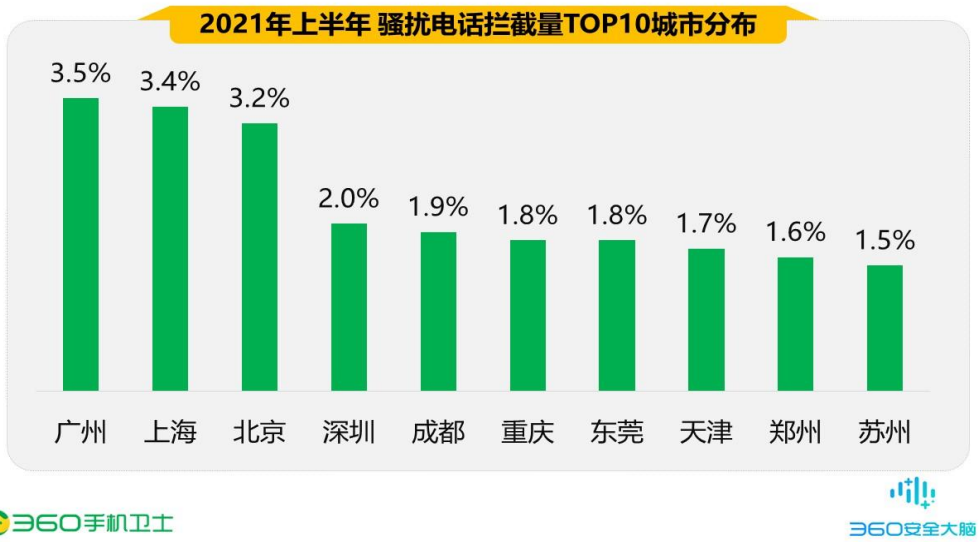


4. 骚扰电话归属地分布

2021 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 13.0%；其次是山东（7.8%）、江苏（6.1%）、河南（5.8%）、河北（4.8%），此外四川、浙江、湖南、广西、福建的骚扰电话拦截量也排在前列。



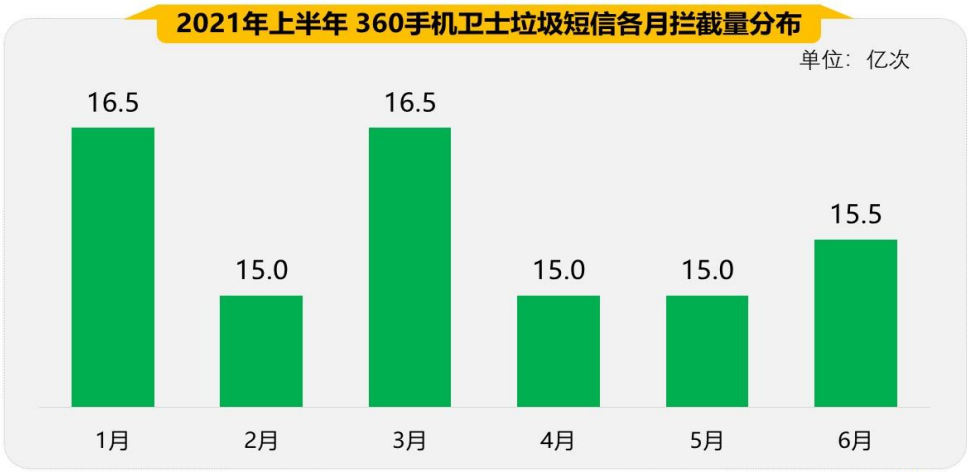
从城市分布来看，广州市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 3.5%；其次是上海（3.4%）、北京（3.2%）、深圳（2.0%）、成都（1.9%），此外重庆、东莞、天津、郑州、苏州的骚扰电话拦截量也排在前列。



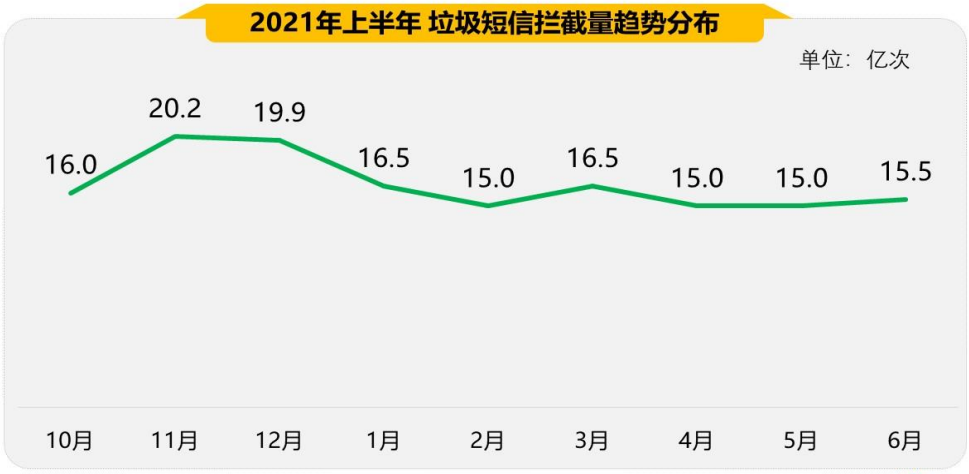
四、 垃圾短信

1. 垃圾短信拦截量

2021 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 93.4 亿条，同比 2020 年上半年度（74.9 亿条）上升了 24.7%，平均每日拦截垃圾短信约 5159.9 万条。下图为 2021 年上半年度 360 手机卫士垃圾短信各月拦截量分布：

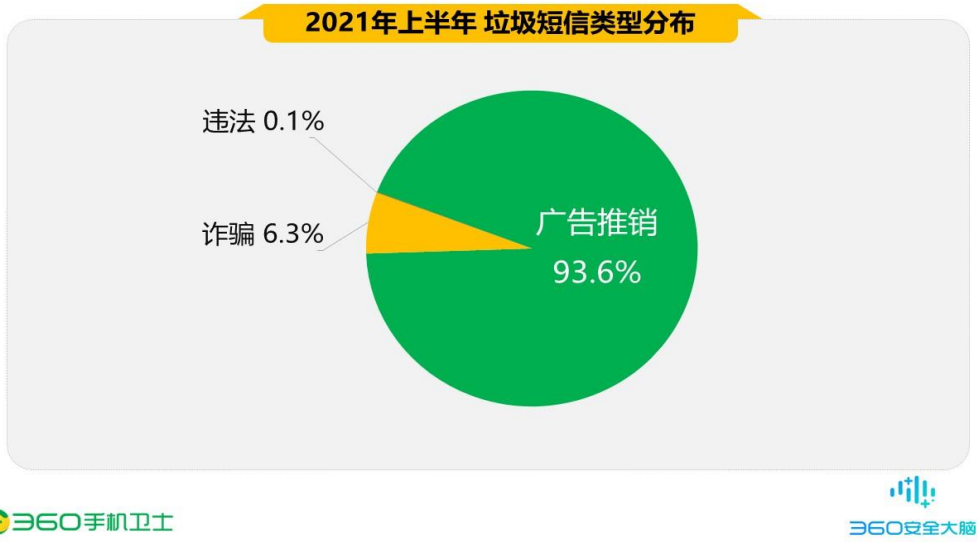


根据垃圾短信拦截量趋势分布，由于第一季度 2 月份春节期间各类发送垃圾短信的从业人员减少、企业放假休息，各类广告推销类型短信减少，导致 2 月份垃圾短信数量降低，但第二季度分月数据呈现逐渐走高趋势。下图为垃圾短信拦截量趋势分布：

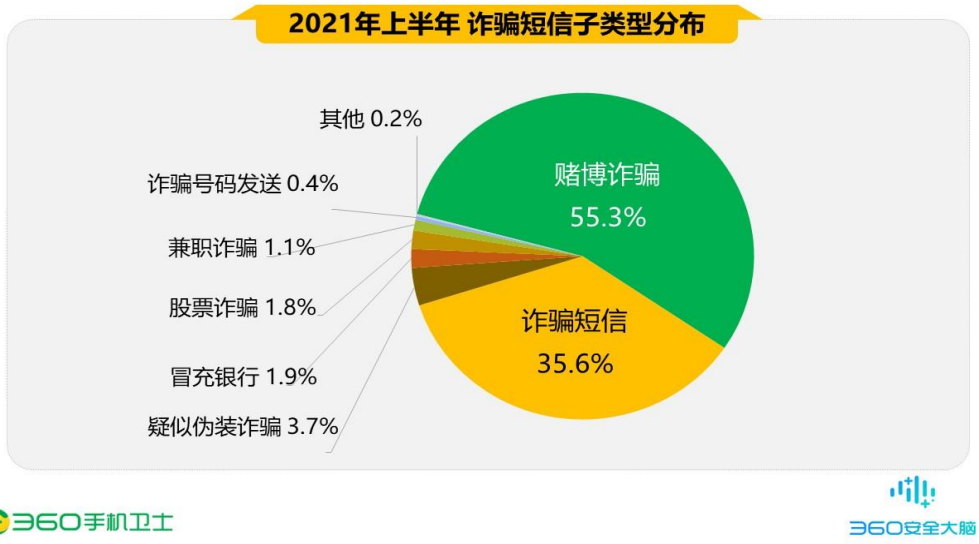


2. 垃圾短信类型分析

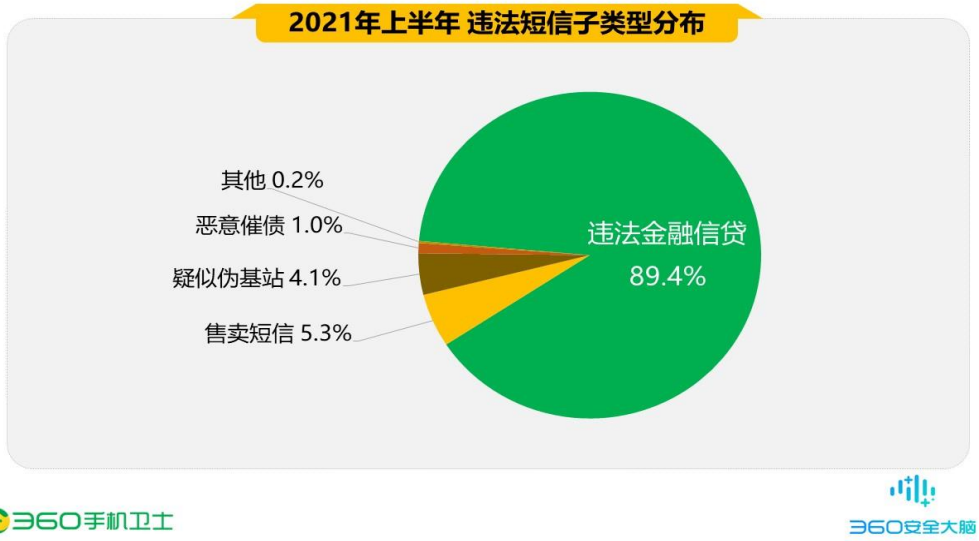
2021 年上半年度，垃圾短信的类型分布中广告推销短信最多，占比为 93.6%；诈骗短信占比 6.3%；违法短信占比 0.1%。



从诈骗短信拦截类型来看，赌博诈骗以 55.3%的比例位居首位；其次为诈骗短信（35.6%）、疑似伪装诈骗（3.7%）、冒充银行（1.9%）、股票诈骗（1.8%）、兼职诈骗（1.1%）、已识别诈骗号码所发送的诈骗短信（0.4%）等。下图为 2021 年上半年度诈骗短信子类型分布：

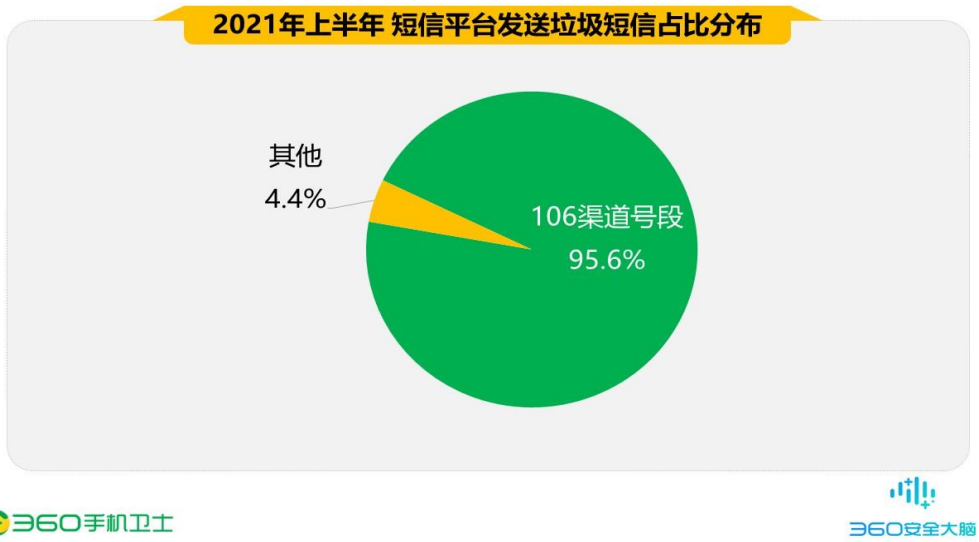


从违法短信拦截类型来看，违法金融信贷短信以 89.4%的比例位居首位；其次为售卖信息（5.3%）、疑似伪基站发送（4.1%）、恶意催债（1.0%）等。下图为 2021 年上半年度违法短信子类型分布：



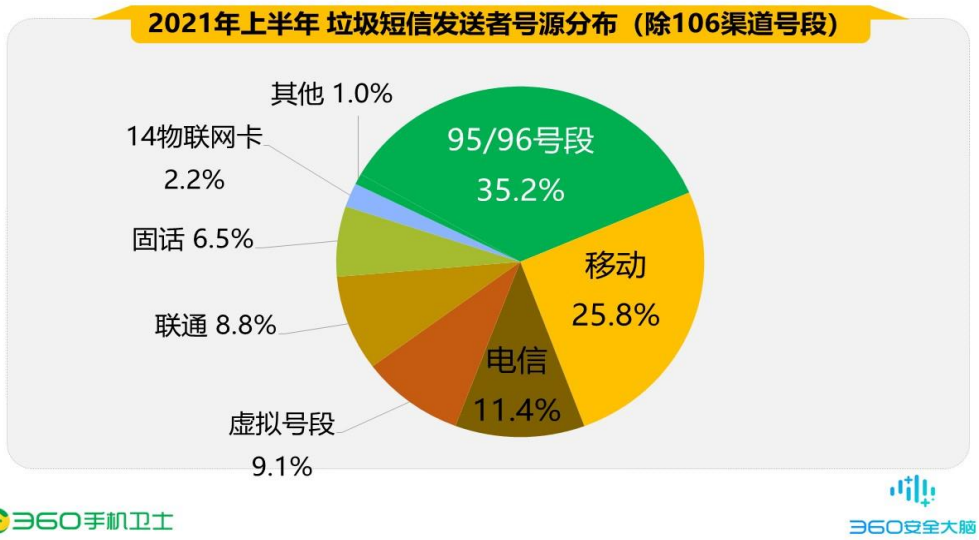
3. 垃圾短信发送者运营商号源分布

2021 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 95.6%；利用其他号段传播垃圾短信占比约 4.4%。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，发送成本低、传播范围广的特点被黑灰产业利用，一直是传播违法诈骗类短信的重要渠道，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 2021 年上半年度短信平台发送垃圾短信占比分布：



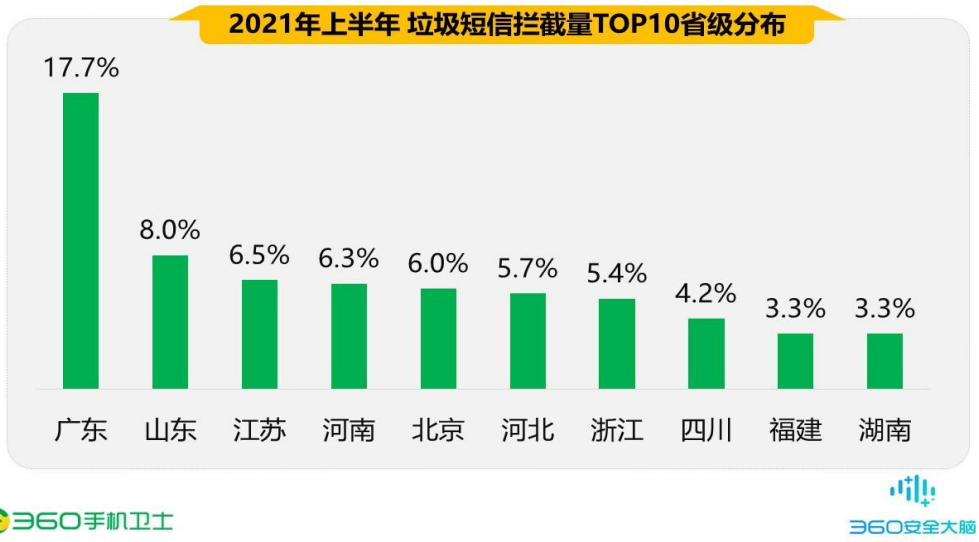
2021 年上半年度，除短信平台 106 开头号段发送垃圾短信外，从其他发送者号码个数分布看，利用 95/96 号段发送垃圾短信的最多，占比 35.2%；其次是运营商为中国移动的个人手

机号（25.8%）、运营商为中国电信的个人手机号（11.4%）、虚拟运营商号段（9.1%）、运营商为中国联通的个人手机号（8.8%）、固话（6.5%）与 14 物联网卡（2.2%）等。

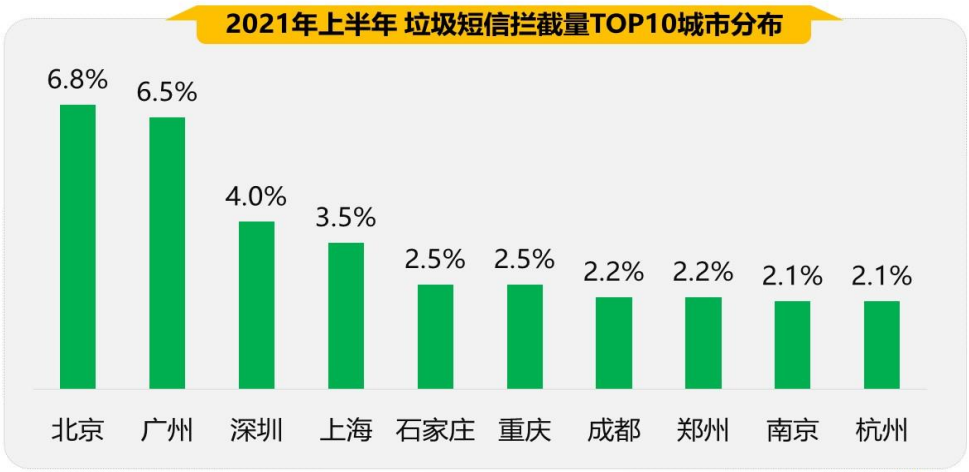


4. 垃圾短信拦截量地域分析

2021 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 17.7%；其次是山东（8.0%）、江苏（6.5%）、河南（6.3%）、北京（6.0%），此外河北、浙江、四川、福建、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 6.8%；其次是广州（6.5%）、深圳（4.0%）、上海（3.5%）、石家庄（2.5%），此外重庆、成都、郑州、南京、杭州的垃圾短信拦截量也排在前列。


2021年上半年 垃圾短信拦截量TOP10城市分布
6.8%
6.5%
4.0%
3.5%
2.5%
2.5%
2.2%
2.2%
2.1%
2.1%
北京
广州
深圳
上海
石家庄
重庆
成都
郑州
南京
杭州

第六章 2021 上半年度网络安全行业动态

一、 工业和信息化部扎实部署推进“断卡行动”

工业和信息化部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，坚持以人民为中心，聚焦当前行业治理难点和群众痛点，近期联合公安部发布了《关于依法清理整治涉诈电话卡、物联网卡以及关联互联网账号的通告》，指导电信企业建立高风险电话卡“二次实人认证”制度，集中对公安机关通报的涉案电话卡、高风险电话卡以及关联互联网账号进行了系统清理整治，着力切断电信网络诈骗通信渠道。自今年 5 月以来，首批依法关停公安机关通报的涉案电话卡 6055 张，处置涉案关联互联网账号 18552 个，组织对 1536.17 万张“睡眠卡”等高风险电话卡进行了二次实人认证和处置，有力打击了各类违规办卡、养卡屯号行为。从公安机关通报看，近期全国电信网络诈骗犯罪立案数据环比下降了 14.3%，案件持续高发的势头到了一定遏制。

下一步，工业和信息化部将进一步加大工作力度，下大力气为群众办实事，持续深化防范治理电信网络诈骗各项工作，全力推进“断卡”、“打猫（猫池、GoIP 设备）”、互联网反诈、短信预警等涉及群众利益的重点事项，推动形成“标本兼治、协同联动”长效机制，坚决维护好广大人民群众的合法利益与财产安全[1]。

二、 公安部组织开展新一轮集中收网行动 依法严厉打击涉电信网络诈骗 APP 技术开发违法犯罪团伙

5 月 11 日 14 时，在公安部统一指挥下，北京、辽宁、湖南、广东等 26 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 APP 技术开发支持的违法犯罪团伙。截至当日 18 时，共捣毁技术开发窝点 110 余个，抓获违法犯罪嫌疑人 440 余名。

当前，通过虚假 APP 实施的电信网络诈骗案件持续高发，已占所有电信网络诈骗案件的 60%以上。公安部对此高度重视，先后组织开展多次集中抓捕行动，依法严厉打击此类违法犯罪活动。同时，深入研判此类案件规律特点，深挖涉诈 APP 开发、封装、应用各个环节，全面分析为电信网络诈骗提供信息支持、技术支撑、转账洗钱等非法服务情况，梳理出一批涉诈 APP 技术开发人员违法犯罪线索，部署开展了新一轮集中收网行动，对涉诈 APP 违法犯罪活动形成强有力的震慑。

据了解，自去年 10 月全国“断卡”行动开展以来，公安机关成功打掉一大批非法开办贩

卖“两卡”违法犯罪团伙，缴获一大批用于电信网络诈骗活动的电话卡和银行卡。随着非法电话卡、银行卡不断减少，一些诈骗窝点出现“卡荒”，诈骗分子转变犯罪手法，大肆使用虚假 APP 实施诈骗。在非法利益驱使下，一些技术开发人员沦为诈骗团伙帮凶，“量身定制”具有各种诈骗功能的虚假 APP。他们从对接诈骗团伙需求、编写程序代码，到购买域名、租用服务器，再到 APP 封装和分发，形成了分工明确的专业化犯罪链条。其开发的虚假 APP 仿照一些知名正规应用平台进行包装，达到以假乱真的目的，极具迷惑性。诈骗团伙诱骗受害人点击链接或扫描二维码下载虚假 APP，通过 APP 的相应功能进行沟通联络、窃取信息、诱骗转账付款等操作，实施贷款诈骗、刷单诈骗、“杀猪盘”诈骗等各类诈骗活动，严重危害人民群众财产安全和合法权益。

公安部有关负责人表示，面对电信网络诈骗犯罪的新动向，公安机关将始终保持高压严打态势，加强分析研判、创新打法战法，坚持打团伙、捣窝点、断链条、摧灰产，坚决从源头上遏制电信网络诈骗犯罪多发高发态势，切实维护人民群众财产安全和合法权益。公安机关正告为电信网络诈骗等违法犯罪提供技术支撑、资金转移等各类非法服务的人员，认清形势悬崖勒马，主动投案自首，争取宽大处理。同时，公安机关提醒广大群众增强防范意识，对于未知来源的 APP 不下载、不点击、不扫码，防止被骗[2]。

三、 “两高一部”发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》

2021 年 6 月 22 日，最高人民法院、最高人民检察院、公安部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》（以下简称《意见二》）正式公布。

近些年来，电信网络诈骗犯罪活动持续高发多发，犯罪形势日趋严峻复杂。围绕电信网络诈骗犯罪，还产生了一系列黑灰产业链，形成大量上下游关联犯罪，成为电信网络诈骗犯罪不断发展蔓延的催化剂和助燃剂，严重侵害了人民群众的财产安全和其他合法权益，严重影响社会和谐稳定。以习近平同志为核心的党中央高度重视打击治理电信网络诈骗违法犯罪工作，习近平总书记多次作出重要指示批示，为打击治理工作指明了方向、提供了根本遵循。最高人民法院、最高人民检察院、公安部等部门坚决贯彻落实习近平总书记重要指示批示精神，在注重综合施策、源头治理的同时，坚持依法从严惩处的方针，坚决予以严厉打击。为此，中央部署深入开展打击治理电信网络新型违法犯罪专项行动，取得显著成效。2016 年 12 月，最高人民法院、最高人民检察院、公安部联合发布了《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》（以下简称《意见一》），为公检法机关依法办案提供更加明确具体的适用法律依据。四年来，全国公安机关、检察院、法院适用刑法、相关司法解释以及《意见一》侦查、起诉、审判了一大批电信网络诈骗犯罪案件及其关联犯罪案件，95%以上的被告人被判处有期徒

刑以上刑罚，对于有效打击遏制电信网络诈骗犯罪活动发挥了重要作用。

为适应新形势的发展和现实斗争需要，进一步明确法律标准，依法严厉惩治、有效打击电信网络诈骗及其关联犯罪，最高人民法院、最高人民检察院、公安部针对实际情况，坚持问题导向，深入调查研究，广泛征求意见，反复研究论证，根据刑法和有关司法解释的规定，联合制定出台了《意见二》。《意见二》在《意见一》的基础上，对于电信网络诈骗犯罪以及涉手机卡、信用卡犯罪等关联犯罪，提出更加明确具体的适用法律依据。我们相信，《意见二》的制定出台，对于政法机关更加有力、准确、及时、有效地打击电信网络诈骗犯罪及其关联犯罪，必将发挥重要的作用。

《意见二》共十七条。针对司法实践中存在的新的突出问题，如电信网络诈骗犯罪案件及关联犯罪案件的管辖、跨境电信网络诈骗犯罪案件的取证、涉手机卡、信用卡即所谓“两卡”犯罪案件的处理、办理电信网络诈骗犯罪案件的政策适用等问题进行了规定。主要体现了三方面的原则性要求：（一）继续坚持从严惩处方针，强调贯彻宽严相济刑事政策；（二）继续坚持全面惩处方针，突出打击“两卡”犯罪重点；（三）继续坚持依法惩处方针，注重加强办案程序性保障[3]。

四、 12381 涉诈预警劝阻短信系统正式启用 首次实现对潜在受害用户短信实时预警

7 月 14 日，工信部联合公安部在京举行 12381 涉诈预警劝阻短信系统启动仪式暨新闻发布会，正式启用 12381 涉诈预警劝阻短信系统，通报信息通信行业防范治理电信网络诈骗工作情况。

当前电信网络诈骗作案手法变化快、迷惑性强、查处难度大，严重侵害人民群众的财产安全与合法权益。工信部联合公安部进一步创新工作方法和思路，坚持打防并举、防范为先，想方设法减少发案，研发了 12381 涉诈预警劝阻短信系统，首次实现了对潜在涉诈受害用户进行短信实时预警，最大限度为群众避免损失。

会上，工信部反诈中心演示了 12381 涉诈预警劝阻短信系统功能。该系统可根据公安机关提供的涉案号码，利用大数据、人工智能等技术自动分析发现潜在受害用户，并通过 12381 短信端口第一时间向用户发送预警短信，提示用户可能面临“贷款”“刷单返利”“冒充公检法”“杀猪盘”等 9 类电信网络诈骗案件。当用户接收到 12381 涉诈预警劝阻短信时，说明正遭受网络诈骗侵害，应提高警惕，及时中止与诈骗分子联系或止付资金，如有疑问可拨打公安机关 110、96110 号码进行咨询。该系统不关联用户个人信息，全程无人工干预，部署了防攻击、防泄露、防窃取等防护手段，可有效保障个人信息安全[4]。

参考文献

[1] 工信部. 工业和信息化部扎实部署推进"断卡行动"[EB/OL] https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_f0d26b02263e4341b91514d8214d0fea.html, 2021/07/06

[2] 中国政府网. 公安部组织开展新一轮集中收网行动 依法严厉打击涉电信网络诈骗APP 技术开发违法犯罪团伙[EB/OL]. http://www.gov.cn/xinwen/2021-05/12/content_5605957.htm，2021/05/12

[3] 公安部. “两高一部”发布《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》[EB/OL]. https://www.mps.gov.cn/n2254098/n4904352/c7942849/content.html,2021/06/22

[4] 新华网. 12381 涉诈预警劝阻短信系统正式启用 首次实现对潜在受害用户短信实时预警[EB/OL]. http://www.xinhuanet.com/legal/2021-07/15/c_1127656923.htm,2021/07/15