中国手机安全状况报告 2021年度

电信网络诈骗

打防管控宣

涉网犯罪反制

网络黑灰产

出品单位：360手机卫士、360天枢智库、360政企安全联合发布

前言

近年来，随着我国经济社会向数字化快速转型，犯罪结构发生了根本性变化，传统犯罪持续下降，以电信网络诈骗为代表的新型犯罪快速上升并成为“主流”，严重阻碍了我国数字经济的健康发展。通过 360 手机卫士近 10 年来对黑灰产研究，发现现阶段，整体黑灰产业链，已经形成了较为“金字塔”形的结构体系，自上而下人员数量逐渐增多，技术门槛逐步降低，产业分工明确。作为金字塔顶层的负责技术以及信息服务的人员，是整个产业链的技术核心，不断迭代其诈骗手法以及对抗手段，导致电信网络诈骗等新型网络犯罪打不胜打，防不胜防。

在 2021 年黑产链条节点上，诈骗引流产业逐渐脱离境内渠道商而采用境外渠道商，今年发现高发的杀猪盘、虚假兼职、身份冒充等诈骗场景中，均出现国际通道短信以及境外电话的身影；诈骗手法从恶意行为转向欺诈内容，各类恶意、涉诈应用开始降低应用索要手机权限的比重，甚至不索要手机权限，转而通过内容引导的方式，直接要求或诱骗受害人转钱；部分黑产依托于互联网商业化技术完成自有化生态环境建设及闭环，部分诈骗团伙为掌控整个诈骗环境，使用第三方聊天 SDK 搭建集成涉诈网站的通联应用实施诈骗；同类诈骗窝点抱团数量增加、同一窝点业务多元化，导致识别、鉴别、拦截难度直线递升，用户在未依靠网络安全工具的情况下，仅依靠社会经验、安全常识，已不具备鉴别的能力，已从全民识诈转变成黑产技术反制 + 全民反诈知识能力提升。

面对严峻的电信网络诈骗现状，公安部陆续开展了各类专项打击行动，2021 年截至 11 月，全国共破获电信网络诈骗犯罪案件 37 万余起，抓获违法犯罪嫌疑人 54.9 万余名[1]，黑产在国内的生存空间遭到严重压缩。与此同时，360 手机卫士与北京反诈中心联合推出了“360 手机卫士反诈中心”，是反诈中心首次融入到一款大众化的网络安全产品中，既是反诈举措深入民间的具体行动，也是警企合作共同普及反诈的典范。

《2021 年度中国手机安全状况报告》将从黑灰产业链现状、诈骗手法、攻防手段入手、依托 360 安全大脑能力，深度剖析电信网络诈骗等新型网络犯罪，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-黑灰产业链现状

第一章　信息泄露成精准定向诈骗的主要帮凶

经济的快速发展和信息网络的广泛普及，使得大众对于互联网的依赖性越来越强，个人信息不断在互联网留下痕迹，于此同时，个人信息经济价值的日益显著，导致侵犯公民个人信息的犯罪屡打不绝，且成为滋生电信网络诈骗、敲诈勒索等下游违法犯罪的源头，社会危害日益突出并多发。

一、移动互联网使用的各类必要条件“藏匿”隐私安全隐患

移动互联网的普及，移动终端的激增，满足大众日常使用所需的应用类别不断扩增，一些 APP 会通过借助操作系统向用户申请开启权限来收集相应的个人信息，过度索取权限已成为了行业的“潜规则”。反观用户角度，大多数人在面对 APP 的权限授权提示时，并未深究其授权目的，也较难判断必要权限与过度索取权限，导致个人信息被过度收集，于此同时，部分企业安全意识、安全建设能力、登录校验机制薄弱，冒充登录、数据库被“脱库”事件频发，个人信息安全难以保障。

二、黑灰产业中窃取个人信息技术手段日趋成熟

短信嗅探技术、免杀木马技术、应用伪装技术，悄无声息实现信息窃取。目前市面上的 APP，在进行用户登录校验时，多使用短信验证码的方式，即账号与设备绑定，验设备不验人，故当前不法分子可通过短信嗅探技术截获短信验证码，登录受害人账户进行资料修改、转账等操作。同时由于安卓市场的多样性，用户可通过多种渠道获得应用安装包，不法分子逐渐脱离常见的应用商店，通过如下图展示的分发平台传播“免杀”的、界面伪装的恶意程序诱导受害人安装，截获受害人手机中的个人信息，借此盗刷资金或进行敲诈勒索。

图 1　分发平台界面

三、精准的个人信息成诈骗人员定向诈骗的利器

受害人之所以相信骗子，源于对方准确的说出了其身份、购物、资产等信息，因此在庞大的地下黑灰产隐私窃取行业中，网络诈骗的信息窃取显得更加有针对性，不再是早期盲从的“脱库”，而是进行例如同生活圈、同朋友圈等社会工程学挖掘，试图完整的掌握特定人员的生活习惯与轨迹，完成画像分析，再使用定制的剧本进行精准的定向诈骗。

第二章、境外号码替代境内号码，成诈骗电话、诈骗短信传播主力

近年来，随着我国经济社会的快速发展，犯罪结构发生了根本性变化，传统犯罪持续下降，以电信网络诈骗为代表的新型犯罪快速上升并成为主流，面对严峻的电信网络诈骗现状，公安部陆续开展了“断卡”、“打猫”等专项打击行动，黑产在国内的生存空间遭到压缩。无卡可用后，一部分黑产选择通过技术手段进行断卡攻防对抗，一部分黑产开始向境外引流产业转移，使用境外号码，拨打诈骗电话，发送诈骗短信。

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，我们发现在2021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，且数量远高于传统的境内号码。同时，在研判的过程中，我们发现境外诈骗窝点有存在使用号码防封技术的现象。

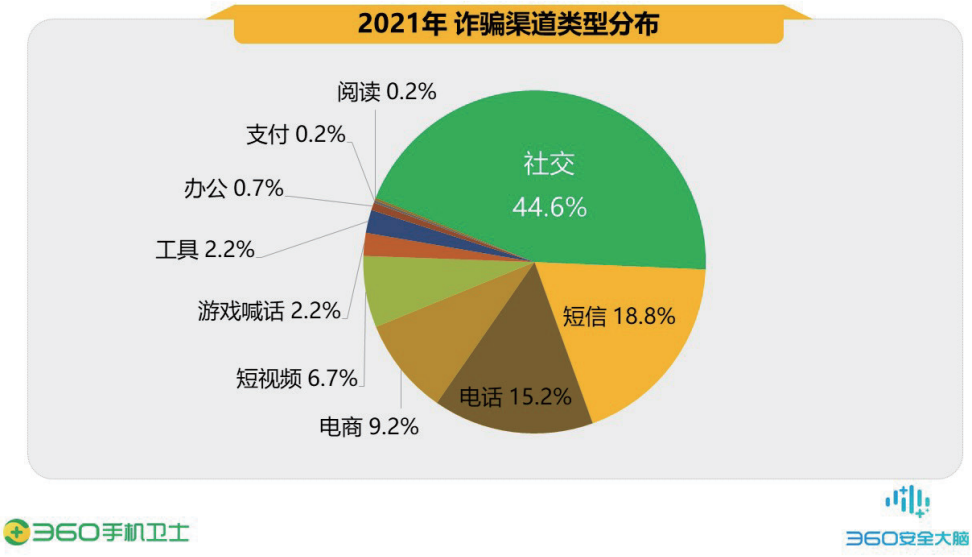


图 2　2021年诈骗渠道类型发布

一、境外短信推广渠道及发送方式

2021 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，例如诈骗短信“0060**：你好，你出 1OO，埒 1OOO，1 岍 5OOO，伽 \/:1**”。目前一部分诈骗窝点自己搭建卡池，一部分使用第三方的国际短信渠道，在分析中发现境外社交软件群相较于其他渠道推广态度更加明确，国际短信渠道商在推广过程中，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，甚至还可提供短信攻防内容模板。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。

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，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。

图 3　境外短信渠道发送的ETC诈骗短信

二、境外诈骗电话呼出原理

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。

图 4　网络电话APP购买网络电话号码节目

三、境内黑产号码防封手段

于此同时，黑产使用号码魔方、防封 APP，提高拨打诈骗电话成功率、降低号码被封率。号码魔方是一款涵盖全国号码库资源，可以指定地区按指定格式或号码段生成号码的软件，即将号码按地区、指定规则、运营商、号码去重等进行分类处理的号码组合筛选。结合空号检测、号码组合、某信检测等功能，快速实现组合并筛选出有效号码，降低群呼号码失效率。

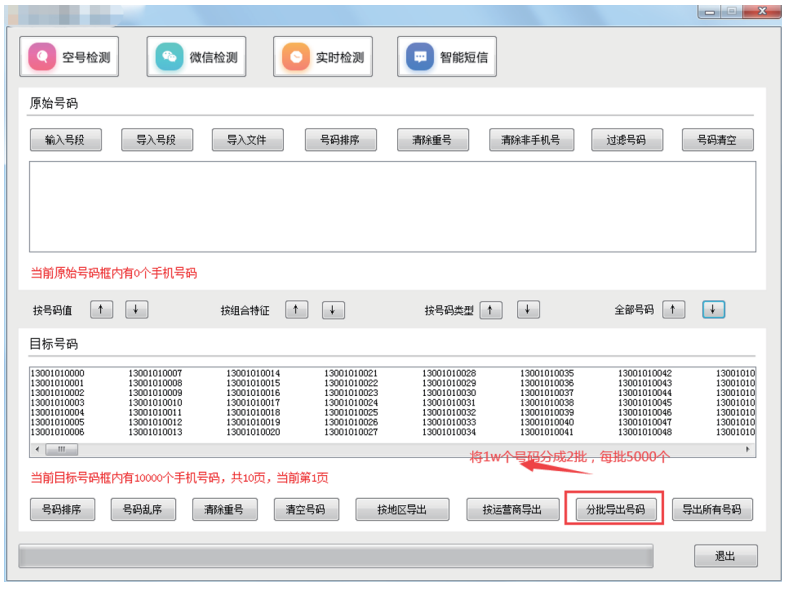


图 5　号码魔方“清洗”号码界面

通过防封产业“流出”的技术解读，目前“运营商”主要通过高频电话、号码投诉等方式收集号码并进行冻结处理。鉴于此种封号策略，市场旺盛的外呼行业，针对性的演变出了呼叫转移、AXB、回拨防封手段。

呼叫转移防封指的是通过软件呼叫转移功能把自己手机号来电转接默认设置为每一个外呼的客户手机号，来实现拨打自己的手机号转接到客户那里。即“自己给自己拨打多次电话，并不会触发运营商的高频封号，从而实现降低封卡风险”。例如，A 通过防封 APP/ 手机设置，将 A 手机号呼叫转移至客户 B 手机号。A 手机号向 A 手机号拨打电话，即可实现 A 号码与 B 号码通话，此时 B 收到的来电号码是 A。由于是 APP 自动设置呼叫转移，通话结束后自动解除呼叫转移，不会影响号码的日常使用。

AXB 模式防封指的是利用透传技术，将给不同的客户打电话，改为给一个固定的号码拨打电话，即中间号。例如：用户 A、B 通过 X 号码 1 对 1 绑定，A 呼叫 B（X 号码介入防封处理转接到 B），B 手机来电显示为 A 用户号码。此种方式从运营商业务上看，是给同一个号码拨打电话，并未产生频繁外呼多个号码的情况，未触发风控封号场景。

回拨电话防封指的是使用第三方回拨电话，即中间号码给双方拨打电话，外呼人员从呼叫方转变成接听方，因为是接听，所以也不会被监测判定为营销行为而封号。

第三章、免签、代收、代付技术成诈骗主流洗钱方式

虚假网赚、虚假投资等诈骗场景中，受害人之所以轻易相信对方，缘于骗局早期，能够获得骗子返回的任务佣金。但短期向不同人员过于频繁进行多笔小额资金支付，轻则引起支付平台的风控警觉，重则遭遇冻卡、断卡风险，那诈骗窝点是如何解决支付难题的呢。于此同时，由于个人无法开通某信、某宝接口，黑产又是如何快速将平台收款与支付订单进行匹配的呢。

一、免签支付成黑产支付接口短缺“救星”

由于个人无法申请微信和支付宝接口，若涉诈平台使用个人二维码进行收款，当充值订单较多时，无法及时匹配订单，故黑产人员使用免签技术进行支付回调。主要方式是利用 APP，监听某信、某宝的收款通知栏的通知 ，做支付回调通知，与支付订单相匹配，实现支付接口的效果。目前免签技术已十分成熟，互联网黑市随处可见免签支付搭建教程与源码。

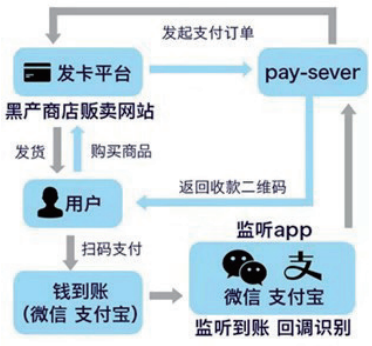


图 6　免签支付流程

图 7　免签支付APP界面

二、代收型、USDT 手段成跑分洗钱重要方式

以高额兼职返利为诱饵，吸引并发展大量正常用户为其提供支付账号，从而将涉诈资金流水隐匿与正常用户的资金流水中，逃避追溯，这便是跑分平台经典的操作方式。根据支付产业的不同，其分为代收型跑分、代付型跑分；根据跑分抵押物的不同，分为人民币跑分、虚拟货币跑分。

代收型跑分指的是吸引用户为其提供收款服务，早期黑产为解决赌博平台收款渠道短缺，银行卡短缺、个人收款账户易风控，企业收款账户黑市价格高等问题，使用兼职众包的形式，通过抵押人民币的方式，吸收大量跑分客的个人某宝、某信收款账户，租借给博彩平台做收款账户。随着虚拟货币的兴起，稳定币的出现，抵押物由人民币转为虚拟货币。这里以赌博平台使用虚拟货币跑分为例，当赌客在赌博平台上有充值需求，赌博平台会将该需求发送到对应的“跑分”平台上，“跑分”平台根据充值金额的需求生成订单并挂单至App 前端供“跑分客”抢单，随后“跑分客”抵押数字货币进行抢单，抢单成功后上传其本人的收款二维码，“跑分客”二维码通过反向链路传输到赌客端，赌客进行付款，“跑分”平台确认赌客已支付，订单完成，并将等额的“跑分客”数字货币押金划拨、扣除。

以代收方式相对的是代付，代付型跑分指的是以高额兼职返利为诱饵，吸引用户为其提供其支付账号，从而转租给下游的诈骗团伙，提供小额付款服务。

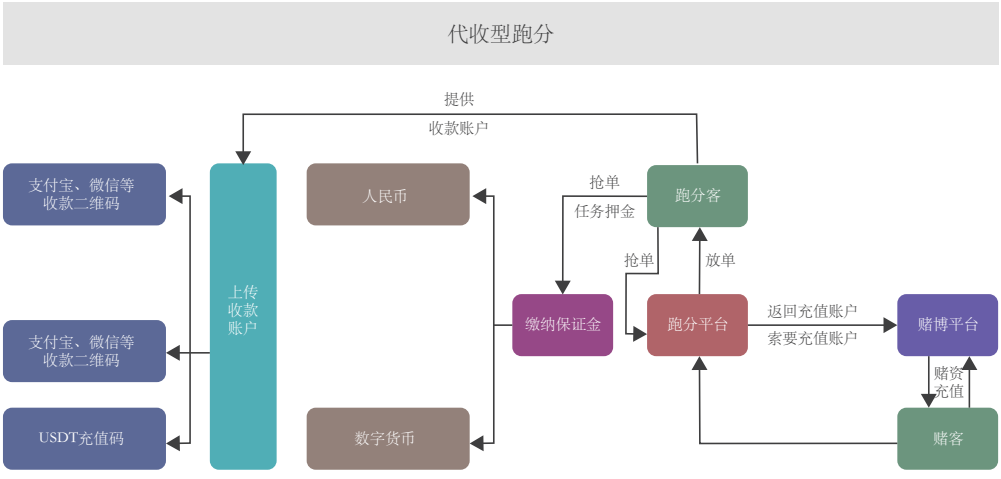


图 8　跑分流程

由于某宝、某信风控等原因，黑产使用的某宝、某信收款账户易被冻结，如何能让受害人扫码转账的时候，资金是直接流转至银行账号，而不是第三方支付账户呢？为此黑产演变出了码转卡产业，即扫码支付二维码后，由原先跳转到“转至某宝账户”，变成跳转至“转账至银行卡界面”，包括某宝转银行卡 / 飞行模式转卡 / 某宝 H5/ 某宝飞行转卡四种方式。于此同时，为提升资金流转效率，黑产使用代付 APP，模拟人工操作网银 APP 进行自动化转账操作。

图 9　自动转账APP运行界面

第二篇 电信网络诈骗-黑灰产攻防技术趋势

第一章、涉诈APP采用界面伪装进行攻防对抗

一款名为“计算器”的安卓应用，在 2021 年出现在安全研究员的面前，其界面与普通计算器并无差异，具备基础的计算功能，但逆向分析后发现，其实际上是一款经过伪装的博彩代理应用，具备成员管理、佣金报表等功能。

博彩代理主要职责是为博彩平台引流推广带来赌客，博彩平台根据代理的业绩给予业务提成。这里以某博彩代理平台的代理说明进行举例，博彩代理的利润主要来自于赌客的提成，与传统销售不同的是，前者属于一次性抽成，后者赌客在参赌过程中会反复产生收益。例如，赌客充值 100 元钱，按照 2.5% 的返佣计算，代理佣金 2.5 元，赌客获利 90 元，又投入 190 元，代理佣金 4.75 元，即赌客 100 元成本，代理获得 2.5+4.75=7.25 元收益。

图 10　博彩代理伪装成计算器界面

一、博彩平台主要功能

为了更好的阐述博彩代理产业链，这里从博彩网站的前台和后台功能角度出发进行分析。博彩平台一般包含博彩项目、合营2个板块，前者为赌客服务，后者专属于代理人员，博彩项目主要为体育、真人、棋牌、电竞、彩票、通过追溯分析发现，每个博彩项目虽跳转的URL不同，但其上线的服务器为同一个，只是方便市场投放，针对不同的项目推出了不同的项目APP进行精准盈利。如集成“体育、真人、棋牌、电竞、彩票、电子竞技”项目的全站APP、仅有电竞项目的电竞APP。

二、博彩代理合营计划

合营指的是博彩平台的代理项目，以拉新返佣的方式，吸引赌客成为博彩平台代理，例如代理 A 为获得佣金，给赌客 B 提供了防溢出的博彩平台应用，赌客 B 不想自己在博彩平台充值，代理 A 在博彩平台代理后台充值后，使用代理代充向赌客 B 在博彩平台的账户充值赌资，赌客 B 参与博彩活动。为方便代理进行合营运营，提供了 2 种用于代理管理赌客的方式，代理管理网站和代理管理 APP，两者内容相同，均包含下级管理、财务中心、提款记录、额度充值、代理代充、财务报表、佣金报表、账变明细、推广中心。只是代理 APP 使用了技术伪装，输入特定的字符才能显示正常的代理 APP 界面。

（1）下级管理

包含会员管理、游戏记录。主要对下线代理赌客进行管理，包括赌客的充值、提款、投注记录、输赢记录、注册时间、登录时间。

（2）财务中心

包含提款记录、代理代充、额度充值、财务报表、佣金报表、账变明细。提款记录指的是将佣金提现至自己的银行卡或虚拟货币账户；额度充值、代理代充指的是代理将资金充入代理平台，给赌客进行赌资代充值；财务报表、佣金报表、账变明细指的是代理的收益情况；推广中心，主要是提供含代理 ID 号的博彩链接（PC 端、H5 端、APP 版），若代理觉得链接太长，不方便传播，该产业还提供防封短链接。

（3）防溢出推广

为了方便代理人员邀请下线注册，博彩平台会给代理人员提供含代理人员参数 ID 的博彩网址、博彩 APP。赌客通过此些网站、APP 注册，代理才可获得佣金。如果下线人员没有使用指定的链接或 APP 注册，代理人员可提供注册人员 ID 进行溢出申请，从而将代理人员与赌客绑定。

（4）支付方式

随着支付方式的发展，演变出了传统转账、代客充值、虚拟货币三种赌资充值方式，传统转账指的是网银转账 / 支付、极速转卡（网银实时转账到银行卡）、银行卡转账 / 转卡、支付宝转账 / 转卡 / 支付、微信转账 / 转卡 / 支付、快捷支付、京东支付、云闪付转账 / 转卡；虚拟货币指的是使用虚拟货币钱包，扫描博彩平台虚拟货币收款二维码，进行虚拟货币转账；代客充值指的是代理人员在代理平台为赌客代充值。出于躲避风控的考虑，目前博彩行业代客充值、虚拟货币充值逐渐成为主流。

图 11　博彩网站使用的支付方式

第二章、裸聊敲诈出现资产保护、免杀、远控等功能变种

当前通过恶意 APP 窃取个人信息、偷录“裸聊”画面，实施网络敲诈勒索违法犯罪活动呈现爆发式增长，成为比较突出的网络违法犯罪。在作案方式上虽与传统的电信网络诈骗相似，但由于诈骗分子掌握到受害人私密信息，对受害人进行恐吓和威胁，成功率远高于传统的哄骗投资类、身份冒充类等电信网络诈骗。2021 年全年，360 安全大脑共截获移动端新增恶意程序样本约 943.1 万个，同比 2020 年（454.6 万个）增长了 107.5%，平均每天截获新增手机恶意程序样本约 2.6 万个。移动端新增恶意程序类型主要为资费消耗，占比 95.3%；其次为隐私窃取（4.1%）、流氓行为（0.5%）与远程控制（0.1%）。下图为 2021 年移动端新增恶意程序类型分布：

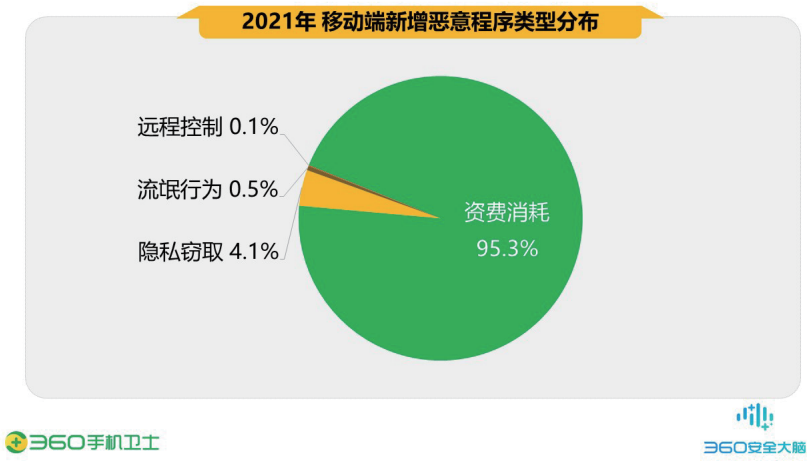


图 12　2021年移动端新增恶意程序类型分布

目前在黑产渠道，裸聊敲诈类开源程序已泛滥成灾，拉低了整个行业的技术门槛，仅通过 web 封装的方式即可实现批量上线生成裸聊敲诈类应用。随着各方对裸聊敲诈类诈骗的重视及打击，裸聊敲诈类应用传播路径被阻断、应用程序被查杀，诈骗成功率下降。

但在今年下半年，我们发现裸聊敲诈产业出现了变化，在针对人群上，仍以安卓用户为主，但增加了对 IOS 系统的技术投入。在攻防技术上，增加了资产保护、程序免杀、手机远控等技术；在关联黑灰产业链上，从分散的应用签名、分发、防封转变成支持一站式运维服务。这里从第二代裸聊敲诈 APP 分析入手，对裸聊敲诈产业进行解读。

一、应用静动态分析

第二代与第一代裸聊勒索 APP 利用手法相同，均是利用 APP 展示色情界面，诱导受害人给予 APP 权限，进而盗取个人隐私信息。当受害人安装应用并启动后，应用加载并给用户展示前台 web 页面，诱导受害人输入手机号、ID 号，授予电话、联系人、短信、相册等权限。一旦用户给予权限，设备信息、通讯录、短信、相册数据便实时回传至诈骗服务器。

第二代相较于第一代，加大了域名和服务器成本投入，增加了域名和服务器的数量，第一代前台展示页和数据回传页使用相同的域名 /IP，仅是通过子域名或链接参数进行区分，一旦前台 WEB 遭遇 DNS 封堵，

数据回传也失效。第二代不仅 WEB 页面和数据回传使用不同的域名和服务器，不同的数据也使用不同的回传服务器，以此降低数据失效风险，并且在回传链接上增加了端口，防止域名暴露后，后台被暴力破解。

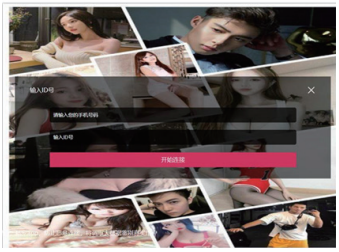


图 13　裸聊敲诈应用界面

当用户在 web 页面填写内容后，js 调用安卓，索要电话、短信、通讯录、SD 卡权限，若未提供权限，提示“App 所需基本权限 ，请允许，未允许将无法提供服务”。获得信息后拼接回传地址 url+ /api/+ 参数（myRoom+ 安卓 ID 等），不同的数据使用不同的回传地址。

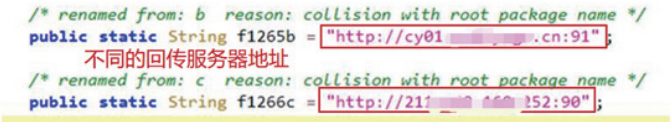


图 14　裸聊敲诈APP回传数据代码逻辑

二、应用攻防特点

通过已掌握的程序说明文件来看，此套程序在增加攻防策略的基础上，还增加了用户过滤、下载链、服务器防封、远程控制等功能。用户过滤指的是为防止多部设备的受害人使用非常用手机安装此 APP，检测安装设备的通讯录数量是否大于 2 条，否则提示 APP 不兼容，引导受害人使用含有联系人的手机进行操作，APP 弹窗提示的说服力强于诈骗人员的话术说服力。

由于各方针对裸聊敲诈类诈骗打击力度的加强，会出现下载链（二维码）失效；用户扫码后，链条跳转至手机浏览器被提示风险；服务器被封后，受害人安装 APP 后，窃取的隐私信息不回传，提供下载链更换、浏览器安全提示防红、APP 服务器更换服务。

远程控制功能指的是通过裸聊勒索后台点击远程按钮后，受害人该 APP 的界面弹出“清理病毒”窗口，诱导受害人点击授权后，可实时查看用户屏幕、也可与用户通话。从黑产渠道传播情况看，今年 7 月份有人在黑产论坛，发布了第二代裸聊勒索 APP 的求购需求，说明第二代裸聊勒索在 7 月前已经在黑产内部圈子中小规模流转。

图 15　某黑产论坛交流裸聊敲诈APP源码

第三章、虚拟货币钱包成盗币黑产目标

一、“空投”、钓鱼网站、虚假钱包APP成主要“盗币”方式

今年9月，监管重拳出击治理“币圈”乱象。国家发改委联合十部委发布《关于整治虚拟货币“挖矿”活动的通知》，人民银行联合十部委发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》，被称为史上最严格虚拟货币政策（简称“924政策”）。政策规定虚拟货币相关交易活动均属非法，随后相关APP在各大应用商店相继下架。“无孔不入的诈骗分子利用这一时间差，找到了可乘之机”。利用用户急于交易的心里，通过多种方式“盗走”用户虚拟货币资产。

目前主要以下3种手法：第一类，以糖果、空投为名，赠送代币的方式，诱导受害人安装虚假的虚拟货币钱包；第二类，冒充虚拟货币交易所，以受害人账户存在风险为由，诱骗用户安装含屏幕共享功能的会议APP、虚拟货币钱包，获得受害人的虚拟货币钱包助记词后，盗取虚拟货币；第三类，通过山寨虚拟货币钱包网站、推广假冒的虚拟货币钱包应用。部分用户由于经验不足、风险意识不强，误入假冒的网站，下载了假冒的虚拟货币钱包，随后被骗子通过approve授权方式盗走虚拟货币。故很多受害人回顾整个过程，百思不得其解，诸如对助记词的保护这样的关键环节也都严格按照网上提醒的过程操作，为什么而还是被盗了。

二、简体中文、英文、日语用户为“盗币”产业主要受害人

通过深入挖掘发现，冒充正规虚拟货币钱包平台这伙人有备而来，通过 360QUAKE 网络空间测绘平台分析，发现仅冒充 im** 虚拟货币钱包的钓鱼网站关联服务器就多达几十个，IP 归属地涉及韩国、美国、新加坡、日本、中国香港等地，关联网站字体涉及简体中文、英文、日语，说明此批黑产人员的目标为全球虚拟货币用户。

通过对此类网站源码复现，发现其后台主要包含空投页面、下线代理、鱼苗统计等功能，空投页面指的是根据虚拟货币名称自动化生成空投的钓鱼页面，例如狗狗币、火币，当受害人访问此钓鱼页面，并点击获得空投时，页面会拉起手机已安装的虚拟货币钱包 APP，当受害人在虚拟货币钱包完成授权（approve）操作后，其虚拟货币授权信息就进入到了鱼苗管理页面中。通过鱼苗管理页面查看每日截获的虚拟货币授权信息，进行批量盗刷。同时为了售卖盗币系统，通过代理下线的功能，售卖盗币平台后台权限。

图 16　某虚拟货币钓鱼网站盗取的信息

据相关报道，因下载假虚拟货币 APP 导致资产被盗的用户规模逾万人，被盗金额高达十三亿美元。鉴于恶劣的黑产环境，360 安全大脑已上线“虚拟钱包诈骗模型”，用户安装风险 APP 时，360 手机卫士会及时拦截，避免用户遭受财产损失。

第四章、“第三方聊天系统”助力黑产完成诈骗生态闭环

一、依托“第三方在线客服系统”，黑产摆脱传统社交软件“易冻号”束缚

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，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。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。

图 17　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。

二、依托“通联 APP”，黑产完成诈骗生态闭环

部分诈骗团伙为掌控整个诈骗环境，使用第三方聊天 SDK 搭建集成涉诈网站的通联应用实施诈骗。以虚假兼职诈骗使用的通联应用为例，不法分子通过发送“确认收货，送早餐机”的短信吸引受害人关注，随后以领任务的方式，诱导受害人安装通联 APP，通过该软件的聊天功能给用户发布兼职任务，即要求受害人在该软件内嵌的虚拟货币平台完成指定的投注刷量操作，受害人前期完成任务后，给予蝇头小利，待用户增

加投注金额后，拒绝提现请求，骗走资金。该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。

图 18　某通联APP界面

通过对应用逆向分析，发现此类应用通过第三方聊天 SDK 进行搭建，应用框架搭建完成后，将诈骗网址内嵌在该聊天软件中，后续通过引流话术，将受骗人拐骗盗到该聊天软件中进行话术洗脑。一方面，避开了传统聊天软件的风控封号机制；一方面涉诈网站内嵌在通联应用中，受害人无法查看到具体的网址，不能使用浏览器访问该网址，也不会触碰到浏览器的安全风控。于此同时，由于应用增加了验证码机制，安全分析人员即使获得应用安装包，在缺乏邀请码的情况下，传统分析手段也很难捕获该网址。借助通联应用，黑产人员完成了诈骗场景的闭环。

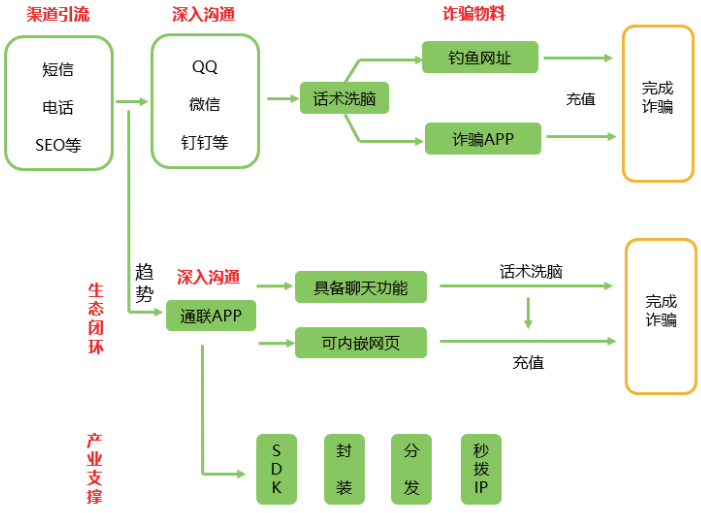


图 19　利用通联APP诈骗路径

第三篇 电信网络诈骗场景

第一章、新技术应用

一、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某信，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，添加了短信内的某信账号，骗子确认用户是通过短信添加后，邀请用户进某信群领礼品。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。

图 20　虚假兼职引流话术

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、某信多次引流跳转，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，诱导添加某信的短信，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。

二、开了个屏幕共享，钱没了

虚拟货币高价值属性吸引了大批用户进场，互联网出现了一种冒充虚拟货币交易所客服，盗取虚拟货币钱包“助记词”的诈骗手法。诈骗分子去电用户后，自称是某虚拟货币交易所安全中心风控部的客服人员，用户在该交易所购买的虚拟货币，被查出卖家存在涉嫌“洗钱”行为，需要用户配合调查。随后引导受害人安装含屏幕共享功能的“会议”APP 和新的数字货币钱包 APP。

进入会议后，引导用户将原虚拟货币交易所的虚拟货币转移至新的虚拟货币钱包中进行账户升级维护，升级维护后平台将返还用户虚拟货币，期间不会有任何损失。但用户发现资金丢失，无法联系到对方，得知受骗。

专家解读

受害人在使用虚拟货币钱包过程中,被诈骗人员利用视频会议 APP 的屏幕共享功能,获取了钱包助记词。利用助记录登录受害人钱包或其他钱包导入助记词功能，获得了虚拟货币的所有权，进行了资产转移。

安全提示

接到“客服”类电话，对方要求进行资金相关操作时，切记通过其他渠道确认客服真伪，同时勿向对方提供涉及资金相关的信息，例如银行卡密码、短信验证码、钱包助记词等。

第二章、新话术场景

一、诈骗短信盯上“新冠疫苗预约”

在全网关注新冠疫苗怎么“打的”当下，网络犯罪分子再次“趁机搅局”，360 手机卫士接到用户反馈称其收到境外号码发送的仿冒新冠疫苗预约接种的短信，点击短信中的“中国疾病预防控制中心网站“后，页面要求填写姓名、银行卡号、银行卡密码、余额、手机号、手机短信验证码等信息，当填写完以上信息后，页面则以审核未通过为由，要求受害人保持卡内余额超过 5000 元，随后受害人的银行卡资金被盗刷。

图 21　虚假疫苗预约短信

专家解读

此类诈骗利用了疫情之下，人们迫切进行新冠疫苗接种的需求，诱导受害人访问钓鱼网站。通过对钓鱼网址源码分析，发现其首先通过 UserAgent 判断访问设备类型，当访问设备不是手机版浏览器时，提示请使用手机登录；使用 Drop-Ip 功能屏蔽指定地区的 IP；使用支付校验接口判断页面所填写的银行卡号所属银行及是否符合银行卡号规则，实现限制安全研究人员对钓鱼网站进行分析，提高钓鱼网站仿真度和存活时长。

安全提示

提高安全意识，不要轻易点击此类短信中拦截，对于安全软件已拦截的网站不要继续访问。切记对以各类理由索要银行卡密码、银行卡交易验证码的行为提高警惕。

二、“分享朋友圈领百元红包”，这波“福利”你赶上了吗？

2021 年春节期间，不少群出现了诱导分享“红包”广告，如“** 捞两亿生活补贴”、“新婚福利红包”等。进入链接后点击“现在去领”会出现“提现红包”的界面，点击“提取”会跳转至抢到“227.91 元”的界面，点击领取会提示分享后才能领取。看到此种链接，由于抽中的现金红包不少，也没要求填个人信息，上演了群、朋友圈互转链接的现象。但点击分享后，红包没领到，页面却无法回退，不断刷新出各式各样的色情小说、虚假兼职广告

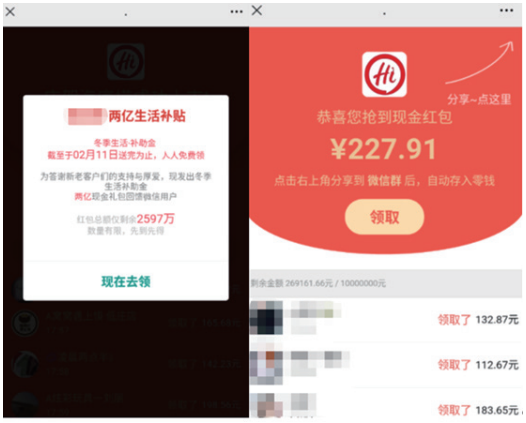


图 22　虚假红包钓鱼网站界面

专家解读

此类红包并不能领取，是黑灰产为色情小说、虚假兼职广告引流的手段。黑灰产使用强制裂变分享源码搭建红包引流平台，当用户访问该红包链接后，强制用户分享，当用户以为分享成功后可以领取红包时，自动跳转到对应的广告页面，当访客点击返回时跳转广告页面。以此不断在页面轮回刷新广告。

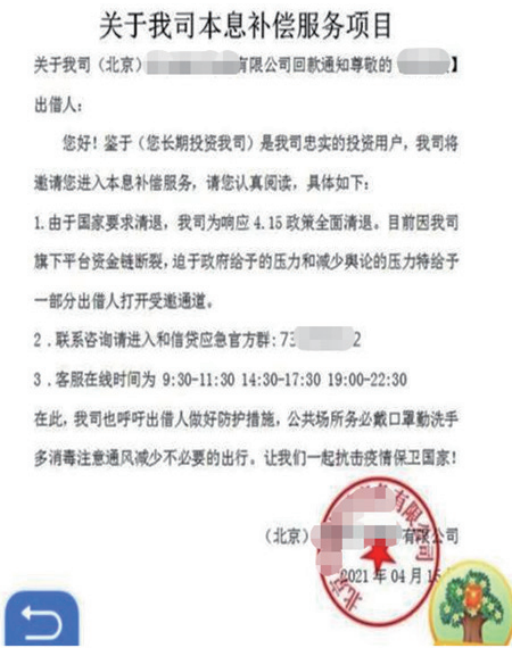
专家解读

需要分享朋友圈才能领取的“红包”，目的就是诱导关注营销公众号或者垃圾广告，不要点开陌生链接，小心手机被安装木马病毒而导致金融账户被盗刷。对于需要填写详细的个人信息才能领取的“红包”，绝对有诈！骗子通过信息掌握你的个人情况和关系网络，便可针对性实施诈骗。

三、P2P“内策回款”骗局

用户是“和信贷”的出借人，该平台3年没回款。用户在互联网看到了“和信贷最新消息”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，根据群主的指引，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，即在指定的美盛资本 APP 进行充值、投资操作。用户在美盛资本 APP 充值3772元，在规划师的引导了下进行回款操作，但首笔就亏损10元，要退出被客服拒绝后，发觉受骗。


关于我司本息补偿服务项目

关于我司（北京）[redacted]有限公司回款通知尊敬的[redacted]】

出借人：

您好！鉴于（您长期投资我司）是我司忠实的投资用户，我司将邀请您进入本息补偿服务，请您认真阅读，具体如下：

1.由于国家要求清退，我司为响应4.15政策全面清退。目前因我司旗下平台资金链断裂，迫于政府给予的压力和减少舆论的压力特给予一部分出借人打开受邀通道。

2.联系咨询请进入和信贷应急官方群：73[redacted]2

3.客服在线时间为 9:30-11:30 14:30-17:30 19:00-22:30

在此，我司也呼吁出借人做好防护措施，公共场所务必戴口罩勤洗手多消毒注意通风减少不必要的出行。让我们一起抗击疫情保卫国家！

（北京）[redacted]有限公司

2021 年 04 月 15

图23　虚假回款引流话术

专家解读

从诈骗手法上看，其为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，引导至点位盘平台，对股票、贵金属、虚拟货币进行买涨或买跌的投机行为。本次案例，其借助大量 P2P 处于跑路阶段，出借人无法回本的背景，在互联网发布回款新闻，吸引受害人关注。对于受害人而言，我总觉得我能赚到超出认知水平以外的钱，对于犯罪分子来说，只是换个服务器，就能多骗一个。

安全提示

对于形形色色的投资骗局，总计一句话就是“甜蜜的谎言”，本质上都是以高额回报作为诱饵设下圈套，诱导受害人在指定的投资平台入金，而这些所谓的“投资平台”，不过是犯罪分子搭建的虚假外壳，看似正规，实则后台暗箱操作，切勿轻易相信零风险高回报的项目。

第四篇 反电信网络诈骗行业动态

第一章、法律法规颁布

一、数据安全法：护航数据安全 助力数字经济发展

随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。党中央对此高度重视，就加强数据安全工作和促进数字化发展作出一系列部署。按照党中央决策部署和贯彻总体国家安全观的要求，全国人大常委会积极推动数据安全立法工作。经过三次审议，2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议通过了数据安全法。这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于 2021 年 9 月 1 日起施行。

制定数据安全法是维护国家安全的必然要求。数据是国家基础性战略资源，没有数据安全就没有国家安全。数据安全法贯彻落实总体国家安全观，聚焦数据安全领域的风险隐患，加强国家数据安全工作的统筹协调，确立了数据分类分级管理，数据安全审查，数据安全风险评估、监测预警和应急处置等基本制度。通过建立健全各项制度措施，提升国家数据安全保障能力，有效应对数据这一非传统领域的国家安全风险与挑战，切实维护国家主权、安全和发展利益。

制定数据安全法是维护人民群众合法权益的客观需要。数字经济为人民群众生产生活提供了很多便利，同时各类数据的拥有主体更加多样，处理活动更加复杂，一些企业、机构忽视数据安全保护、利用数据侵害人民群众合法权益的问题也十分突出，社会反映强烈。数据安全法明确了相关主体依法依规开展数据活动，建立健全数据安全管理制度，加强风险监测和及时处置数据安全事件等义务和责任，通过严格规范数据处理活动，切实加强数据安全保护，让广大人民群众在数字化发展中获得更多幸福感、安全感。

制定数据安全法是促进数字经济健康发展的重要举措。近年来，我国不断推进网络强国、数字中国、智慧社会建设，以数据为新生产要素的数字经济蓬勃发展，数据的竞争已成为国际竞争的重要领域。数据安全法坚持安全与发展并重，在规范数据活动的同时，对支持促进数据安全与发展的措施、推进政务数据开放利用等作出相应规定，通过促进数据依法合理有效利用，充分发挥数据的基础资源作用和创新引擎作用，加快形成以创新为主要引领和支撑的数字经济，更好服务我国经济社会发展。[2]

二、表决通过！个人信息安全有了专门法律保护

十三届全国人大常委会第三十次会议 8 月 20 日表决通过《中华人民共和国个人信息保护法》，自 2021 年 11 月 1 日起施行。

明确不得过度收集个人信息、大数据杀熟，对人脸信息等敏感个人信息的处理作出规制，完善个人信息保护投诉、举报工作机制……这部专门法律充分回应了社会关切，为破解个人信息保护中的热点难点问题提供了强有力的法律保障。

个人信息保护法明确了个人信息处理和跨境提供的规则、个人信息处理者的义务等内容。本法规定，任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

针对过度收集信息、大数据杀熟的问题，本法明确，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式；个人信息处理者利用个人信息进行自动化决策，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

针对滥用人脸识别技术问题，本法要求，在公共场所安装图像采集、个人身份识别设备，应设置显著的提示标识；所收集的个人图像、身份识别信息只能用于维护公共安全的目的。

对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，本法特别规定了其需要履行的义务，如建立健全个人信息保护合规制度体系，定期发布个人信息保护社会责任报告，接受社会监督等。

个人信息保护法还进一步强化了相关部门的监管职责，从严惩治违法行为。履行个人信息保护职责的部门发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。[3]

三、反电信网络诈骗法（草案）公布并公开征求意见

2021 年 10 月，第十三届全国人大常委会第三十一次会议对《中华人民共和国反电信网络诈骗法(草案)》(以下简称“草案”）进行了审议，已公布并公开征求意见。

草案共三十九条，主要内容包括：一是反电信网络诈骗工作的基本原则。强调坚持系统观念，注重源头治理、综合治理，全面落实打防管控各项措施；规定各部门职责、企业职责和地方政府职责；加强协同联动工作机制建设。二是完善电话卡、物联网卡、金融账户、互联网账号有关基础管理制度；对办理电话卡、金融账户的数量和异常办卡、开户情形进行限制，防范开立企业账户风险；有针对性地完善物联网卡销售、使用监测制度。三是支持研发电信网络诈骗反制技术措施，统筹推进跨行业、企业统一监测系统建设，为利用大数据反诈提供制度支持。规定金融、通信、互联网等领域涉诈异常情形的监测、识别和处置，包括高风险电话卡、异常金融账户和可疑交易、异常互联网账号等，规定相应救济渠道等。此外草案在加强对涉诈相关非法服务、设备、产业的治理，治理改号电话、虚假主叫和涉诈非法设备等方面也有所涉及。[4]

第二章、政府重拳出击

一、打击整治非法开办贩卖电话卡银行卡犯罪“断卡”行动成效显著

自去年 10 月全国“断卡”行动开展以来，各地各部门迅速行动，密切协作，打击惩戒治理多管齐下，集中打击犯罪团伙，清理电话卡、银行卡，从根源上有效遏制电信网络诈骗案件快速上升势头，今年 6 月至 8 月全国电信网络诈骗犯罪发案连续 3 个月实现同比下降。

一年来，国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室先后组织开展 6 次全国集群战役，全国公安机关坚持摧网络、打团伙、断通道，累计打掉涉“两卡”违法犯罪团伙 2.7 万个，查处违法犯罪嫌疑人 45 万名，查处金融机构和通信企业内部人员 1000 余名，有力打击了“两卡”犯罪分子的嚣张气焰。随着“断卡”行动深入推进，电信网络诈骗团伙获取“两卡”的寄递贩卖通道受阻，诈骗窝点用于作案的“两卡”严重不足，大量涉案资金被冻结，一些诈骗分子甚至直接利用本人银行账户转账洗钱，犯罪团伙作案成本大幅提升，对电信诈骗活动实现重创。

工作中，各地各部门坚持综合施策，强化行业治理，切实形成整体合力。最高人民法院、最高人民检察院、公安部、工业和信息化部、中国人民银行联合发布《关于依法严厉打击惩戒治理非法买卖电话卡银行卡违法犯罪活动的通告》，最高人民法院、最高人民检察院、公安部联合发布《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）》，为“断卡”行动提供了强有力法律政策支撑。工信部升级启动“断卡行动 2.0”，组织通信企业集中清理电话卡 6400 余万张，拉网排查物联网卡 14 亿张，推出“一证通查”服务切实解决冒用他人身份办卡问题。人民银行组织清理“不动户”“一人多卡”和频繁挂失补换卡等异常银行账户 14.8 亿个，对 130 余家银行和支付机构开展专项检查，暂停 620 家银行网点 1 至 6 个月开户业务。[5]

二、“断流”专案行动打掉非法出境团伙 9419 个

斩链条、断通道，挖“金主”、打“蛇头”……针对组织偷渡境外实施电信网络诈骗犯罪活动的高发态势，公安部今年 5 月以来部署全国公安机关开展“断流”专案行动，发起凌厉攻势，目前进展顺利、成效初显。

公安部 26 日召开新闻发布会。公安部刑侦局副局长姜国利介绍，“断流”专案行动已打掉“3 人以上结伙”非法出境团伙 9419 个，破获刑事案件 4160 起，抓获犯罪嫌疑人 33860 名。其中，组织招募者 931 名、运送接应者等黑灰产人员 913 名、非法出境人员 32016 名，串并破获电诈案件 1021 起，挖出境外电诈窝点 100 个、“金主”82 名。

据悉，今年 1 月至 9 月，全国共破获电信网络诈骗案件 26.2 万起，抓获犯罪嫌疑人 37.3 万名，同比分别上升 41.1% 和 116.4%；共紧急止付涉案资金 2770 亿元。6 月至 9 月，发案数连续 4 个月实现同比下降。

公安部刑侦局二级巡视员郑翔表示，在公安机关依法严厉打击电信网络诈骗犯罪的过程中，大量犯罪团伙为逃避打击不断向境外转移。受疫情等因素影响，境外电诈窝点快速增长，特别是东南亚地区已成为此类犯罪的主要聚集地。

公安机关呼吁广大群众不要受所谓的跨国“高薪职业”诱惑加入诈骗团伙，并积极提供线索，协助侦破案件，全力支持“断流”专案行动的开展。[6]

第三章、行业平台建设

一、公安部推出国家反诈中心 APP 注册用户超 6500 万 构筑防诈反诈的“防火墙”

6 月 17 日，公安部召开新闻发布会，通报全国公安机关打击治理电信网络诈骗犯罪举措成效。

公安部刑事侦查局副局长姜国利会上表示，电信网络诈骗犯罪是一种利用互联网实施的新型犯罪，公安

机关在加强打击的同时，坚持防范为先，充分利用新技术新方法，不断在加强提高群众反诈防诈的意识和能力上下功夫。

姜国利介绍，公安部推出了国家反诈中心 APP 和宣传手册，努力为人民群众构筑一道防诈反诈的“防火墙”。国家反诈中心 APP 会及时发布典型案例，普及防骗知识，提升群众防骗意识和识骗能力；对收到的涉诈短信和电话、登录的涉诈网址，会尽可能识别并发出预警提示；群众可以通过 APP 一键举报涉诈信息。目前，国家反诈中心 APP 的全国注册用户已超过 6500 万，已向用户发送预警 2300 万次，接受群众举报涉诈线索 65 万条，在防范诈骗工作中发挥了重要作用。

姜国利称,公安部精心制作的《防范电信网络诈骗宣传手册》,向广大人民群众介绍了网络贷款、刷单返利、“杀猪盘”、冒充电商物流客服、冒充熟人或领导、冒充“公检法”、虚假投资理财、虚假购物、注销“校园贷”、网络游戏虚假交易等 10 种常见的电信网络诈骗类型，剖析了典型案例、揭露了诈骗手法，为易受骗群体“量身定制”反诈防骗提示。提醒广大人民群众入脑入心，牢记“三不一多”原则：“未知链接不点击，陌生来电不轻信，个人信息不透露，转账汇款多核实”，谨防上当受骗。[7]

二、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。[8]

三、警企联合反诈！北京反诈中心联合 360 手机卫士推出“反诈中心”

11 月 9 日，360 手机卫士官方发布了其与北京反诈中心联合推出的“360 手机卫士反诈中心”。本次合作，是反诈中心首次融入到一款大众化的网络安全产品中，既是反诈举措深入民间的具体行动，也是警企合作共同普及反诈的典范。

从产品功能层面，360 手机卫士反诈中心内嵌了北京反诈中心的全民反诈 APP 入口，不仅可以一键通往北京反诈中心的全民反诈 APP，还能将 360 手机卫士的预警线索实时同步给公安。[7]公安部门可根据 360 手机卫士反诈中心提供的信息线索直接联系潜在受害者，切实提高反诈效率。不仅如此，360 手机卫士反诈中心还具备个人反诈防护、家庭反诈小组以及被诈骗求助等多重功能，可经过细分场景（诈骗前、中、后）来拆解反诈需求，再通过分级预警能力及时拦截或阻断诈骗，辅助用户及时止损，有效追损。

反诈离不开安全数据的支撑，360 手机卫士反诈中心的个人反诈防护功能，设有最全号码库，具备对境外或者 VOIP 形式诈骗电话的识别能力，可对诈骗短信中包含 QQ、微信、url，以及 APP 的下载链接，进行

本地拦截；APP 识别功能，也已获取既遂诈骗案件样本并分析扩充涉诈样本库超 20 万。

机器智能反诈只是一方面，人在反诈中同样起着不可忽视的作用。360 手机卫士反诈中心允许用户根据自身需要，组建专属家庭反诈小组，当家人收到风险电话、短信或试图安装风险 APP 时，“家庭守护者”会第一时间收到预警通知。“被诈骗求助功能”则是由 360 安全员提供人工咨询服务，给予受骗用户专业建议，协助用户及时止损，有效追损。

360 十余年来深耕网络安全所积累的安全能力，360 内部数据统计，360 在网络端平均每天需处理 300 亿 URL 数据，识别出约 40 万违法、疑似欺诈、钓鱼网址，拦截垃圾短信 1.09 亿条，拦截诈骗短信 300 万条，同时每天新增 5 万条移动终端恶意程序文件，目前为止已累计总量 7 千万高危涉诈木马病毒样本、2.4 亿风险程序样本。此次与北京反诈中心的合作，也将继续加强反诈能力。

截止至 8 月，360 手机卫士推出的决明预警平台，已累计为全国公安机关推送反诈预警数据 1697 万条。全国累积 504 家省、市、区县级公安局和运营商应用决明平台的反诈预警数据进行反诈劝阻。值得一提的是，360 手机卫士反诈中心覆盖的 7+2 类涉诈案例场景，预警精准度超过 90%。

此次，360 手机反诈中心的推出，是 360 公司坚守社会责任，承担互联网公司“科技报国”使命的体现。未来，作为个人网络安全的守卫者，360 手机卫士将联合警方，继续守护亿万中国网民的上网安全。[9]

第五篇 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

从以上内容可以看出相较于之前发现的黑产，今年的诈骗团伙在技术、引流、话术等方面均进行了产业技术迭代，导致识别、鉴别、拦截难度直线递升，用户在未依靠网络安全工具的情况下，仅依靠社会经验、安全常识，已不具备鉴别的能力。从 2021 年整体的黑产攻防手法看，部分黑产已完成自有化生态环境建设及闭环，外界无法感知也无法进入。目前电信网站诈骗治理，已从全民识诈转变成黑产技术反制 + 全民反诈知识能力提升，故从技术层面对诈骗黑产进行趋势预测。

一、诈骗引流产业逐渐脱离境内渠道商而采用境外渠道商

随着“断卡”行动深入推进，电信网络诈骗团伙获取“两卡”的寄递贩卖通道受阻，诈骗窝点用于作案的“两卡”严重不足，大量涉案资金被冻结，大量手机卡被查封，境内电话、短信引流渠道遭切断，黑产开始向境外引流产业转移，使用境外号码，拨打诈骗电话，发送诈骗短信。

二、诈骗手法从恶意行为转向欺诈内容

移动互联网发展早期，手机权限机制、应用商店市场不完善，网民在互联网公开渠道下载应用时，往往遭受虚假、仿冒、恶意应用的滋扰。此些应用通过私发、回复短信的方式，代扣用户手机话费或窃取用户手机内所存储的个人信息进行贩卖。随着安卓版本的升级、手机权限的完善、应用商店审核机制加强，网民安全意思的提高，一方面恶意应用很难上架到正规的应用商店中，另一仿冒即使从第三方下载应用，安装时也会遭受到手机权限和杀毒软件双重阻挡。在此种情况下，各类恶意、涉诈应用开始降低应用索要手机权限的比重，甚至不索要手机权限，转而通过内容引导的方式，直接要求或诱骗受害人转钱，由于没有明显的行为执行动作，且内容内置在 APP 内，杀毒软件查杀难度提高。

三、诈骗信息反识别黑产将逐渐依托于互联网巨头商业化技术提升自身能力

随着反诈治理力度的加强，执法机关、网络安全企业合力共治涉诈产业，涉诈使用的钓鱼网址、恶意应用遭到阻断和封堵，存活周期缩短，黑产逐渐批量化生成钓鱼网址、恶意应用，并采用一案一用的方式躲避打击。

由于第三方商业化产品已具备完善的备案信息和防护能力，黑产逐渐利用第三方商业化产品，搭建钓鱼网址、恶意应用，如使用第三方在线客服、第三方聊天 SDK 搭建引流交流工具，提升了识别和反追溯的成本。

四、同类诈骗窝点抱团数量增加、同一窝点业务多元化

随着黑产上游供应商技术实力的成熟，下游诈骗窝点不再绝对化强调技术自控，而是采用外采的方式与其他同类诈骗窝点共用采买同一个家供应商的不同产品或相同产品，例如博彩行业逐渐使用包网平台提供的一站式博彩平台，裸聊敲诈窝点使用某工作室开发的通讯录窃取程序。而在对窝点研判的过程中，也发现同

一个窝点，实施不同诈骗场景的现象，例如裸聊敲诈窝点，也同时实施杀猪盘诈骗。

第二章、防范互联网平台及技术被黑灰产利用的应对措施

互联网行业在不断的发展，从 PC 互联网时代到移动互联网时代。黑灰产业也在不断的发展，从 PC 互联网时代“单兵”作战，到移动互联网时代“集团化”作战。随着黑灰产行业成长的“集团”化，人员分工的“链接”化，攻防对抗将是互联网行业与黑灰产“企业”不断厮杀成长的一场持久战。面对黑灰产的厮杀该如何应对？

一、平台审核机制规范化，加大二次校验力度

诈骗事件多发，究其原因，一方面是由于黑灰产资源售卖渠道多、开源程序多、制作教程多，搭建成本低、搭建难度低。通过搜索引擎、电商平台等渠道可以找到众多的源码。此些源码中，甚至存在一些法律禁止或打“擦边球”的项目，如博彩平台源码。作为渠道入口的平台，需要对此些违规的产品进行过滤，降低其在搜索结果中的权重，降低其造成的影响。

一方面是由于第三方技术平台对于其服务的使用者，没有进行完善的资格审核和二次校验。如使用第三方客服平台的注册人为某科技有限公司，但实际使用此第三方在线客服服务者是博彩平台。平台在前期校验购买服务的资格后，仍需要对使用者进行监督，防止平台被利用。

二、关注黑灰产动向，针对黑灰产手法，通过多种方式实时调整识别拦截手段

黑灰产在技术、话术等多方面，不断完善其自身的诈骗手法，防止在实施诈骗的过程中被识别。如诈骗团伙在使用未含备案信息的域名被安全厂商识别出诈骗特征后，转而开始利用含有备案信息的域名来躲避安全厂商对于欺诈类域名的识别，在防洪域名仍被拦截后，使用聊天软件 SDK 搭建含钓鱼网址的自有聊天软件，再引导受害人使用该软件访问钓鱼网址，完成诈骗生态闭环，双方呈现出动态博弈的特征。

面对此种现象，治理不能仅仅“盯着”实施诈骗的样本本身，进行事后拦截，需要执法机关、网络安全场景、技术开发企业共同探讨治理对策，及时发现开发者、使用者进行事前打击、阻断。

参考文献

[1] 公安部 . 打击电诈这一年：破获案件 37 万余起 发案数持续下降 [EB/OL].
https://app.mps.gov.cn/gdnps/pc/content.jsp?id=8294713，2021/12/31

[2] 中国人大网 . 数据安全法：护航数据安全 助力数字经济发展 [EB/OL]
http://www.npc.gov.cn/npc/c36748/202106/5bb18ae096d540d286df57c5639f035d.shtml，2021/06/10

[3] 中国人大网 . 表决通过!个人信息安全有了专门法律保护 [EB/OL].
http://www.npc.gov.cn/npc/c30834/202108/52678c929bca4012a5b24c86811ef4ce.shtml，2021/08/23

[4] 新华网 . 反电信网络诈骗法（草案）公布并公开征求意见 [EB/OL].
http://www.xinhuanet.com/info/20211027/caf4d7df78fa4f4ea2306443652df8f6/c.html，2021/10/27

[5] 公安部 . 打击整治非法开办贩卖电话卡银行卡犯罪“断卡”行动成效显著 [EB/OL].
https://www.mps.gov.cn/n2255079/n4876594/n5104076/n5104077/c8161838/content.html，2021/10/11

[6] 公安部 .“断流”专案行动打掉非法出境团伙 9419 个 [EB/OL].
https://www.mps.gov.cn/n2255079/n6865805/n7355741/n7355786/c8185470/content.html，2021/10/27

[7] 央视网 . 公安部推出国家反诈中心 APP 注册用户超 6500 万 构筑防诈反诈的“防火墙”[EB/OL].
https://news.cctv.com/2021/06/17/ARTIlINjDKeOIDDxI8jhGSSZ210617.shtml?spm=zm1033-001.0.0.1.fxXw5C&file=ARTIlINjDKeOIDDxI8jhGSSZ210617.shtml，2021/06/17

[8] 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

[9] 中国网财经 . 警企联合反诈!北京反诈中心联合 360 手机卫士推出“反诈中心”[EB/OL].
http://tech.china.com.cn/roll/20211109/382392.shtml，2021/11/09

附录

一、2021年手机诈骗概况

1. 报案数量与类型

2021 年全年，360 手机先赔共接到手机诈骗举报 2336 起。其中有效诈骗申请 1205 起，涉案总金额高达 2549.2 万元，人均损失 21156 元。在所有有效申请中，交友占比最高为 25.8%；其次是虚假兼职（24.5%）和金融理财（15.6%）等。从涉案总金额来看，虚假兼职类诈骗总金额最高，达 819.2 万元，占比 32.1%；其次是交友诈骗，涉案总金额 786.4 万元，占比 30.8%；金融理财排第三，涉案总金额为 486.3 万元，占比 19.1%。下图为 2021 年手机诈骗类型的举报类型与涉案金额分布情况：

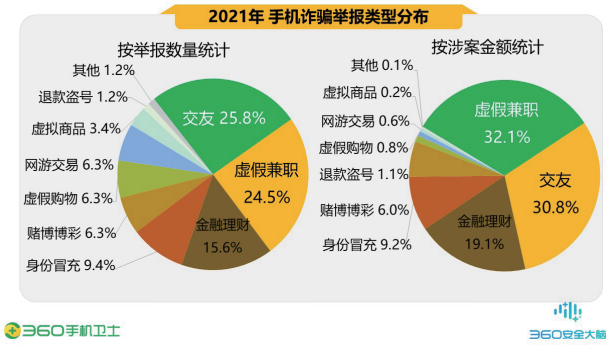


图 24　2021年手机诈骗举报类型分布

2. 受害者性别与年龄

2021 年全年，从举报用户的性别差异来看，男性受害者占 62.4%，女性占 37.6%，男性受害者占比高于女性。从人均损失来看，男性为 19727 元，女性为 23527 元，女性人均损失高于男性。下图为 2021 年手机诈骗受害者性别差异：

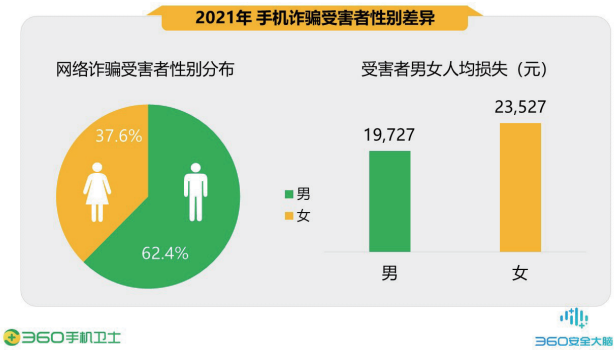


图 25　2021年手机诈骗受害者性别差异

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 38.8%，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 28.1%；80 后占比为 24.6%；70 后占比为 6.5%、60 后占比为 1.4% 等。下图为 2021 年手机诈骗受害者年龄段分布：

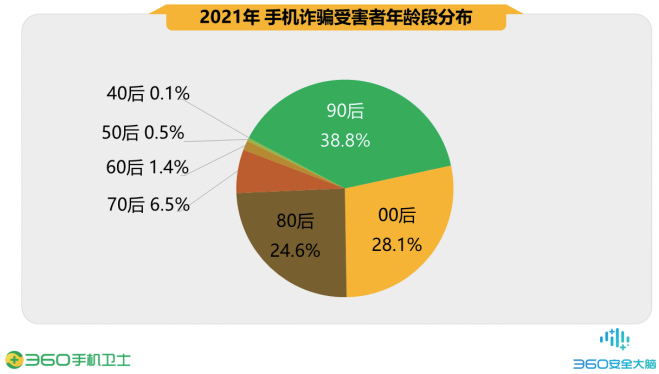


图 26　2021年手机诈骗受害者年龄段分布

从被骗网民的年龄段及人均损失来看，2021 年全年，90 后与 80 后为诈骗高发人群。

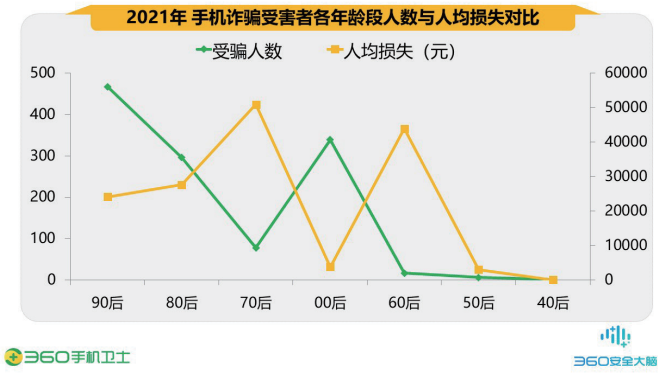


图 27　2021年手机诈骗受害者各年龄段人数与人均损失对比

3. 受害者地域分布

2021 年全年，从各地区手机诈骗的举报情况来看，山东（8.7%）、广东（7.8%）、河南（6.0%）、四川（5.7%）、河北（5.5%）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 33.7%。下图给出了 2021 年手机诈骗举报数量最多的 10 个省份：

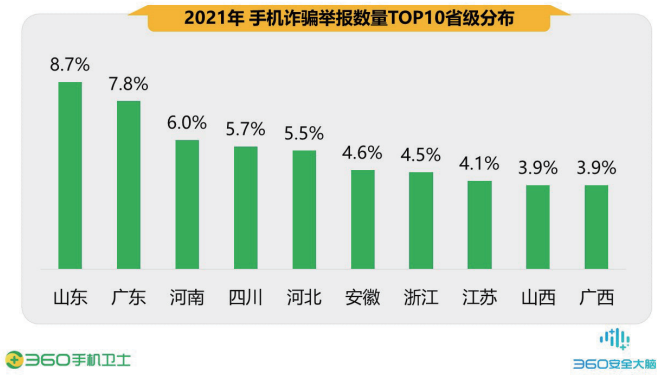


图 28　2021年 手机诈骗举报数量TOP10省级分布

从各城市手机诈骗的举报情况来看，北京（2.7%）、广州（1.6%）、成都（1.3%）、深圳（1.3%）、西安（1.2%）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 8.1%。下图给出了 2021 年手机诈骗举报数量最多的 10 个城市：

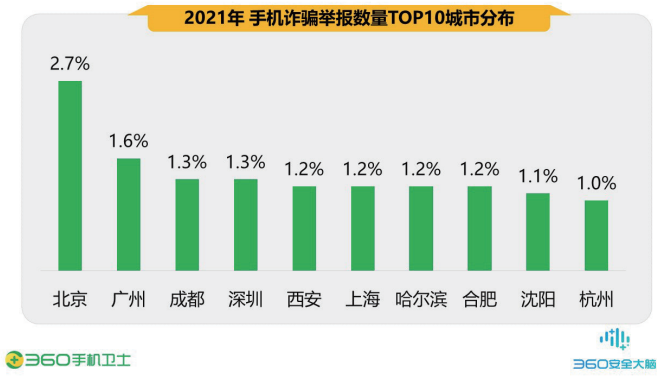


图 29　手机诈骗举报数量TOP10城市分布

二、恶意程序

1. 恶意程序新增样本量与类型分布

2021 年全年，360 安全大脑共截获移动端新增恶意程序样本约 943.1 万个，同比 2020 年（454.6 万个）增长了 107.5%，平均每天截获新增手机恶意程序样本约 2.6 万个。下图给出了 2013 年 -2021 年移动端新增恶意程序样本量统计：

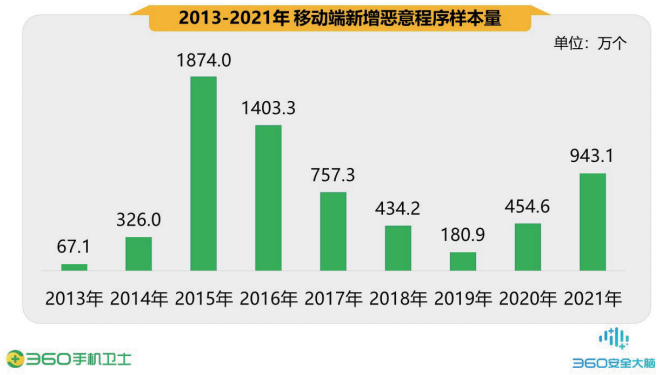


图 30　2013-2021年 移动端新增恶意程序样本量

2021 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：

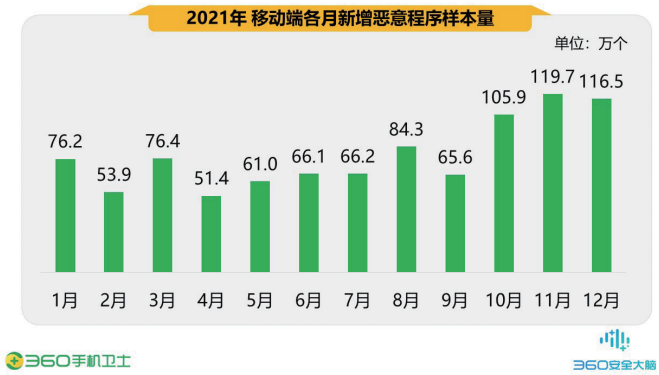


图 31　2021年 移动端各月新增恶意程序样本量

2021 年全年，移动端新增恶意程序类型主要为资费消耗，占比 95.3%；其次为隐私窃取（4.1%）、流氓行为（0.5%）与远程控制（0.1%）。下图为 2021 年移动端新增恶意程序类型分布：

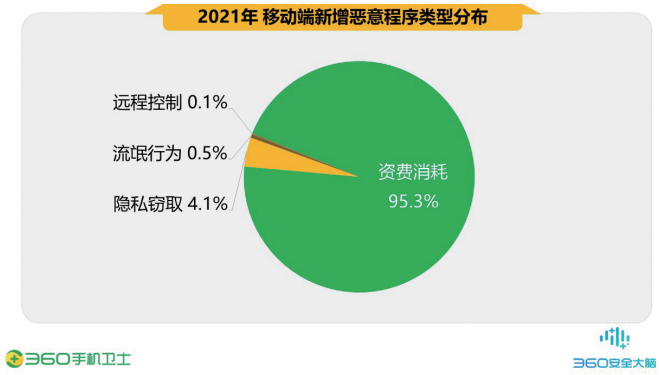


图 32　2021年 移动端新增恶意程序类型分布

2. 恶意程序拦截量

2021 年全年，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 82.4 亿次，平均每天拦截手机恶意程序攻击约 2257.8 万次。下图为 2021 年移动端各月恶意程序拦截量统计：

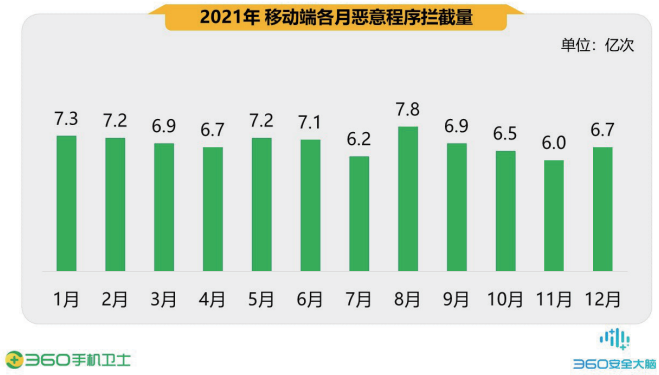


图 33　2021年 移动端各月恶意程序拦截量

3. 恶意程序拦截量地域分布

2021 年全年，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 10.1%；其次为山东（7.7%）、江苏（7.2%）、河南（7.1%）、四川（5.4%），此外浙江、河北、安徽、湖南、云南的恶意程序拦截量也排在前列。

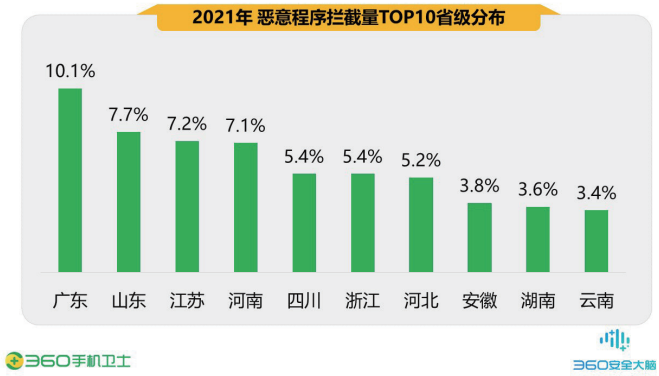


图 34　2021年 恶意程序拦截量TOP10省级分布

从城市分布来看，遭受手机恶意程序攻击最多的城市为上海市，占全国拦截量的2.6%；其次为广州（2.2%）、成都（2.0%）、重庆（2.0%）、北京（2.0%），此外深圳、杭州、郑州、苏州、天津的恶意程序拦截量也排在前列。

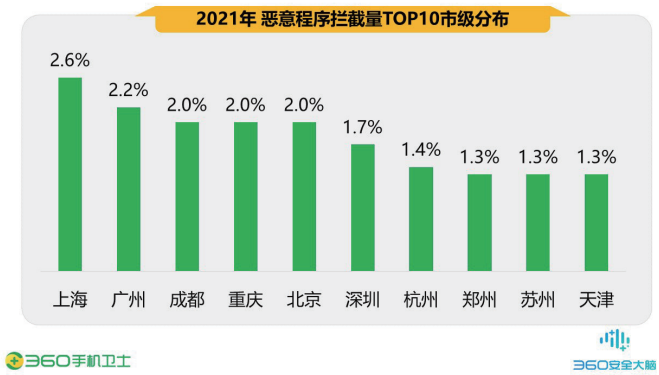


图 35　2021年 恶意程序拦截量TOP10市级分布

三、钓鱼网站

1. 移动端钓鱼网站拦截占比

2021 年全年，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 933.4 亿次，同比 2020 年（1006.4 亿次）下降了 7.3%。其中，PC 端拦截量约为 927.7 亿次，占总拦截量的 99.4%，平均每日拦截量约 2.5 亿次；移动端拦截量约为 5.6 亿次，占总拦截量的 0.6%，平均每日拦截量约 154.2 万次。下图为 2021 年钓鱼网站拦截占比分布：

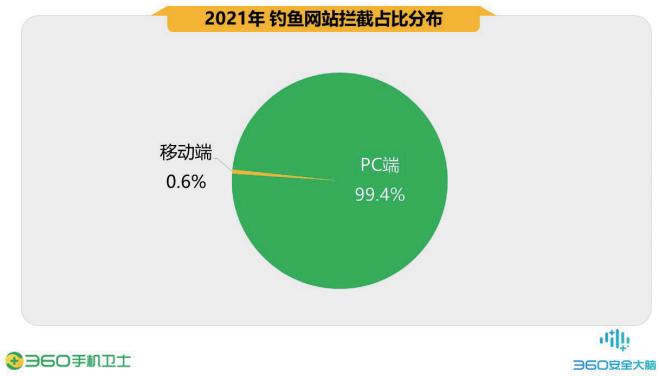


图 36　2021年 钓鱼网站拦截占比分布

2. 移动端钓鱼网站各月拦截量分布

2021 年全年，360 安全大脑在移动端拦截钓鱼网站攻击约为 5.6 亿次，下图为 2021 年钓鱼网站各月拦截量分布：

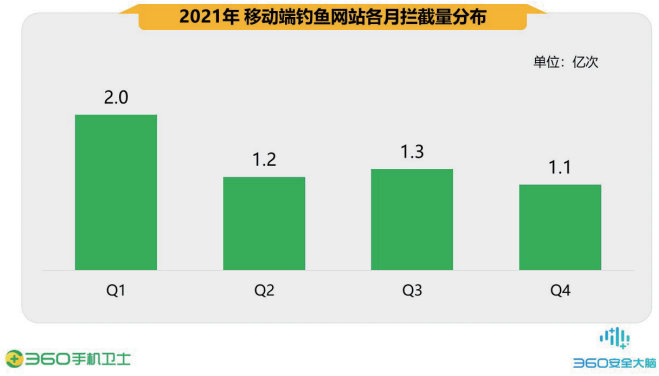


图 37　2021年 移动端钓鱼网站各月拦截量分布

3. 移动端钓鱼网站类型分布

2021 年全年，移动端拦截钓鱼网站类型主要为色情，占比高达 56.4%；其次为境外彩票（34.4%）、赌博（6.4%）、虚假购物（1.9%）、金融证券（0.7%）与其他（0.2%）。下图为 2021 年移动端拦截钓鱼网站类型分布:

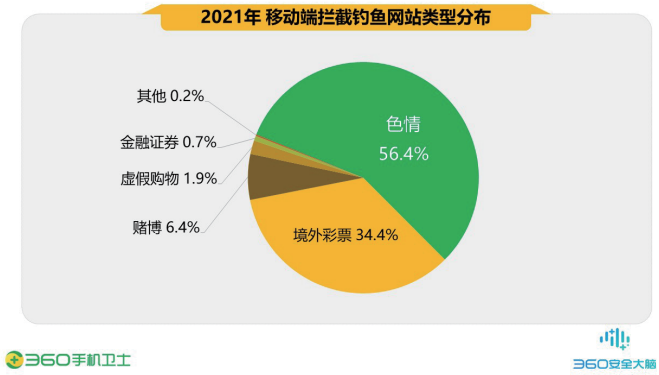


图 38　2021年 移动端拦截钓鱼网站类型分布

4. 移动端钓鱼网站新增量

2021 年全年，360 安全大脑共截获各类新增钓鱼网站 1.6 亿个，同比 2020 年（1.1 亿个）上升了 39.5%，平均每天新增 42.9 万个。

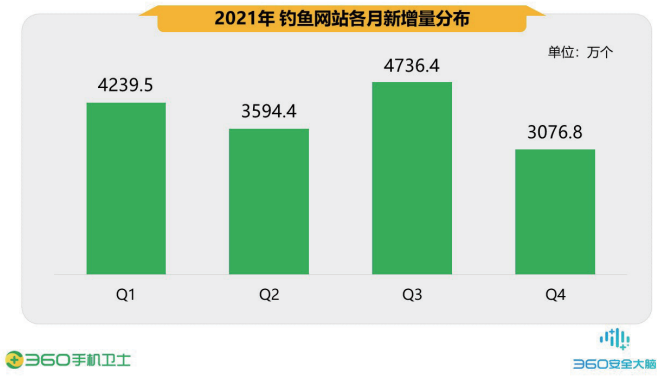


图 39　2021年 钓鱼网站各月新增量分布

在钓鱼网站新增类型中，色情类占据首位，占比 48.4%；其次为赌博类，占比 43.3%。

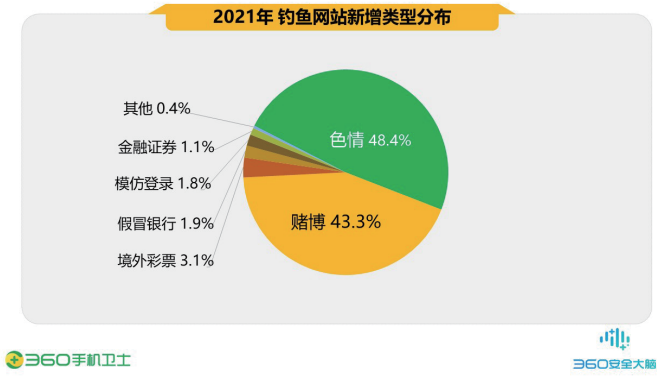


图 40　2021年 钓鱼网站新增类型分布

5. 移动端钓鱼网站拦截量地域分布

2021 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 23.0%；其次为福建（7.4%）、广西（7.0%）、山东（5.4%）、浙江（4.8%），此外江苏、河南、湖南、河北、四川的钓鱼网站拦截量也排在前列。

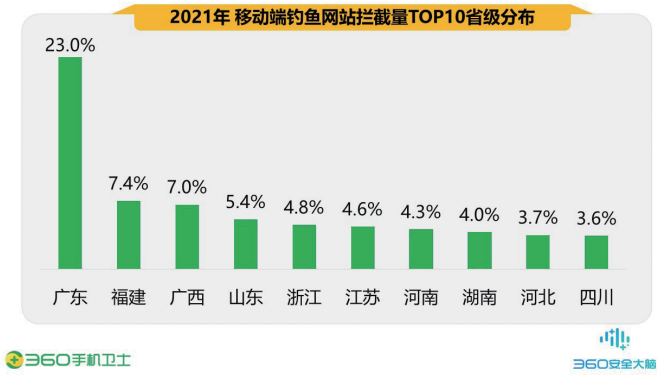


图 41　2021年 移动端钓鱼网站拦截量TOP10省级分布

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 4.9%；其次为深圳（3.2%）、北京（2.9%）、上海（2.5%）、东莞（2.5%），此外泉州、佛山、南宁、重庆、成都的钓鱼网站拦截量也排在前列。

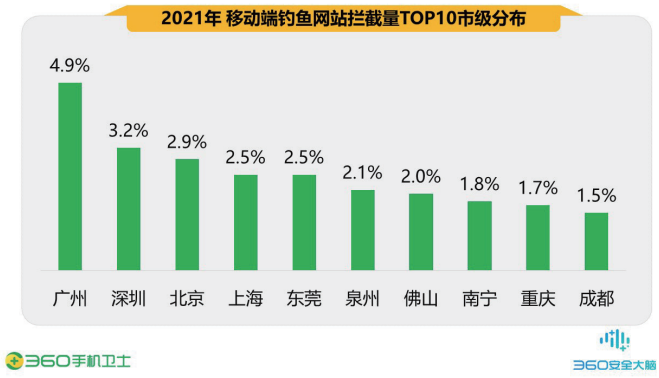


图 42　2021年 移动端钓鱼网站拦截量TOP10市级分布

四、骚扰电话

1. 骚扰电话标记拦截量

2021 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 228.0 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。环比 2020 年（224.3 亿次）上涨了 1.7%。下图给出了 2014 年 -2021 年用户标记骚扰电话拦截号码次数统计：

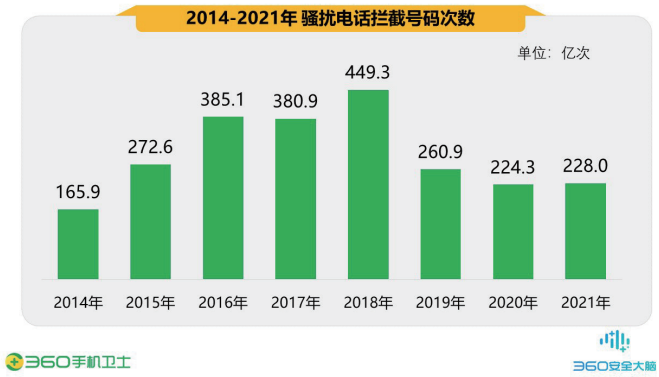


图 43　2014-2021年 骚扰电话拦截号码次数

下图为 2021 年骚扰电话各月拦截号码次数分布：

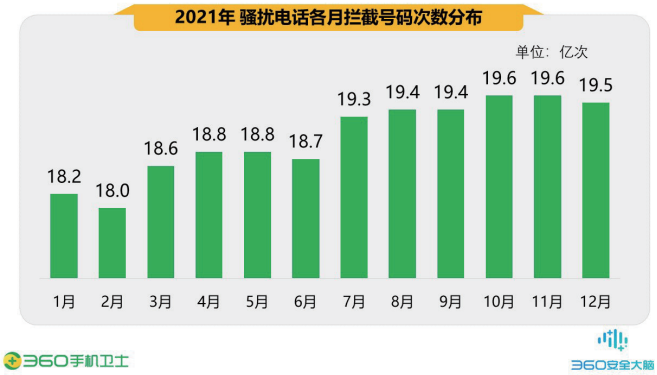


图 44　2021年 骚扰电话各月拦截号码次数分布

分析 2021 年 360 手机卫士识别和拦截骚扰电话趋势可见，骚扰电话呼入量受到节假日、电商节等特殊时段影响，波动性较为明显。下图为 2021 年识别与拦截骚扰电话趋势统计：

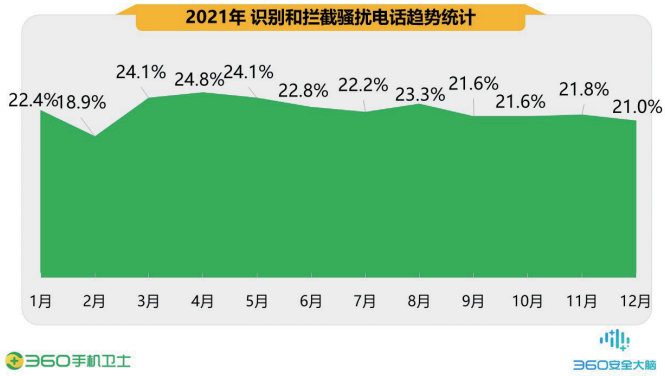


图 45　2021年 识别和拦截骚扰电话趋势统计

2. 骚扰电话拦截类型分布

2021 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 84.0% 的比例位高居首位；其次为广告推销（11.0%）、房产中介（4.0%）、保险理财（0.4%）、疑似欺诈（0.3%）、招聘猎头（0.2%）与响一声（0.1%）。下图为 2021 年骚扰电话拦截类型分布：

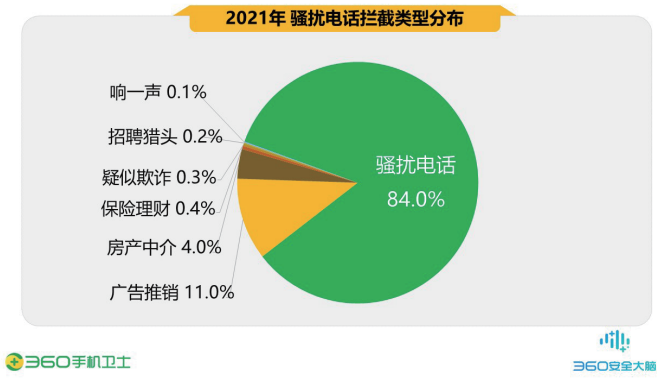


图 46　2021年 骚扰电话拦截类型分布

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 39.5%；其次为运营商为中国移动的个人手机号（23.7%）、运营商为中国联通的个人手机号（22.0%）、运营商为中国电信的个人手机号（9.7%）、虚拟运营商（4.5%）与 95/96 开头号段（0.5%）。下图为 2021 年骚扰电话拦截号码号源分布：

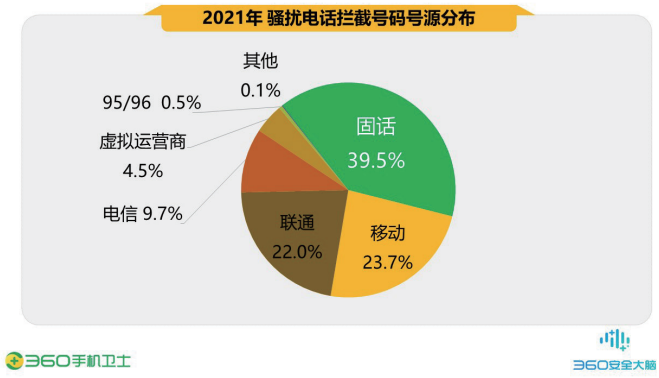


图 47　2021年 骚扰电话拦截号码号源分布

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 76.5%；虚拟运营商也是骚扰电话类占据首位，占比 66.4%。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。

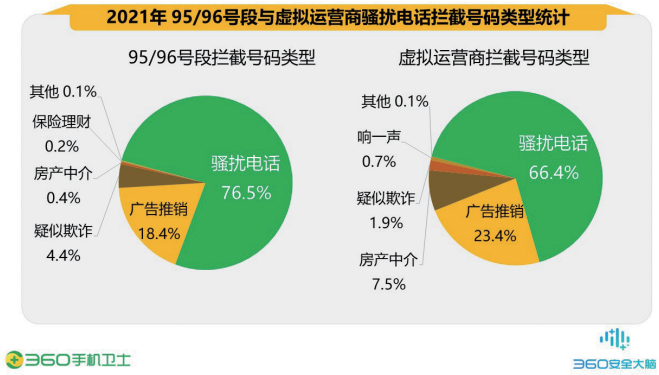


图 48　2021年 95/96号段与虚拟运营商骚扰电话拦截号码类型统计

4. 骚扰电话归属地分布

2021 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 13.1%；其次是山东（7.7%）、江苏（6.1%）、河南（5.6%）、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。

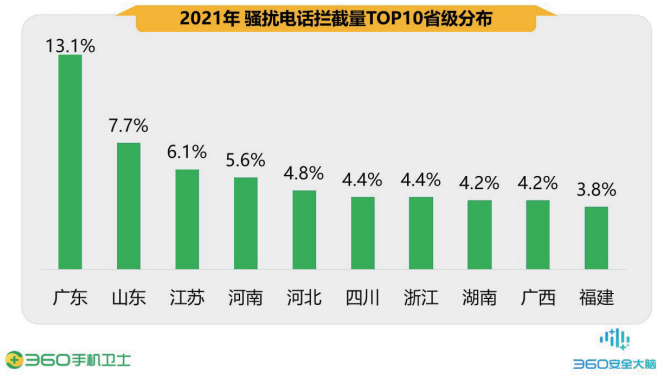


图 49　2021年 骚扰电话拦截量TOP10省级分布

从城市分布来看，上海市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 3.6%；其次是广州（3.6%）、北京（3.5%）、深圳（2.2%）、成都（2.0%），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。

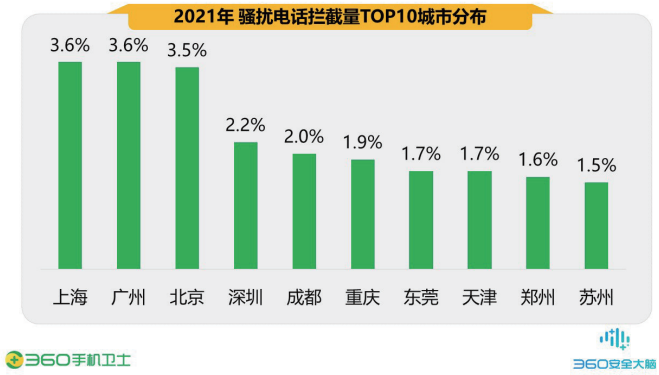


图 50　2021年 骚扰电话拦截量TOP10城市分布

五、垃圾短信

1. 垃圾短信拦截量

2021 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 167.2 亿条，同比 2020 年（177.3 亿条）下降了 5.7%，平均每日拦截垃圾短信约 4581.1 万条。

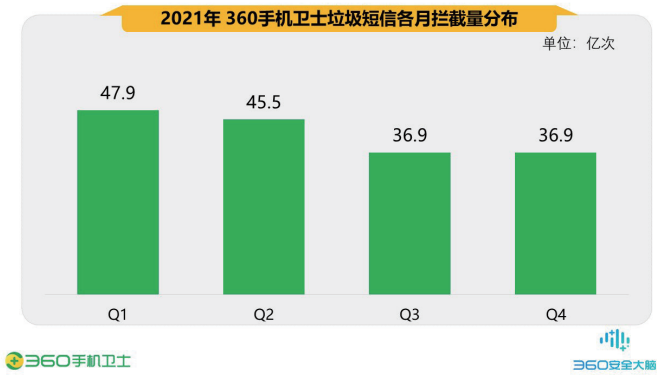


图 51　2021年 360手机卫士垃圾短信各月拦截量分布

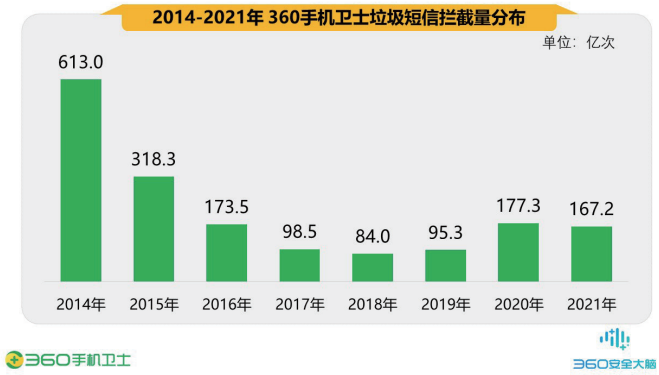


图 52　2014-2021年 360手机卫士垃圾短信拦截量分布

2. 垃圾短信类型分析

2021 年全年，垃圾短信的类型分布中广告推销短信最多，占比为 94.0%；诈骗短信占比 5.9%；违法短信占比 0.1%。

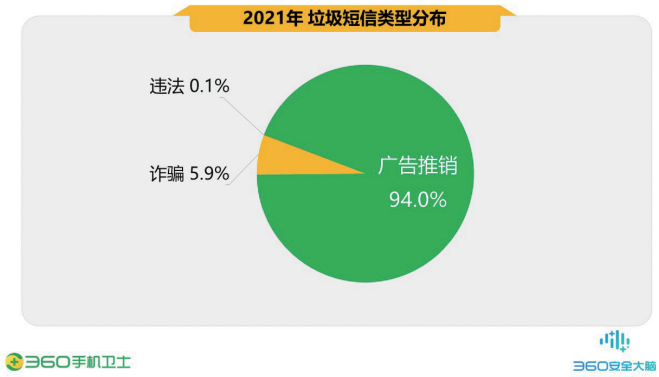


图 53　2021年 垃圾短信类型分布

从诈骗短信拦截类型来看，赌博诈骗以 48.4% 的比例位居首位；其次为诈骗短信（43.3%）、疑似伪装诈骗(3.1%)、股票诈骗(1.6%)、冒充银行(1.6%)、兼职诈骗(1.1%)与短信内容中预留联系方式涉嫌诈骗(0.6%)等。下图为 2021 年诈骗短信子类型分布：

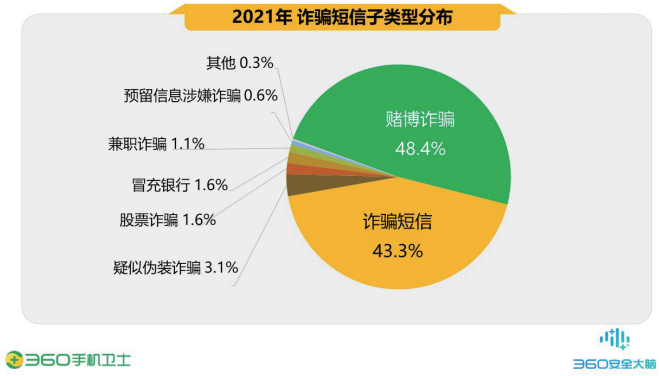


图 54　2021年 诈骗短信子类型分布

从违法短信拦截类型来看，违法金融信贷短信以 63.1% 的比例位居首位；其次为其他违法短信（29.8%）、售卖信息（3.2%）、疑似伪基站发送（2.9%）、恶意催债（0.5%）与色情短信（0.5%）。下图为 2021 年违法短信子类型分布：

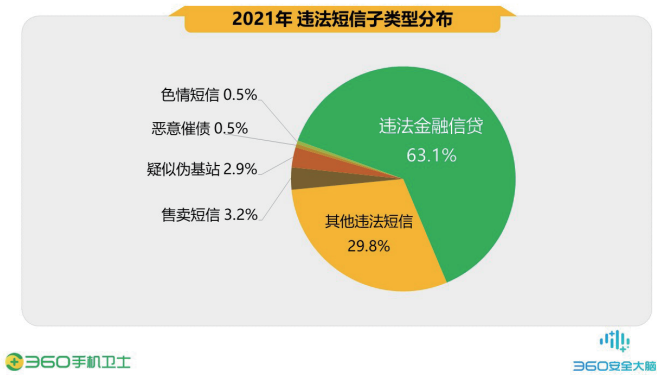


图 55　2021年 违法短信子类型分布

3. 垃圾短信发送者运营商号源分布

2021 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 96.3%；利用其他号段传播垃圾短信占比约 3.7%。下图为 2021 年短信平台发送垃圾短信占比分布：

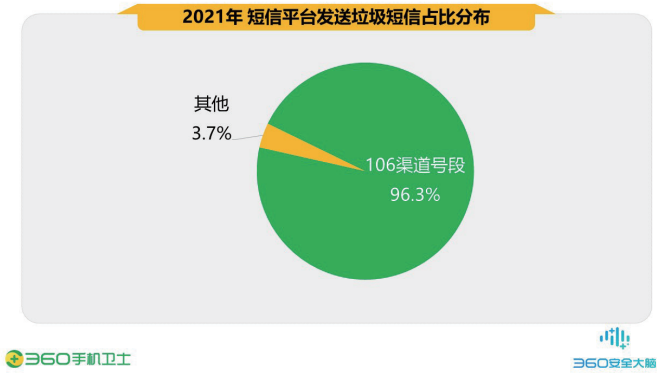


图 56　2021年 短信平台发送垃圾短信占比分布

2021 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 95/96 号段发送垃圾短信的最多，占比 32.7%；其次是运营商为中国移动的个人手机号（21.9%）、虚拟运营商（12.3%）、运营商为中国电信的个人手机号（11.5%）、运营商为中国联通的个人手机号（10.5%）、固话（7.0%）与 14 物联网卡（3.3%）等。

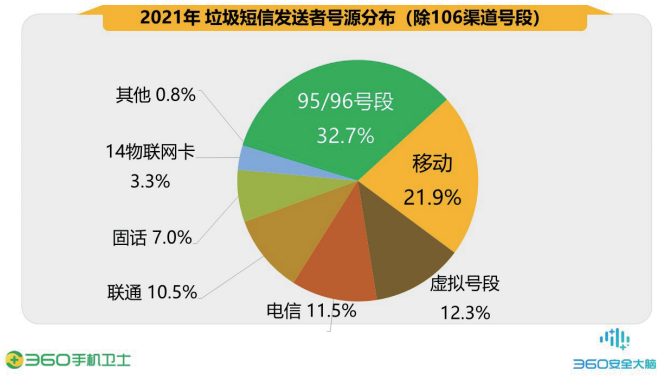


图 57　2021年 垃圾短信发送者号源分布（除106渠道号段）

4. 垃圾短信拦截量地域分析

2021 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 18.4%；其次是山东（7.4%）、江苏（6.8%）、北京（6.7%）、浙江（5.8%），此外河南、河北、四川、上海、湖南的垃圾短信拦截量也排在前列。

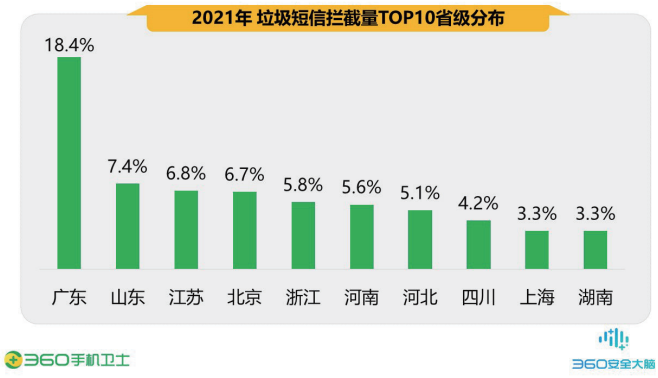


图 58　2021年 垃圾短信拦截量TOP10省级分布

从城市分布来看，广州市用户收到的垃圾短信最多，占全国垃圾短信拦截量的 7.7%；其次是北京（7.6%）、深圳（4.4%）、上海（3.7%）、南京（2.8%），此外重庆、石家庄、杭州、成都、西安的垃圾短信拦截量也排在前列。

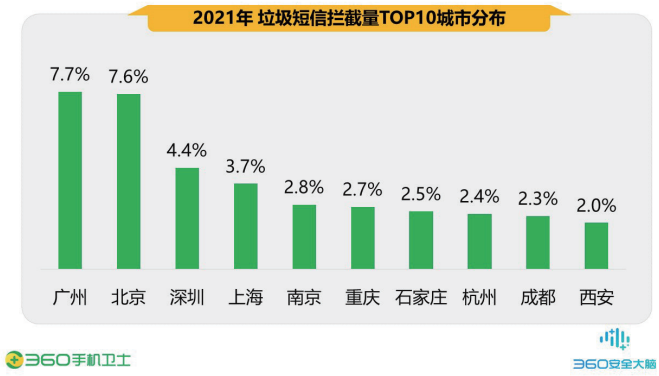


图 59　2021年 垃圾短信拦截量TOP10城市分布