2021 年第三季度

中国手机安全状况报告

2021 年 11 月 15 日

前言

随着互联网以及信息化的飞速发展，传统犯罪不断向新型互联网方向转变，而且案件多发高发、手法“不断创新”、产业链条稳定且生态化。电信网络诈骗成本低、上手快、收益高，不法分子在低风险高回报的诱惑下不断升级迭代诈骗手法，运用新技术、新手段，日益呈现出智能化、产业化、同质化等特点。

近几年，利用互联网技术衍生出的黑灰产行业正在形成规模，曾经隐蔽的角落逐渐从“暗流”走向“奔涌”。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，技术含量逐步降低，产业分工非常明确。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。

今年下半年发现，多种产业链进行了更新升级。裸聊敲诈产业在针对人群上虽然仍以安卓用户为主，但增加了对 IOS 系统的技术投入，增加了资产保护、程序免杀、手机远控等攻防技术，并提供一站式运维服务。博彩产业采用代理合营的手段，拉新返佣的方式，吸引赌客成为博彩平台代理。而黑灰产行业必备的物料-手机卡，随着“断卡行动”的持续开展，已变得异常的稀缺“珍贵”，于是利用号码魔方、防封策略提高拨打诈骗电话的成功率、降低诈骗手机号被封率的产业逐渐浮出“水面”。

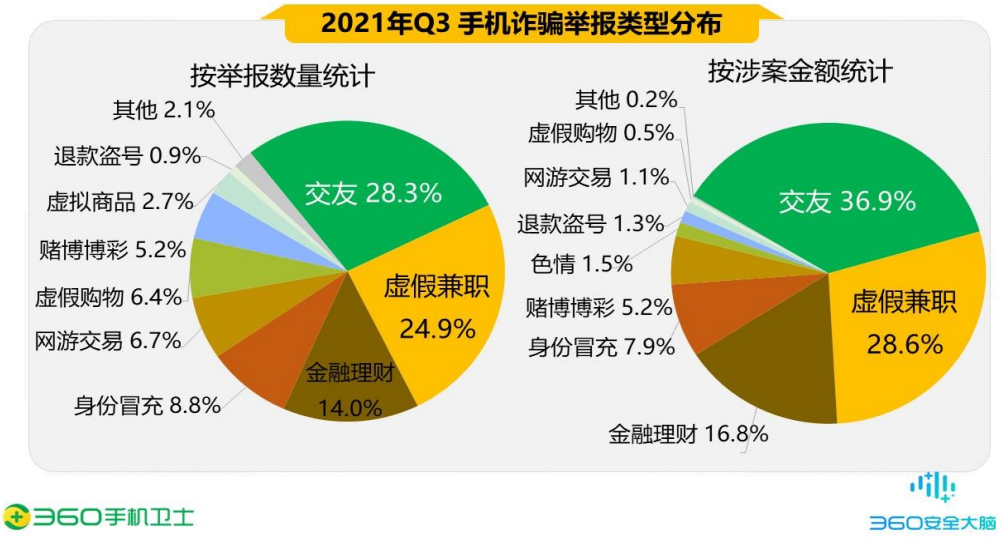
《2021 年第三季中国手机安全报告》将从黑灰产趋势、热门诈骗剧本、最新攻防手段、各维度数据入手，深度剖析黑灰产业。360 安全大脑将持续发挥自身技术优势，综合运用人工智能、大数据、云计算等技术手段有效打击涉诈产业链，维护用户移动信息安全。

目录

第一章　2021 年第三季度手机诈骗概况

一、 报案数量与类型

2021 年第三季度 360 手机先赔共接到手机诈骗举报 584 起。其中有效诈骗申请 329 起，涉案总金额 541.6 万元，人均损失 16463 元。在所有诈骗申请中，交友占比最高达 28.3%；其次是虚假兼职（24.9%）、金融理财（14.0%）、身份冒充（8.8%）、网游交易（6.7%）等。从涉案总金额来看，交友类诈骗总金额最高，达 199.7 万元，占比 36.9%；其次是虚假兼职类诈骗，涉案总金额 154.9 万元，占比 28.6%；金融理财排第三，涉案总金额为 91.1 万元，占比 16.8%。下图为 2021 年第三季度手机诈骗的举报类型与涉案金额分布情况：

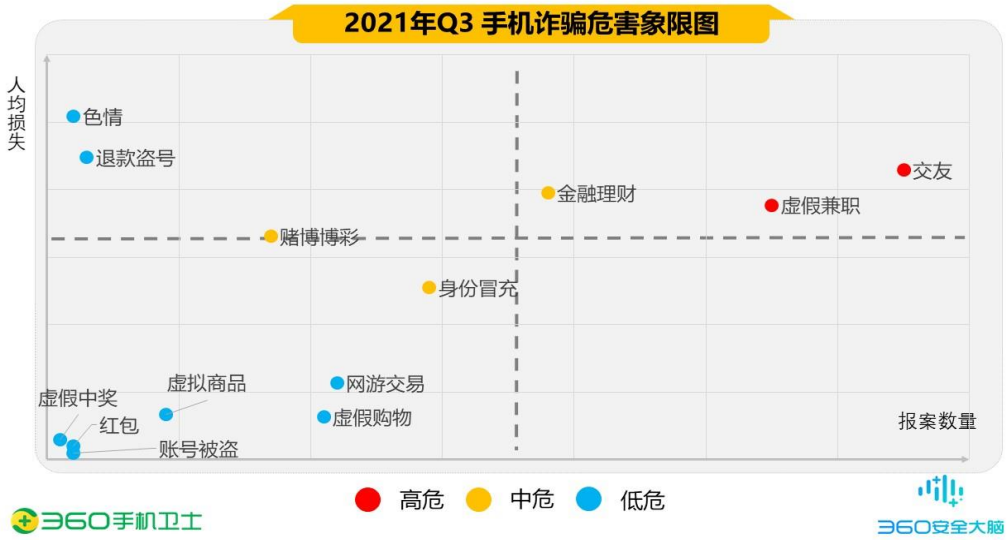


2021 年第三季度，手机诈骗中交友、虚假兼职仍属于高危诈骗类型；金融理财、身份冒充、赌博博彩属于中危诈骗类型。其中，色情类人均损失最高，约 4.0 万元；其次为退款盗号类，人均损失约为 2.3 万元，但由于受骗人数较少，依然属于低危诈骗类型。

[1] 交友类诈骗仍以裸聊遭敲诈为主，但诈骗团伙对裸聊敲诈使用的恶意 APP 进行技术迭代升级，增加了防逆向加密手段，同时具备了远控功能。一方面识别难度增加，另一个方面用户在泄露个人隐私信息的同时，可能还会被不法截获手机屏幕信息进行资金盗刷。

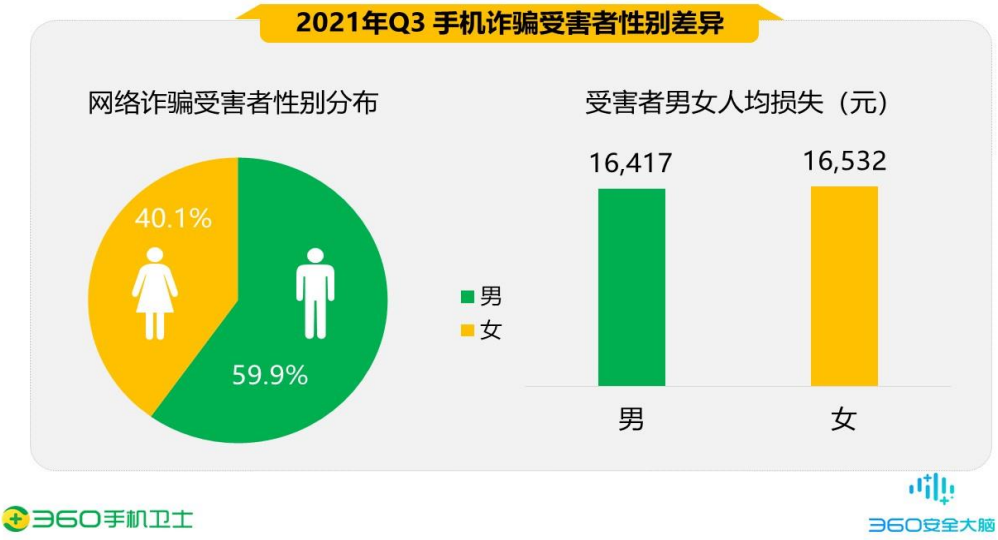
[2]第三季度发现的虚假兼职诈骗中，出现了以免费招嫖为幌子，吸引受害人完成刷单任务的诈骗手法。该手法“前瞻性”的将传统网络招嫖与博彩平台相结合，用户若想招嫖成功

或免费招嫖，需要在指定博彩平台完成相关的投注任务量。在实施诈骗的过程中，不法分子还会通过前期任务的返现的方式，诱导受害人增加投注量，从而骗取更多的充值资金。

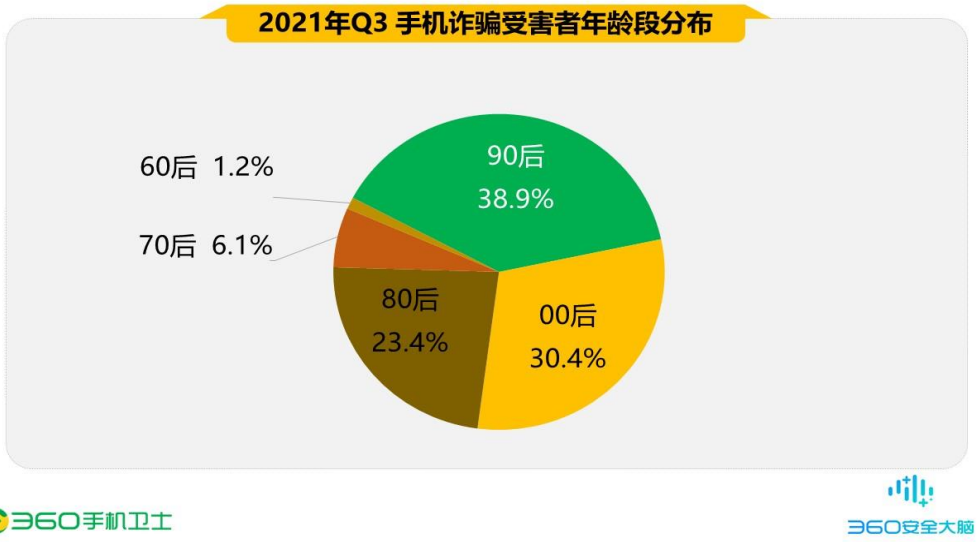


二、 受害者性别与年龄

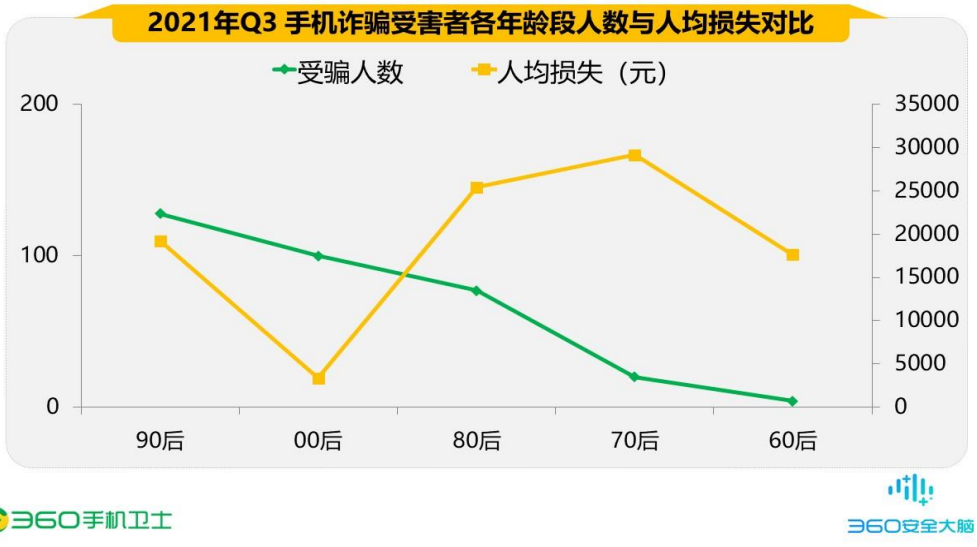
2021 年第三季度，从举报用户的性别差异来看，男性受害者占 59.9%，女性占 40.1%，男性受害者占比高于女性。从人均损失来看，男性为 16417 元，女性为 16532 元，男性人均损失低于女性。下图为 2021 年第三季度手机诈骗受害者性别差异：



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 38.9%，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 30.4%；80 后占比为 23.4%；70 后占比为 6.1%、60 后占比为 1.2%。下图为 2021 年第三季度手机诈骗受害者年龄段分布：

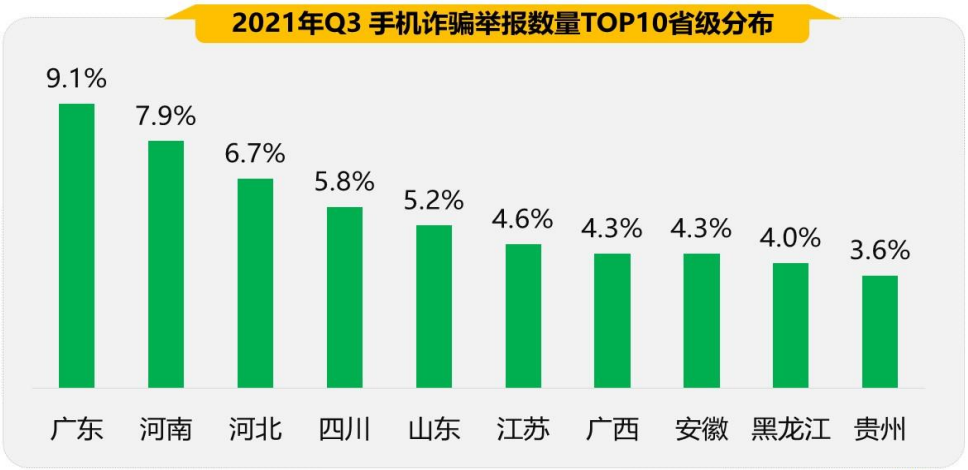


从被骗网民的年龄段及人均损失金额来看，2021 年第三季度，90 后受骗人数依然最多，但 70 后人均损失最高。本季度出现任务型网络招嫖诈骗，由于诈骗手法较新，目标用户明确，提升了 90 后的受骗数量和受骗金额。而 70 后具备了一定的财务积累，但由于其获取网络诈骗相关知识的渠道有限，难以识别钓鱼短信、网址，银行卡资金被盗刷时，损失较高。



三、 受害者地域分布

2021 年第三季度，从各地区手机诈骗的举报情况来看，广东（9.1%）、河南（7.9%）、河北（6.7%）、四川（5.8%）、山东（5.2%）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 34.7%。下图给出了 2021 年第三季度手机诈骗举报数量最多的 10 个省份：



从各城市手机诈骗的举报情况来看，北京（3.3%）、哈尔滨（2.4%）、广州（2.1%）、东莞（1.8%）、濮阳（1.8%）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 11.6%。下图给出了 2021 年第三季度手机诈骗举报数量最多的 10 个城市：

第二章　黑灰产趋势及攻防技术原理分析

一、 博彩代理产业链

1. 伪装成计算器的博彩代理应用

近期发现一款名为“计算器”的安卓应用，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，其背后代表的是博彩代理相关产业。

博彩代理指的是连接博彩平台与赌客之间的中间人，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，下图为某线上博彩平台的代理收益金额表。

2. 博彩代理平台功能分析

2.1 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、电子竞技，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。

2.2 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

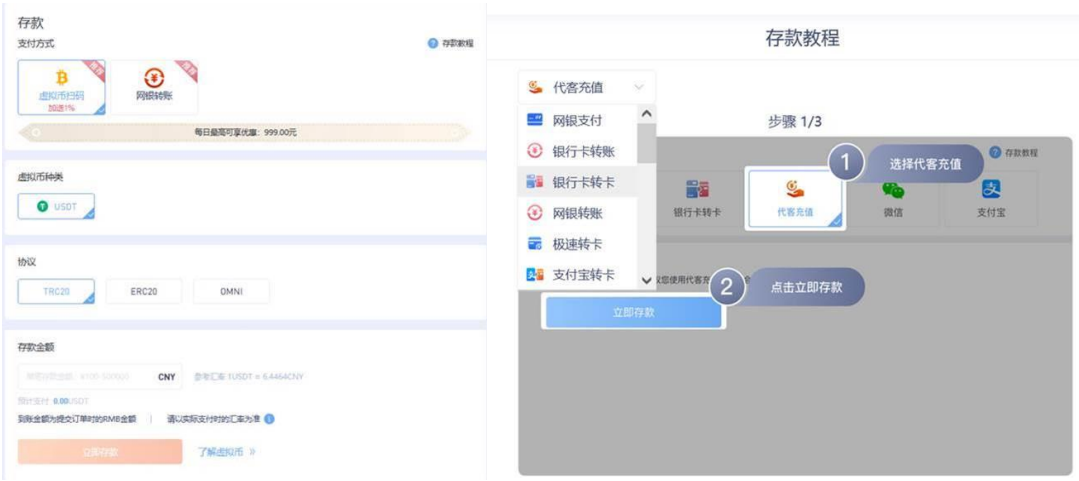
包含提款记录、代理代充、额度充值、财务报表、佣金报表、账变明细。提款记录指的是将佣金提现至自己的银行卡或虚拟货币账户；额度充值、代理代充指的是代理将资金充入代理平台，给赌客进行赌资代充值；财务报表、佣金报表、账变明细指的是代理的收益情况；推广中心，主要是提供含代理 ID 号的博彩链接（PC 端、H5 端、APP 版），若代理觉得链接太长，不方便在传播，该产业还提供防封短链接。

[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。



二、 含远控功能的第二代裸聊敲诈应用分析

1. 裸聊敲诈关联黑产攻防演变

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。

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。

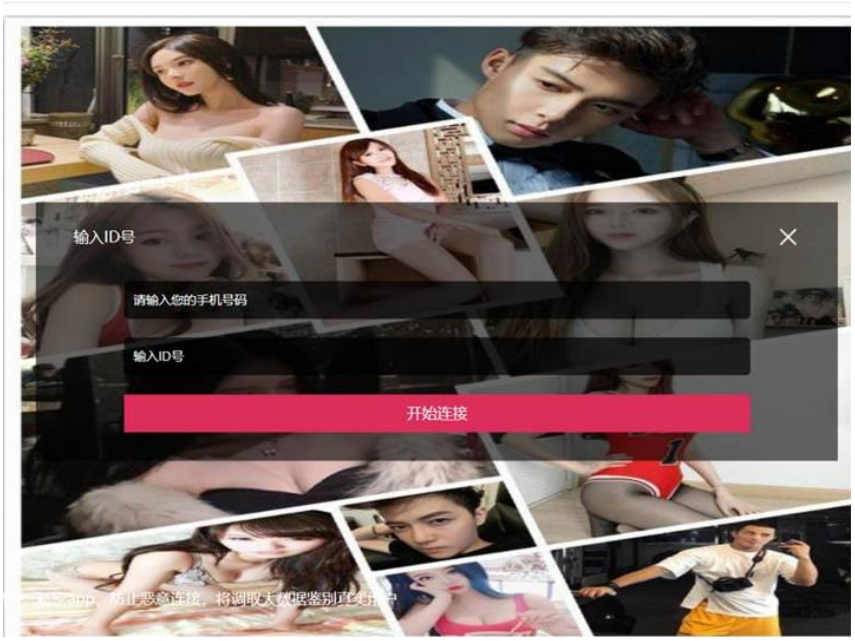
但在今年下半年，我们发现裸聊敲诈产业出现了变化，在针对人群上，仍以安卓用户为主，但增加了对 IOS 系统的技术投入。在攻防技术上，增加了资产保护、程序免杀、手机远控等技术；在关联黑灰产业链上，从分散的应用签名、分发、防封转变成支持一站式运维服务。这里从第二代裸聊敲诈 APP 分析入手，对裸聊敲诈产业进行解读。

2. 第二代裸聊敲诈应用分析

2.1 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。



2.2 静态分析

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。

2.3 裸聊敲诈功能分析

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。

三、 号码防封技术

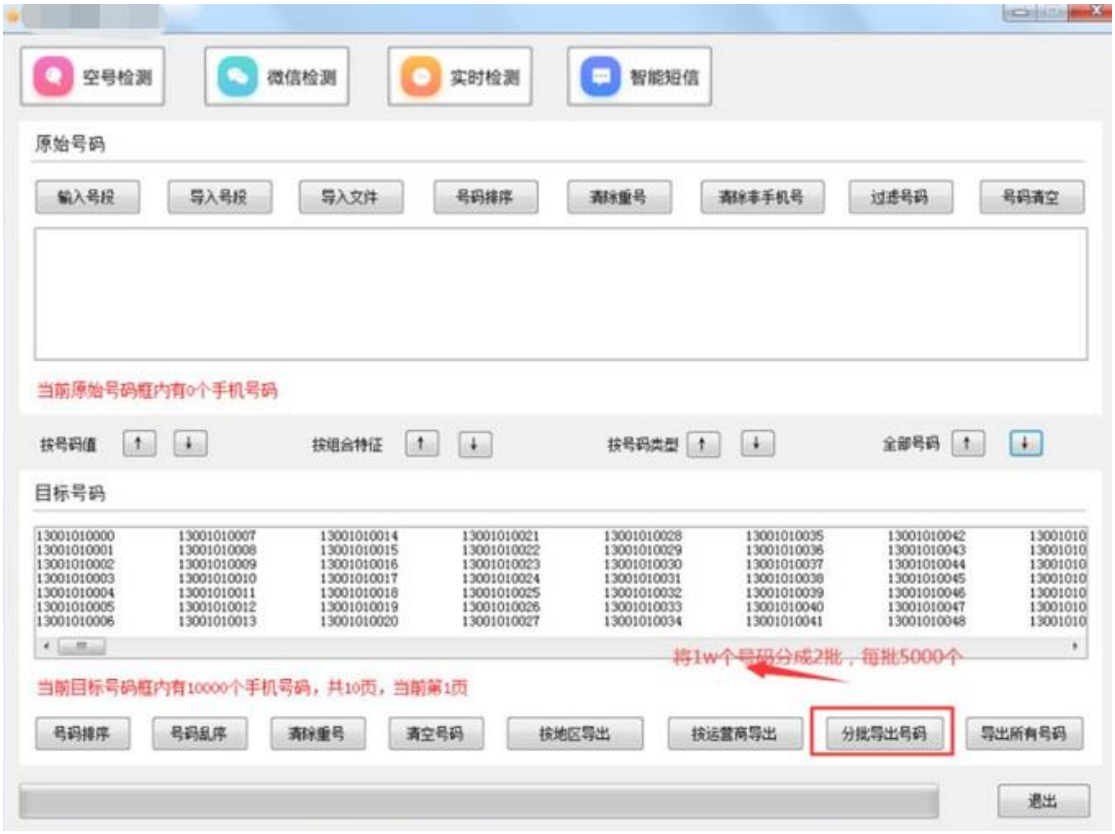
手机卡作为黑灰产行业必备的物料，随着“断卡行动”的持续开展，已变得异常的稀缺“珍贵”，于是利用号码魔方、防封策略提高拨打诈骗电话的成功率、降低诈骗手机号被封率的产业逐渐浮出“水面”。

1. 提高拨打诈骗电话的成功率的“号码魔方”

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、微信检测等功能，快速实现组合并筛选出有效号码，降低群呼号码失效率。

空号检测也称空号在线过滤、在线筛号、号码在线清洗，其原理是通过“运营商”的接口批量查询待检验的号码是否为活跃号（活跃用户）、空号（近一个月内出现过的空号和停机号）、沉默号（超过六个月未激活过的空号或近三个月平均使用流量低于 30M）、风险号（长时间关机或未开通语音服务）。微信检测主要是检测手机号码是否开通微信，开通的微信号是否为活跃号、僵尸号。

号码魔方本用于电商平台杜绝恶意注册刷单、金融平台异常号码、稳定性核实，但诈骗行业使用后，也同时提升了拨打受害人号码的精准度，提高了拨打电话的效率。下图为某号码魔方应用界面。



2. 号码防封产业技术

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，针对性的演变出了各类防封技术。

2.1 呼叫转移防封

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。

2.2 AXB 模式防封

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。

2.3 回拨电话防封

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。

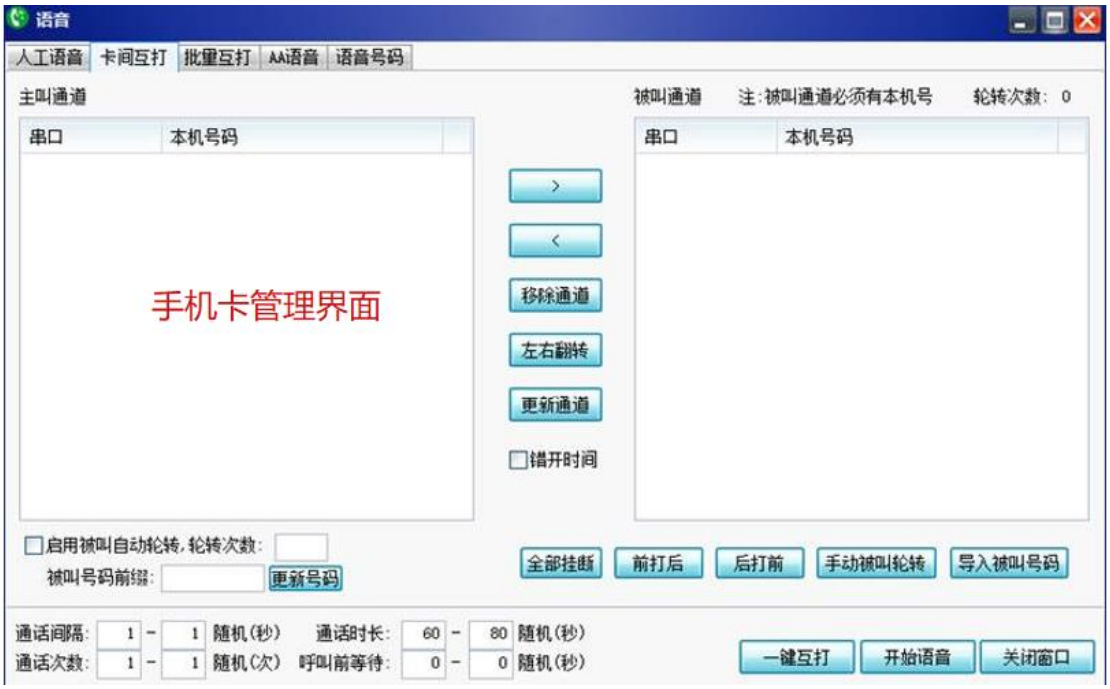
四、 接码产业链

目前主流的一些互联网产品注册、登录的校验方式都为手机号+短信验证码，接码就是使用他人手机号、短信验证码以完成账号注册、登录操作，而接码平台就是对接卡商、接码用户的中介平台。接码平台作为黑产短信验证码供应商，有着源头性和基础性的作用，故对接码产业进行剖析，力图对打击网络黑产提供对策建议。

1. 卡商掌控号码原理

卡商指的是手中掌握大量虚假实名卡、物联网卡、虚拟运营商卡的人员，其使用猫池、卡池设备，配合酷*、嘻*等软件搭建手机号码群控系统，实现手机号养号、批量外呼、短信群接发等服务。这里以酷*软件为例，其通过卡间互打、网络流量、修改串号等功能来实现手机号养号。卡间互打指的是让卡池中手机号互相拨打，从而产生呼叫行为，让运营商以为是正常使用的白号；网络流量指的是通过模拟访问自定义的网址，实现刷流量操作，从而避过“运营商”的空号检测；修改串号指的是对手机号的设备特征进行修改，从而躲避手机客户端应用的风控机制。

卡商搭建完手机号码群控系统后，安装接码平台提供接码卡商客户端软件，选择所接的接码项目，例如京*注册，将手机号、短信验证码资源实时回传至接码平台，供接码用户使用。



2. 接码出码过程

为了“便利”接码用户操作，接码平台提供了 WEB、PC、安卓客户端三种登录方式。接码用户注册、充值后，在项目列表中搜索并选择需接码的项目，选中该项目后 ，筛选所需的号码运营商（境内、境外）、归属地省、市，选择需要接码的手机号，进行接码操作。例如某接码用户想注册*菜，接码客户端的项目列表中搜索“*菜”，将出现的*菜，ID-1185 添加到到收藏

中。随后在收码界面选中已收藏的项目（（菜，ID-1185），选择运营商、号码归属地，点击提取手机号，即可看到短信内容及注册短信验证码。

由于号码有限，部分接码平台的号码已被他人在相同平台注册，此时提取的手机号无法进行注册，用户可使用专属对接功能。专属对接指的是卡商在接码平台，为接码用户提供专属的号码服务。

3. 接码产业洗钱通道

随着多方加大对黑产支付通道的打击力度，各类黑产支付接口资源萎缩，发卡平台成为了接码产业支付渠道的新宠儿。前文提到接码用户若使用接码服务，需要先充值才能使用，这个充值，就是在发卡平台购买点券，再去接码平台进行激活获得对应的服务权限；同样的流程，卡商为接码平台服务后，获得相应的点券，通过发卡平台进行提现操作，即发卡平台为接码平台提供充值、提现服务，由于发卡平台商品的自主性，很难直接将发卡平台与黑产、洗钱直接挂钩，从而逃避了监管。

第三章　热门诈骗剧本

一、 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

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。

二、 远程窃取“钱包助记词”

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。

第四章　2021 年第三季度安全数据

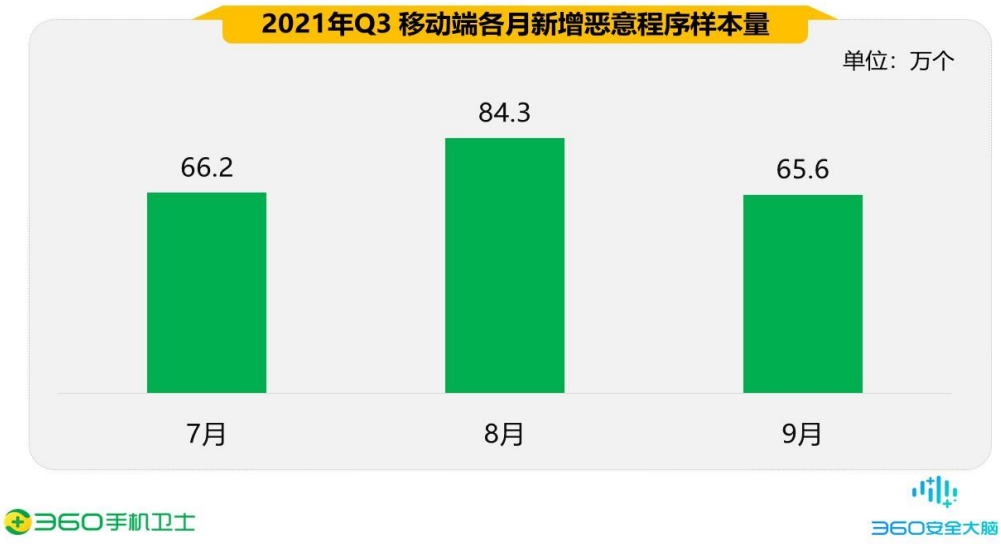
高速发展的移动信息时代，小小的移动设备已经成为民众日常生活中不可或缺的一部分，但是其在方便人们生活的同时，也给了不法分子可乘之机。不法分子“隐蔽”且不断“推陈出新”的攻击手段给人们带来了很多恶劣影响，盗取个人财产、泄露个人隐私信息。对于我们安全厂商来说，如何帮助用户预防以及应对这些攻击一直是我们工作的核心内容。

2021 年第三季度，360 安全大脑不断提升针对移动互联网恶意程序的识别收录能力，截获的移动端新增恶意程序同比有显著提升。针对复杂多样的钓鱼网站攻击，360 安全大脑始终如一的预设钓鱼网站识别规则，建立模型样本库等，对钓鱼网站进行实时拦截，有效防范网络攻击事件的发生，从而避免用户遭受重大财产损失。同时对于骚扰电话以及垃圾短信，360 安全大脑也已于云端建立了相关识别拦截规则，并优化本地算法模型，持续抵制互联网不法信息传播，维护用户移动信息安全。

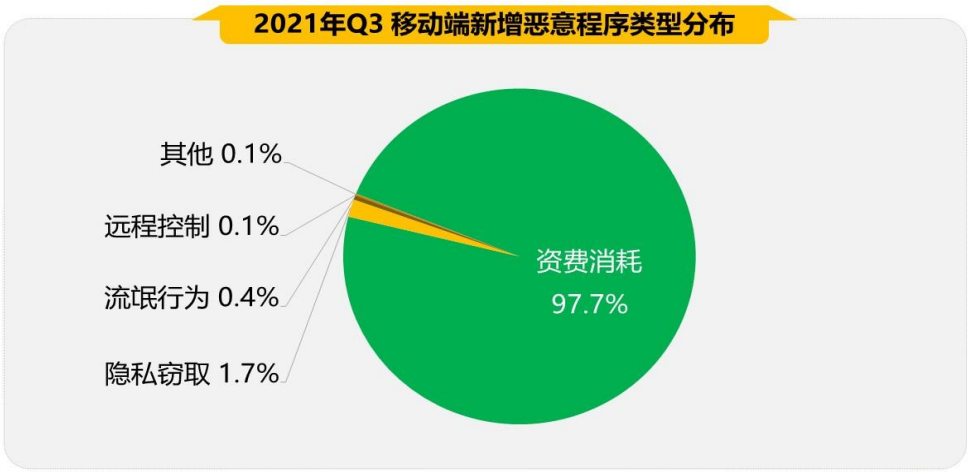
一、 恶意程序

1. 恶意程序新增样本量与类型分布

2021 年第三季度，360 安全大脑共截获移动端新增恶意程序样本约 216.1 万个，同比 2020 年第三季度（118.7 万个）上升了 82.0%，平均每天截获新增手机恶意程序样本约 2.3 万个。下图为 2021 年第三季度移动端各月新增恶意程序样本量统计：



2021 年第三季度，移动端新增恶意程序类型主要为资费消耗，占比 97.7%；其次为隐私窃取（1.7%）、流氓行为（0.4%）、远程控制（0.1%）等。下图为 2021 年第三季度移动端新增恶意程序类型分布：



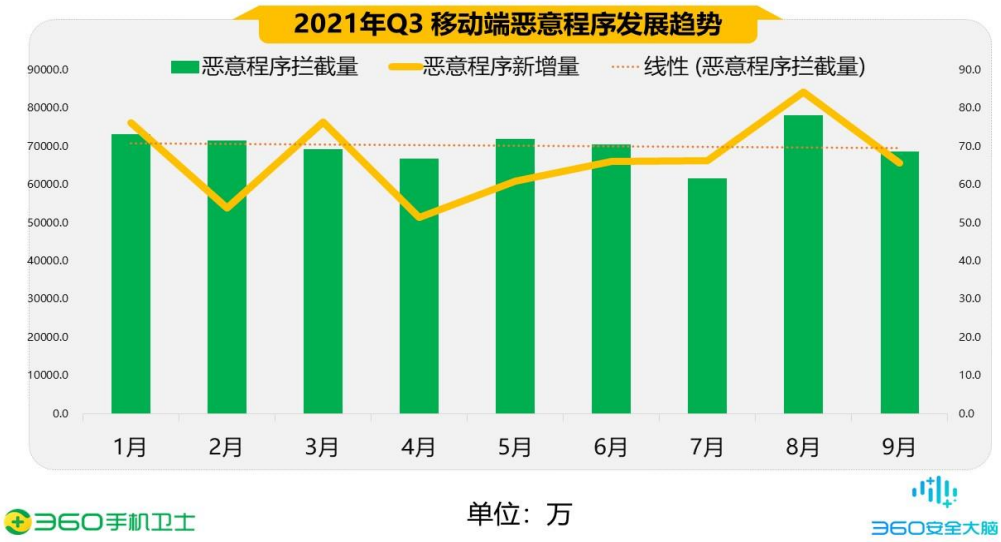
2. 恶意程序拦截量

2021 年第三季度，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 20.9 亿次，平均每天拦截手机恶意程序攻击约 2266.8 万次。下图为 2021 年第三季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 年第三季度，恶意程序新增量在 8 月出现激增峰值，当月恶意程序新增量为 84.3 万，之后 9 月又重新恢复日常情况。观察新增样本类型，主要体现在资费消耗类型。

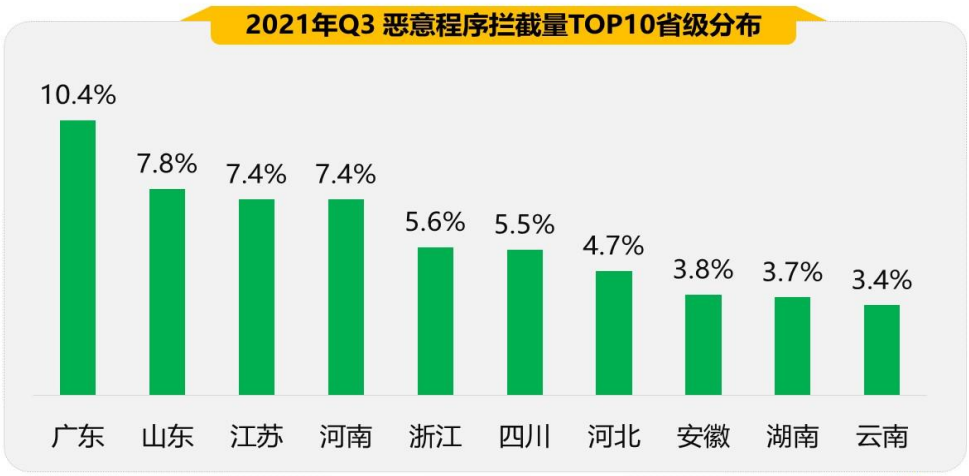
反观恶意程序拦截量趋势，基本较为平稳，360 对恶意程序的拦截能力相对稳定。广泛应用的线上场景，如网络授课、视频会议、远程办公等让大众对于移动网络的日常使用愈加频繁，360 对此一直在持续保证拦截，以便尽可能多地减小用户隐私泄露或者财产损失的风险。



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 年第三季度，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（7.8%）、江苏（7.4%）、河南（7.4%）、浙江（5.6%），此外四川、河北、安徽、湖南、云南的恶意程序拦截量也排在前列。



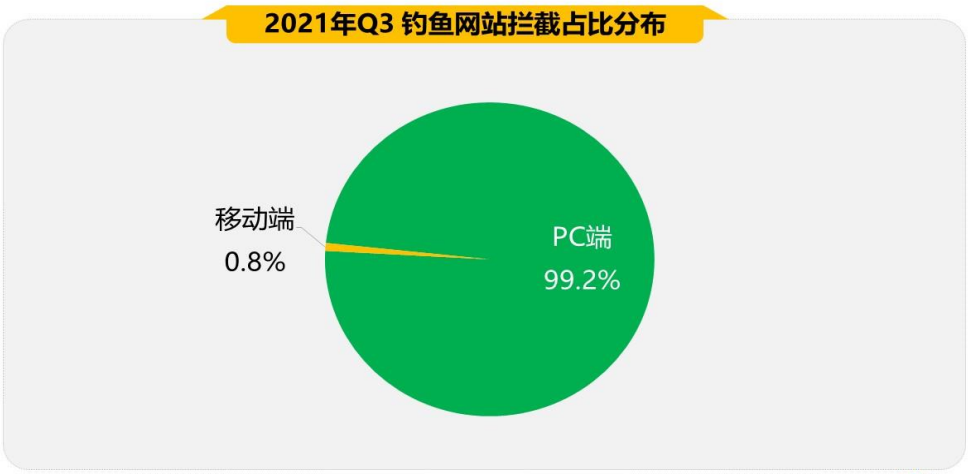
从城市分布来看，遭受手机恶意程序攻击最多的城市为上海市，占全国拦截量的 3.3%；其次为广州（2.2%）、成都（2.2%）、重庆（2.1%）、深圳（1.7%），此外北京、杭州、苏州、郑州、东莞的恶意程序拦截量也排在前列。

二、 钓鱼网站

1. 移动端钓鱼网站拦截占比

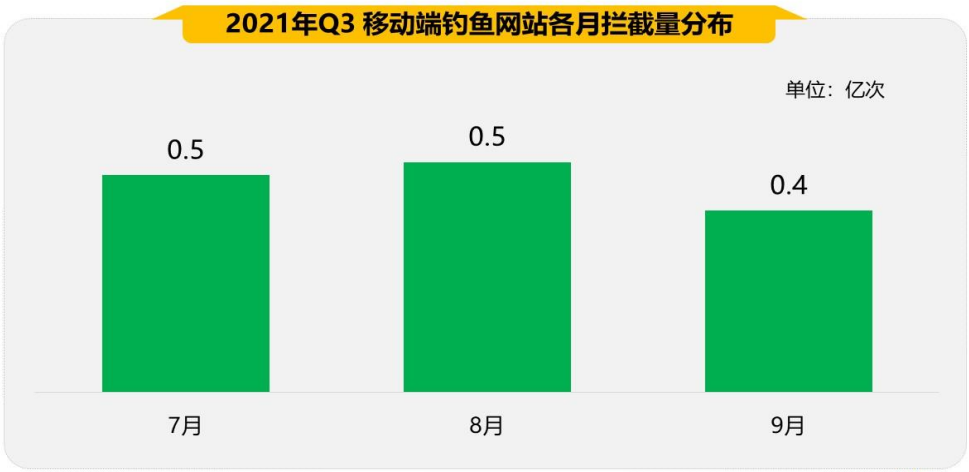
2021 年第三季度，360 安全大脑在 PC 端与移动端共为全国用户拦截钓鱼网站攻击约 168.9 亿次，同比 2020 年第三季度（304.0 亿次）下降了 44.4%。其中，PC 端拦截量约为 167.5 亿

次，占总拦截量的 99.2%，平均每日拦截量约 1.8 亿次；移动端拦截量约为 1.3 亿次，占总拦截量的 0.8%，平均每日拦截量约 145.4 万次。下图为 2021 年第三季度钓鱼网站拦截占比分布：



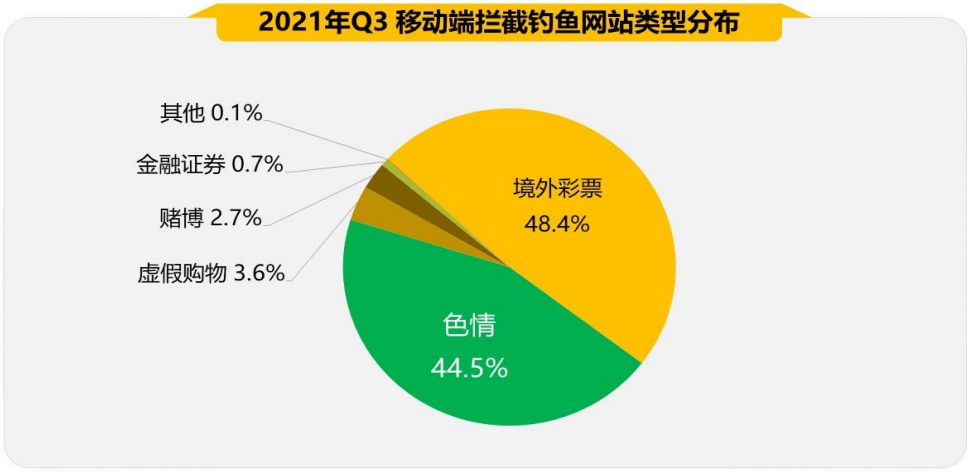
2. 移动端钓鱼网站各月拦截量分布

2021 年第三季度，360 安全大脑在移动端拦截钓鱼网站攻击约为 1.3 亿次，同比 2020 年第三季度（3.6 亿次）下降 63.3%。下图为 2021 年第三季度钓鱼网站各月拦截量分布：



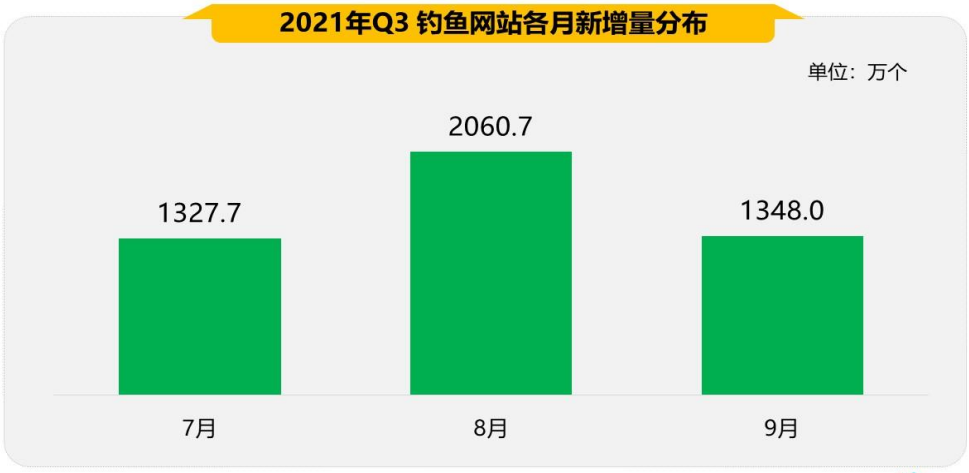
3. 移动端钓鱼网站类型分布

2021 年第三季度，移动端拦截钓鱼网站类型主要为境外彩票，占比高达 48.4%；其次为色情（44.5%）、虚假购物（3.6%）、赌博（2.7%）、金融证券（0.7%）等。下图为 2021 年第三季度移动端拦截钓鱼网站类型分布：

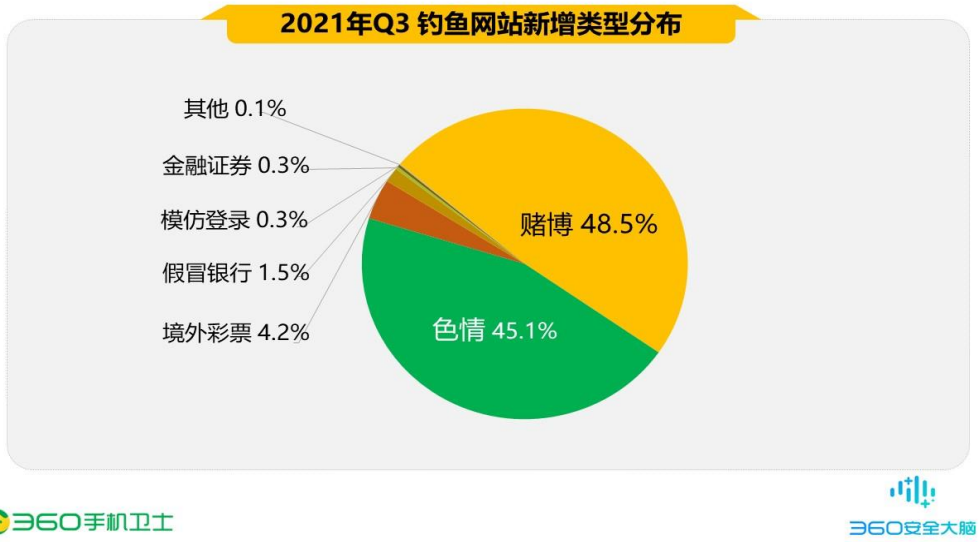


4. 移动端钓鱼网站新增量

2021 年第三季度，360 安全大脑共截获各类新增钓鱼网站 4736.4 万个，同比 2020 年第三季度（4794.5 万个）下降了 1.2%，平均每天新增 51.5 万个。



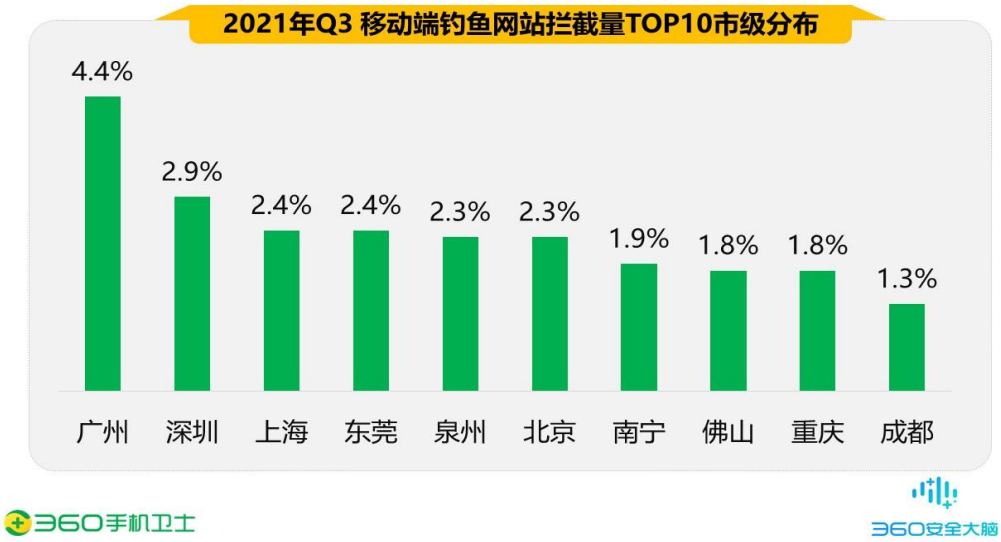
在钓鱼网站新增类型中，赌博类占据首位，占比 48.5%；其次为色情类（45.1%）、境外彩票（4.2%）、假冒银行（1.5%）、模仿登录（0.3%）、金融证券（0.3%）等。在过去的第三季度，360 安全大脑持续对钓鱼网站的类型进行细分，提升样本检测量与样本拦截能力，及时识别各类黑灰产网站，尽可能全面地保证用户的信息安全与财产安全。下图为 2021 年第三季度移动端新增钓鱼网站类型分布：



5. 移动端钓鱼网站拦截量地域分布

2021 年第三季度，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 21.6%；其次为福建（7.5%）、广西（7.1%）、山东（5.9%）、河南（5.2%），此外浙江、湖南、江苏、河北、江西的钓鱼网站拦截量也排在前列。

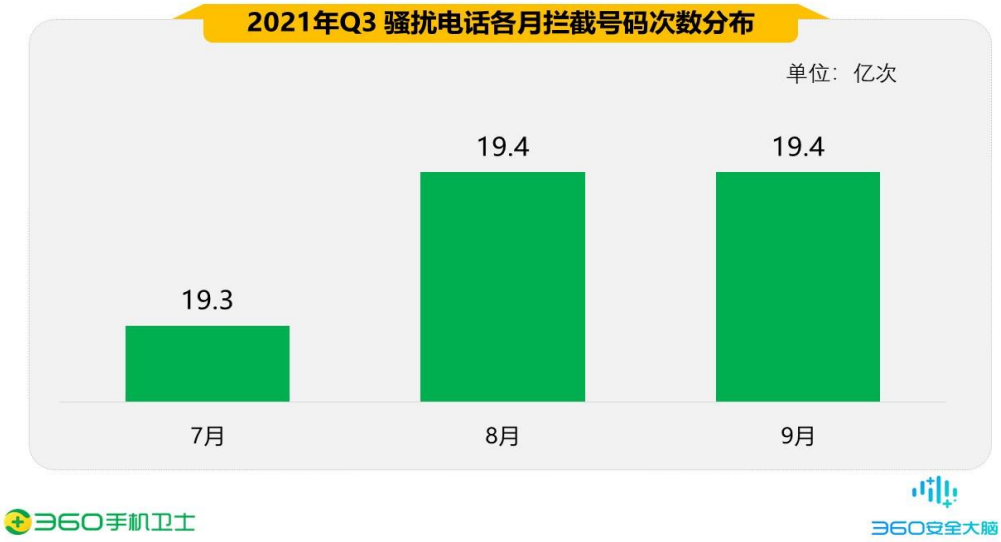
从城市分布来看，移动端拦截钓鱼网站最多的城市为广州市，占全国拦截量的 4.4%；其次为深圳（2.9%）、上海（2.4%）、东莞（2.4%）、泉州（2.3%），此外北京、南宁、佛山、重庆、成都的钓鱼网站拦截量也排在前列。



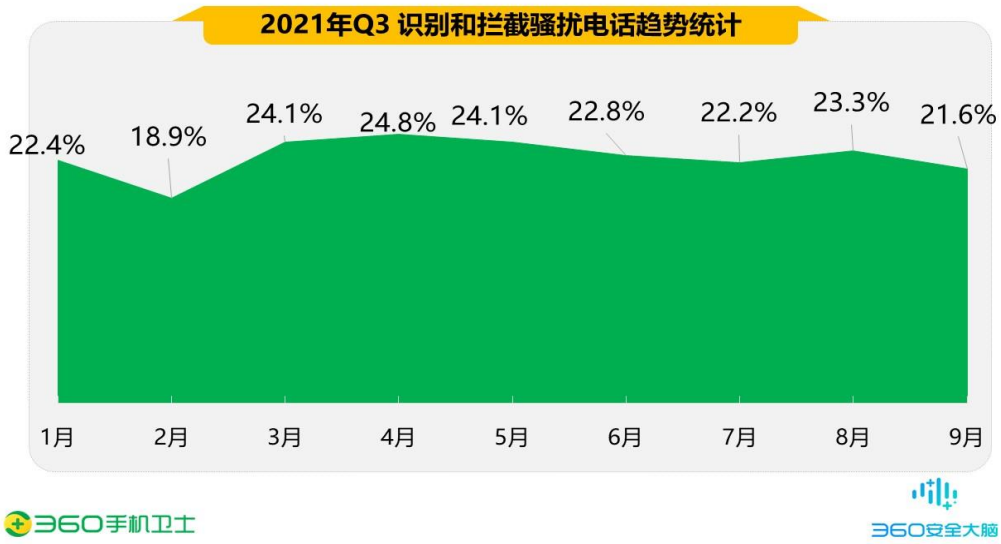
三、 骚扰电话

1. 骚扰电话标记拦截量

2021 年第三季度，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 58.2 亿次，平均每天识别和拦截骚扰电话约 0.6 亿次。同比 2020 年第三季度（56.2 亿次）上升了 3.6%。下图为 2021 年第三季度骚扰电话各月拦截号码次数分布：

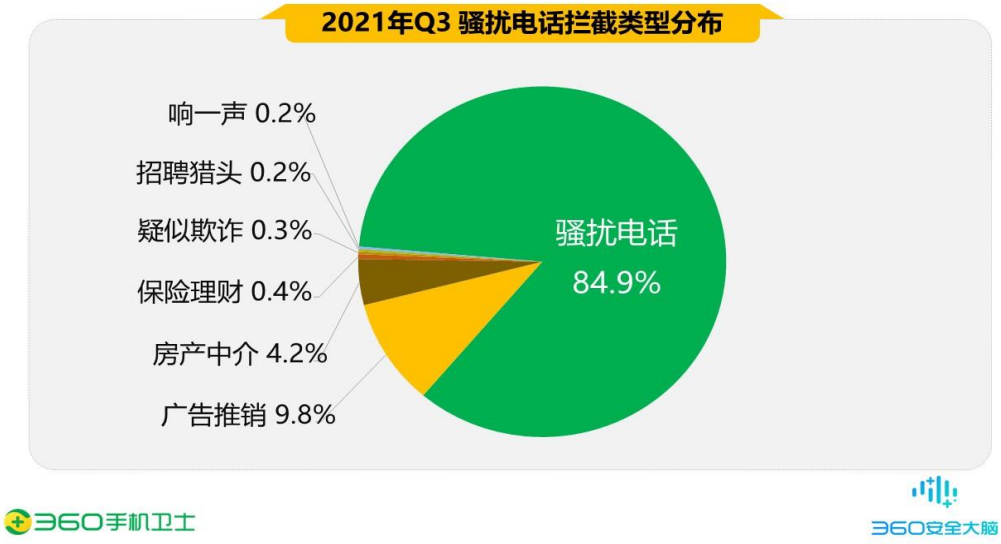


根据各月骚扰电话呼入占比分析，2021 年 2 月份期间正值春节假期，春节期间从事拨打骚扰电话的人员减少，从而导致骚扰电话的呼入量降低。2021 年 3 月份起，骚扰电话拦截量回升，之后拦截量稳中有所下降，第三季度相对稳定。下图为 2021 年第三季度识别与拦截骚扰电话趋势统计：



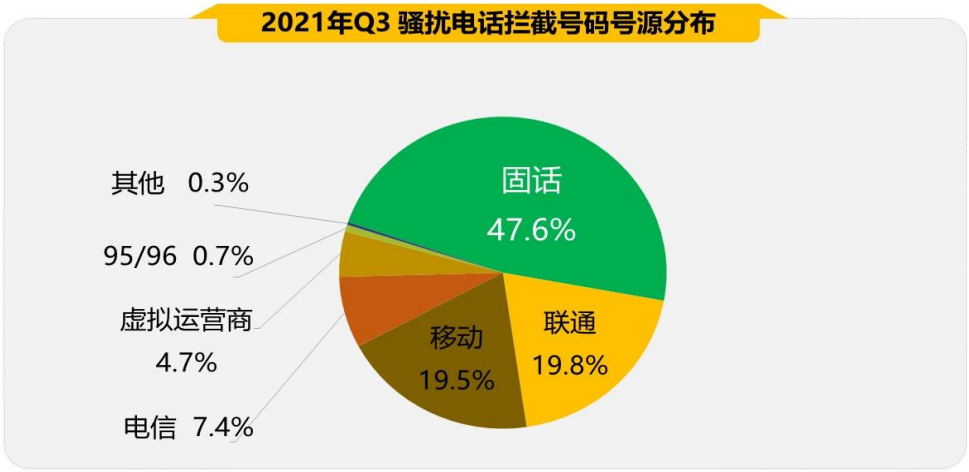
2. 骚扰电话拦截类型分布

2021 年第三季度，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 84.9%的比例位高居首位；其次为广告推销（9.8%）、房产中介（4.2%）、保险理财（0.4%）、疑似欺诈（0.3%）、招聘猎头（0.2%）与响一声（0.2%）。下图为 2021 年第三季度骚扰电话拦截类型分布：

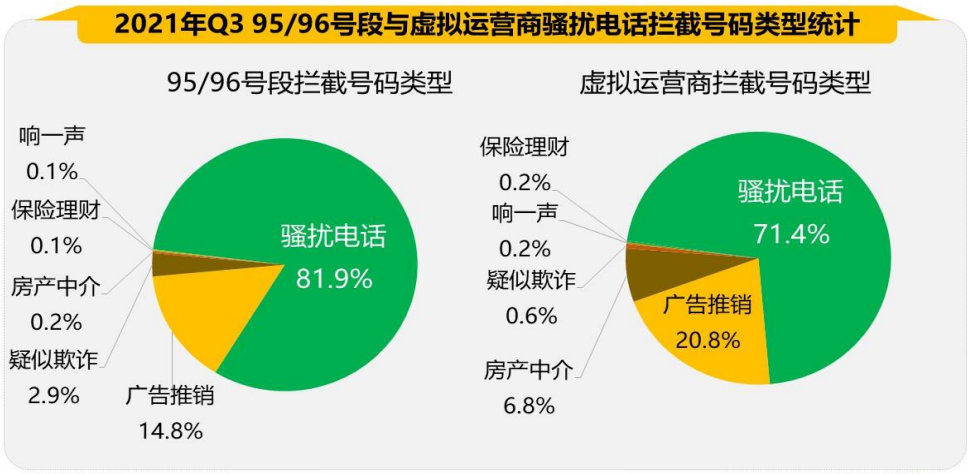


3. 骚扰电话拦截号码号源分布

2021 年第三季度，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 47.6%，其次为运营商为中国联通的个人手机号（19.8%）、运营商为中国移动的个人手机号（19.5%）、运营商为中国电信的个人手机号（7.4%）、虚拟运营商（4.7%）、95/96 开头号段（0.7%）等。下图为 2021 年第三季度骚扰电话拦截号码号源分布：



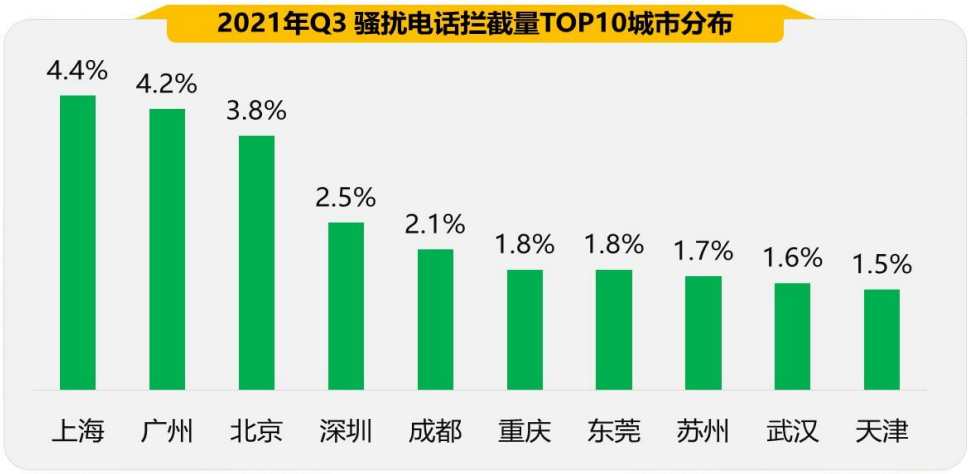
观察 95/96 号段与虚拟运营商骚扰电话拦截号码类型，95/96 号段骚扰电话类占据首位，占比 81.9%；虚拟运营商也是骚扰电话类占据首位，占比 71.4%；广告推销类分别占比 14.8%与 20.8%，类型比例占据前列。95/96 号段与虚拟运营商号码依然是不法分子从事非法行径的主要“工具”之一。



4. 骚扰电话归属地分布

2021 年第三季度，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 14.5%；其次是山东（7.0%）、江苏（6.3%）、浙江（4.8%）、四川（4.6%），此外广西、河北、河南、上海福建的骚扰电话拦截量也排在前列。

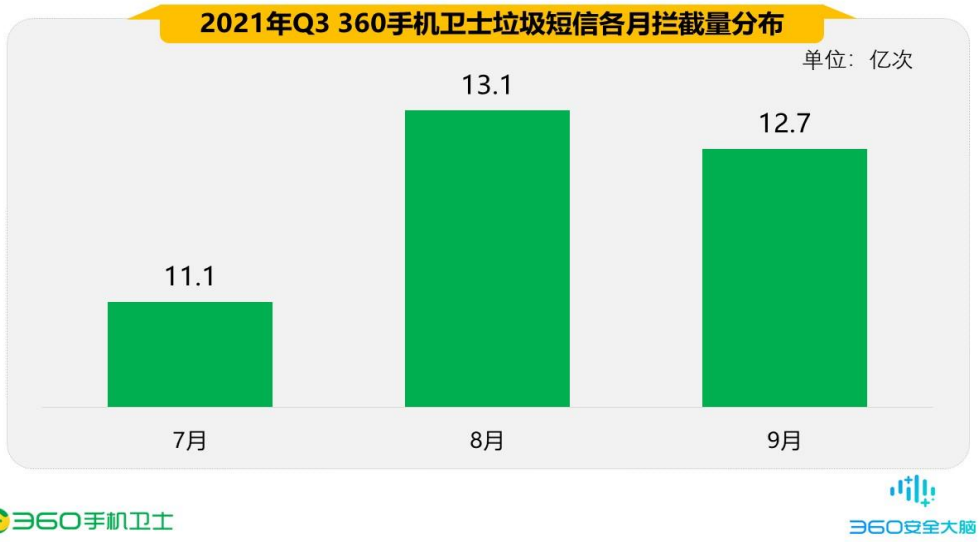
从城市分布来看，上海市用户接到的骚扰电话最多，占全国骚扰电话拦截量的 4.4%；其次是广州（4.2%）、北京（3.8%）、深圳（2.5%）、成都（2.1%），此外重庆、东莞、苏州、武汉、天津的骚扰电话拦截量也排在前列。



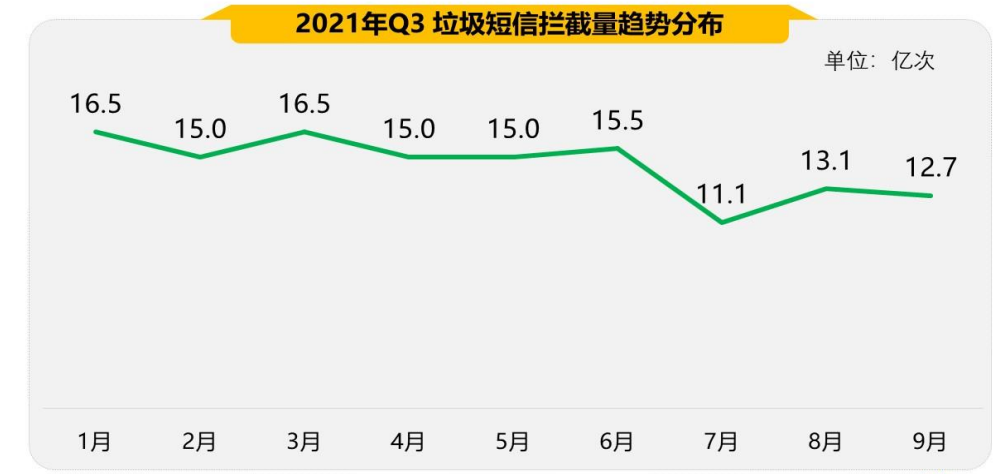
四、 垃圾短信

1. 垃圾短信拦截量

2021 年第三季度，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 36.9 亿条，同比 2020 年第三季度（46.3 亿条）下降了 20.3%，平均每日拦截垃圾短信约 4014.6 万条。下图为 2021 年第三季度 360 手机卫士垃圾短信各月拦截量分布：

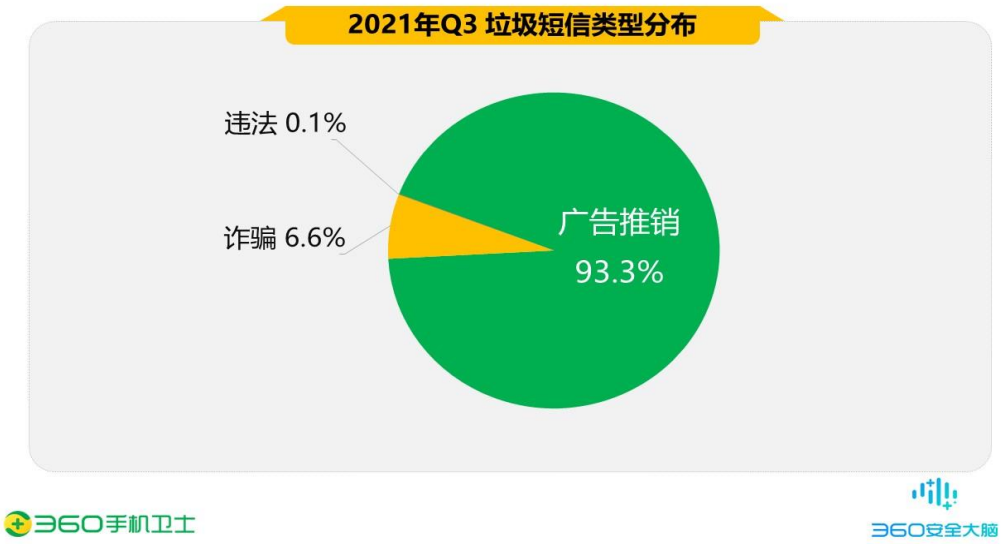


根据垃圾短信拦截量趋势分布，7 月有所下降后，后续逐渐呈现走高趋势。下图为垃圾短信拦截量趋势分布：

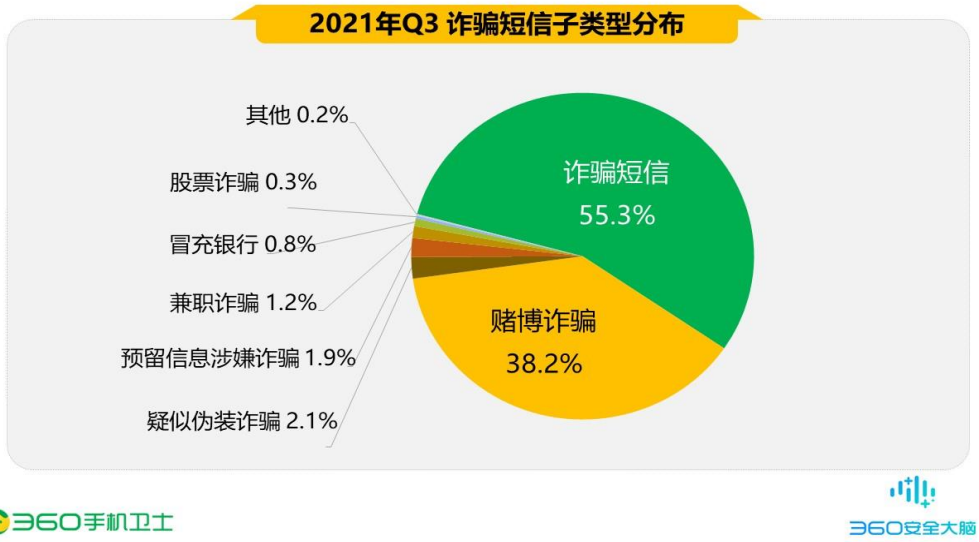


2. 垃圾短信类型分析

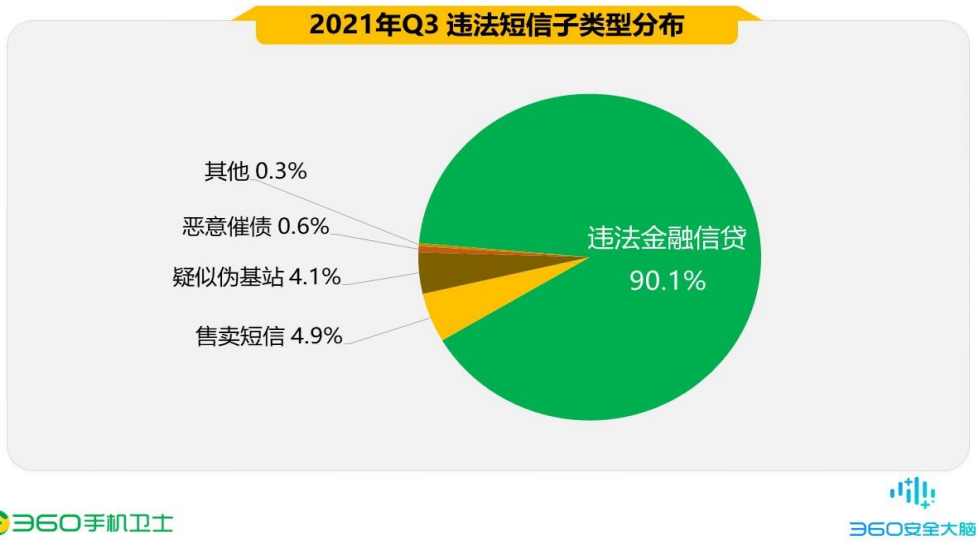
2021 年第三季度，垃圾短信的类型分布中广告推销短信最多，占比为 93.3%；诈骗短信占比 6.6%；违法短信占比 0.1%。



从诈骗短信拦截类型来看，诈骗短信以 55.3%的比例位居首位；其次为赌博诈骗（38.2%）、疑似伪装诈骗（2.1%）、预留信息涉嫌诈骗（1.9%）、兼职诈骗（1.2%）、冒充银行（0.8%）、股票诈骗（0.3%）等。下图为 2021 年第三季度诈骗短信子类型分布：



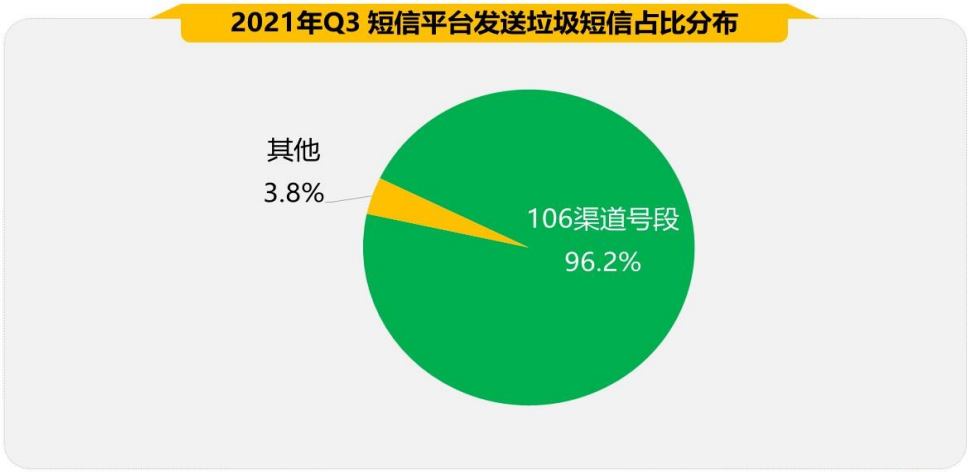
从违法短信拦截类型来看，违法金融信贷短信以 90.1%的比例位居首位；其次为售卖信息（4.9%）、疑似伪基站发送（4.1%）、恶意催债（0.6%）等。下图为 2021 年第三季度违法短信子类型分布：



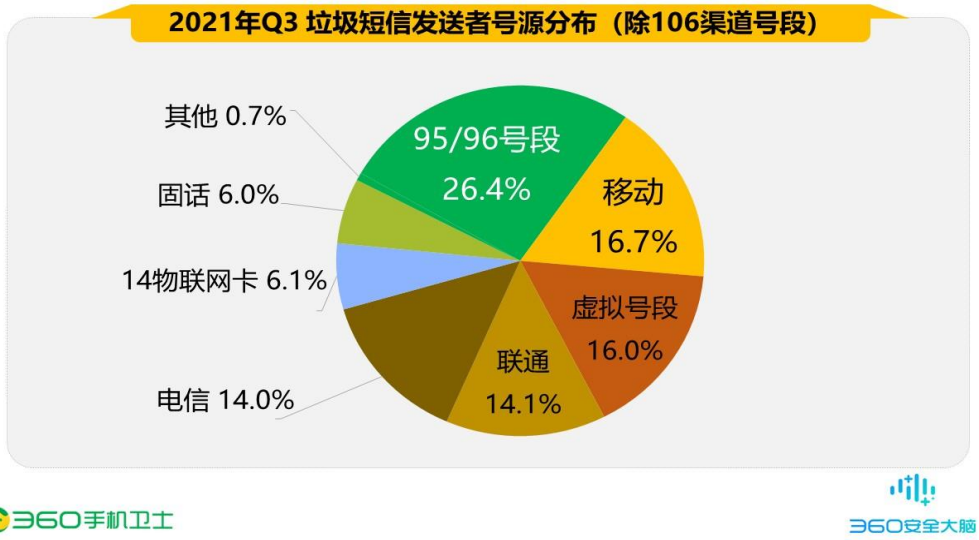
3. 垃圾短信发送者运营商号源分布

2021 年第三季度，短信平台 106 开头号段依然是传播垃圾短信的主要号源，占比高达 96.2%；利用其他号段传播垃圾短信占比约 3.8%。利用短信平台、虚拟运营商号段传播垃圾短信依然是不法分子目前的主要渠道。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，同时在短信内容中利用关键词、变体字等实现“攻防”，帮助不法内容进行传播。

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 年第三季度短信平台发送垃圾短信占比分布：

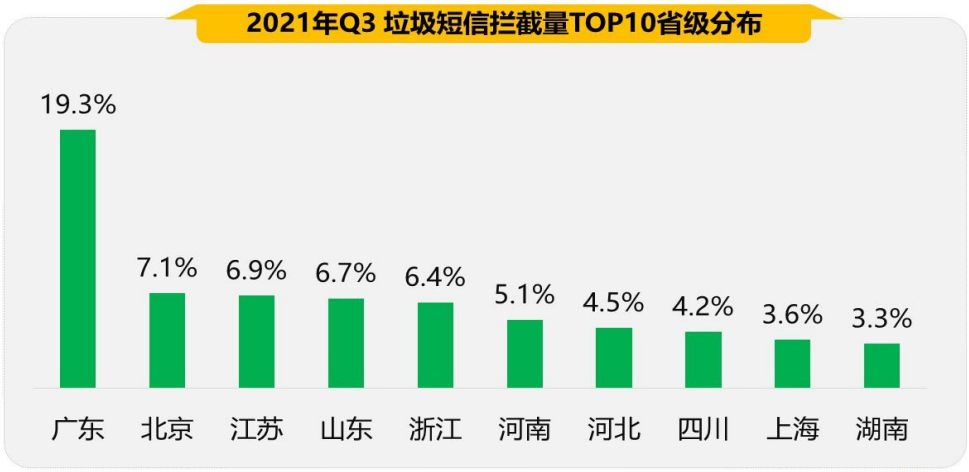


2021 年第三季度，除短信平台 106 开头号段发送垃圾短信外，从其他发送者号码个数分布看，利用 95/96 号段发送垃圾短信的最多，占比 26.4%；其次是运营商为中国移动的个人手机号（16.7%）、虚拟运营商号段（16.0%）、运营商为中国联通的个人手机号（14.4%）、运营商为中国电信的个人手机号（14.0%）、14 物联网卡（6.1%）与固话（6.0%）等。



4. 垃圾短信拦截量地域分析

2021 年第三季度，从各地垃圾短信的拦截量上分析，广东省用户收到的垃圾短信最多，占全国垃圾短信拦截量的 19.3%；其次是北京（7.1%）、江苏（6.9%）、山东（6.7%）、浙江（6.4%），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。



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 9.0%；其次是北京（8.1%）、深圳（4.9%）、上海（4.1%）、南京（3.4%），此外重庆、杭州、石家庄、成都、西安的垃圾短信拦截量也排在前列。