威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

黑产大数据

2024年上半年互联网黑灰产研究报告

THREATHUNTER

目录
Contents

前言

2024 年上半年，黑灰产从业人员人数超过 427 万，威胁猎人监测到国内作恶手机号数量高达 323 万，日活跃风险 IP 数量 1136 万，涉及洗钱银行卡数量 19.5 万。

近年来，数字化与实体经济的融合日渐深入，大规模业务线上场景下，黑灰产对企业业务安全的扰乱更加突出，恶意刷量、薅羊毛、金融欺诈等黑产事件层出不穷，逐渐智能化和链条化的网络黑产运作，给企业带来真金白银的经济损失，影响了企业正常运营及长期发展，打击网络黑灰产，加强有效防御成为各行业企业的目标与共识。

威胁猎人发布**《2024 年上半年互联网黑灰产研究报告》**，从 2024 年上半年互联网黑灰产发展现状、黑灰产攻击资源、黑灰产攻击技术及场景等维度进行全面梳理分析，力求通过客观呈现黑灰产情报数据，帮助更多企业深入直观了解黑灰产业，有效防控各类攻击风险。

相关名词定义：

1、风险 IP：业内也称黑 IP，指存在攻击风险（包括代理、秒拨等恶意行为）的 IP；

2、风险手机号：存在被滥用盗用等风险的手机号，如被黑产用于接收短信，实施批量恶意攻击的手机号，通常从接码平台或发卡平台捕获；

3、风险邮箱：指被黑产用于恶意注册生成的临时邮箱，用以骗取用户重要信息、传播恶意程序等；

4、黑手机卡：指未进行实名登记或以假身份进行实名登记的，并被不法分子利用实施违法犯罪活动的电话卡；

5、猫池卡：指通过“猫池”这一网络通信硬件，实现同时支持多个号码通话、群发短信等功能的黑手机卡；

6、拦截卡：指通过病毒木马控制真实用户手机短信/验证码收发权限的手机卡，通常捕获自拦截卡平台；

7、洗钱银行卡：指被黑产用于非法资金清洗（将违法所得收入合法化）的银行卡，例如赌博及诈骗团伙通过银行卡消费、转账等方式转移洗钱资金；

8、涉赌卡：指常被用于赌博平台内进行充值收款的银行卡，关联资产涉及到赌博洗钱行为。威胁猎人通过人工和自动化结合的方式，从各类赌博平台中监测用于收款行为的银行卡账号信息；

9、跑分卡：指活跃在跑分平台，常被用于各种非法来源资金的流通交易的银行卡。威胁猎人通过自动化的方式，从跑分平台 APP 中获取到跑分订单中的银行卡账号信息；

10、涉诈卡：指常被用于社交黑产群聊中进行诈骗资金转移的银行卡，关联资产涉及到诈骗洗钱行为。威胁猎人通过自动化的方式，从各大匿名社交黑产群聊中发送记录中，提取诈骗团伙使用银行卡账号信息；

11、洗钱对公账户：指被黑产用于非法资金清洗的银行对公账户，因对公账户具有收款额度大、转账次数多等特点，使得“对公账户”常常作为黑钱转账的集中点及发散点；

12、数据泄露事件：威胁猎人安全研究专家针对数据泄露情报的样例等进行分析及验证，确认为真实、有效的数据泄露事件；

13、暗网：指隐藏的网络，普通网民无法通过常规手段搜索访问，需要使用一些特定的软件、配置或者授权才能登录；

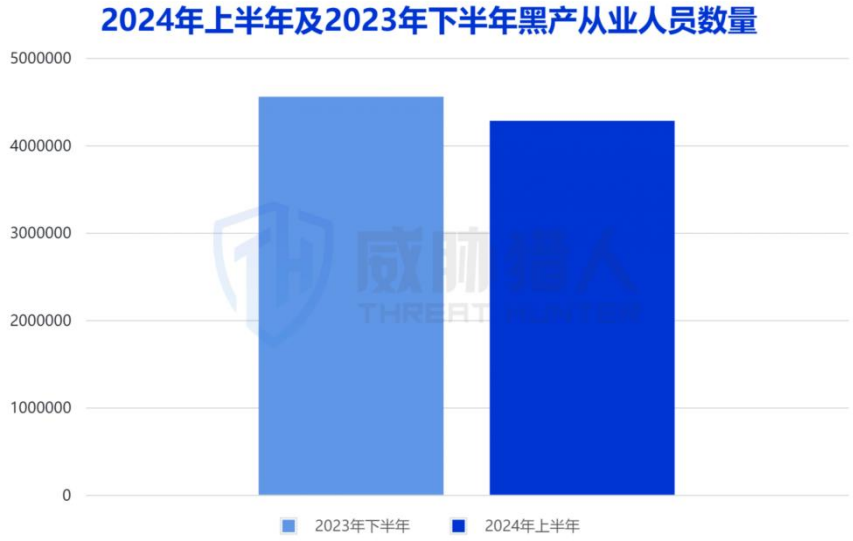
01

2024 年上半年
互联网黑灰产业发展现状

一、2024 年上半年互联网黑灰产业发展现状

1.1 2024 年上半年互联网黑灰产从业人员达 427 万，较 2023 年下半年下降 6.03%

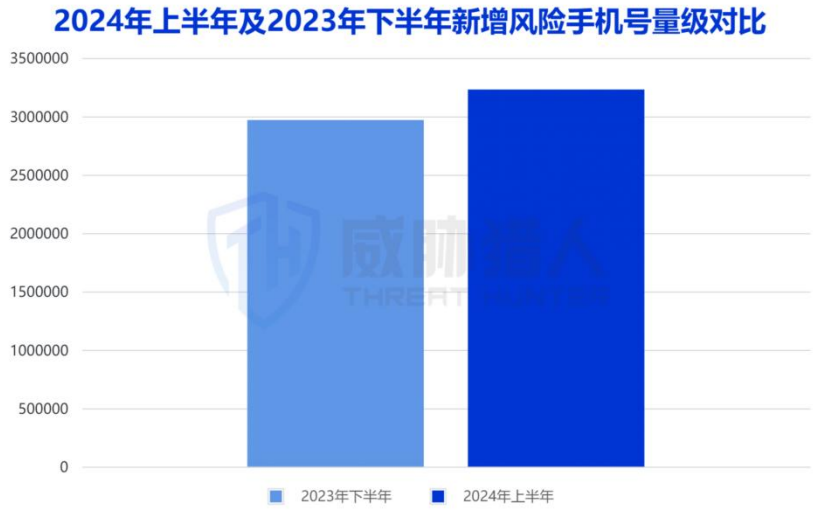
威胁猎人调研统计发现，2024 年上半年互联网黑灰产从业人员数量达到 427 万，较 2023 年下半年略有下降 6.03%。



1.2 2024 年上半年黑灰产资源概况

1.2.1 2024 年上半年新增国内风险手机号总量较 2023 年下半年增长 8.8%

据威胁猎人风险情报平台数据显示，2024 年上半年国内风险手机号数量达到 323 万，较 2022 年增长 8.8%。



1.2.2 2024 年上半年风险 IP 总量较 2023 年下半年增长 44.8%

2024 年上半年，威胁猎人监测发现日活跃风险 IP 数量持续上升，风险 IP 数量达到 1136 万，较 2023 年下半年增长 44.8%。

1.2.3 2024 年上半年涉及洗钱银行卡较 2023 年下半年下降 28%，主要由跑分卡大幅减少所致

2024 年上半年涉及洗钱银行卡数量 19.5 万，较 2023 年下半年下降 28%。涉及洗钱银行卡主要包括跑分卡、涉赌卡、涉诈卡，其中，跑分卡新增数量的降幅最大，较 2023 年下半年下降 50.3%，威胁猎人针对黑产团伙的跑分方式深入挖掘发现，2024 年上半年跑分团伙逐渐由跑分平台转向通过 Telegram 进行跑分，使得监测难度大幅提升。

涉赌卡：指常被用于赌博平台内进行充值收款的银行卡，关联资产涉及到赌博洗钱行为。威胁猎人通过人工和自动化结合的方式，从各类赌博平台中采集用于收款行为的银行卡账号信息。

跑分卡：指活跃在跑分平台，常被用于各种非法来源资金的流通交易的银行卡。威胁猎人通过自动化的方式，从跑分平台 APP 中获取到跑分订单中的银行卡账号信息。

涉诈卡：指常被用于社交黑产群聊中进行诈骗资金转移的银行卡，关联资产涉及到诈骗洗钱行为。威胁猎人通过自动化的方式，从各大匿名社交黑产群聊中发送记录中，提取诈骗团伙使用银行卡账号信息。

02

2024 年上半年
黑产攻击资源分析

二、2024 年上半年黑产攻击资源分析

2.1 2024 年上半年风险手机卡资源分析

2.1.1 2024 年上半年猫池卡资源变化趋势

（1）2024 年上半年国内猫池卡较 2023 年下半年增加 7.71%

据威胁猎人情报平台数据显示，2024 年上半年捕获新增猫池卡 309 万个，较 2023 年下半年上升 7.71%。

猫池卡：指通过“猫池”这一网络通信硬件，实现同时支持多个号码通话、群发短信等功能的黑手机卡。

经威胁猎人情报专家分析，出现这一趋势的主要原因是：

1、2 月因春节期间黑产交易放缓，下游作恶者活跃度降低导致供应量显著下降，节后恢复稳步上涨趋势；

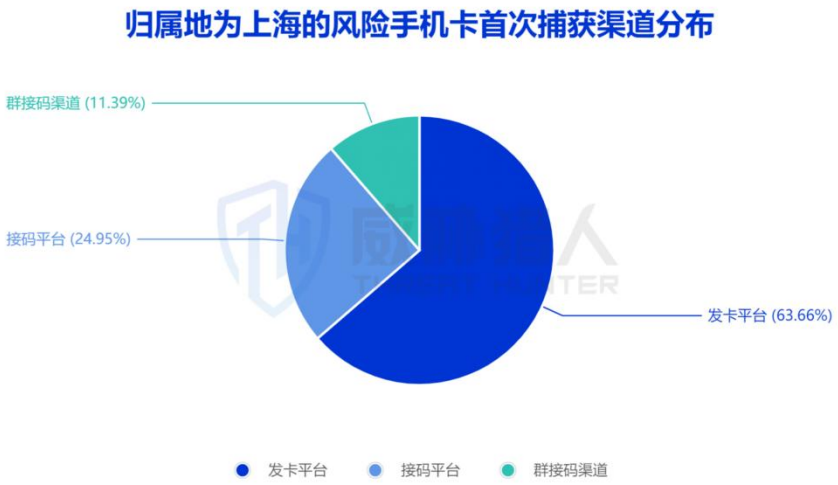
2、6 月猫池卡数量下降主要受到高考期间风控加强的影响，高考期间各大平台账号批量注

册、恶意引流等监测力度大大加强（如不可修改账号名称、头像、介绍等），多个渠道卡商主动反馈受该原因干扰，黑卡供给存在问题。

（2）2024 年上半年新增猫池卡归属最多的三个省份为：上海、山东、辽宁

威胁猎人对 2024 年上半年新增国内猫池卡进行统计分析，发现上海、山东、辽宁三省（含直辖市）为猫池卡归属地最多的三个省份；针对归属城市分析发现，猫池卡归属地最多的三个城市为上海、重庆、武汉。

由下图可见，2024 年上半年上海的猫池卡新增数量远超其他省市，深入分析发现，其主要原因在于 2024 年 3 月及 5 月，国内两大头部发卡平台持有并出售大量归属地在上海的风险手机卡，其数量在新增总量的 40%以上。



（3）2024 年上半年捕获的猫池卡中，归属国内三大运营商的占 76.1%

2024 年上半年监测到猫池卡 364 万张，其中归属国内三大运营商的猫池卡占比 76.1%，归属其他运营商的占比 23.9%。

2.1.2 2024 年上半年拦截卡资源变化趋势

（1）2024 年上半年国内拦截卡较 2023 年下半年增加 42.57%，从新增渠道首次捕获的拦截卡占比高达 94%

2024 年上半年，威胁猎人捕获新增拦截卡达 13.18 万，较 2023 年下半年增加 42.57%。针对捕获的拦截卡进一步分析发现，2024 年上半年新增 6 个拦截卡来源渠道，同时捕获的拦截卡多为系统首次捕获，首次捕获占比高达 94%，拦截卡供应渠道的增加与快速更新，无疑增加了业务方风控难度。

（2）2024 年上半年拦截卡归属最多的三个省份为：福建、广东、四川

针对 2024 年上半年捕获到的国内拦截卡统计分析发现，福建、广东、四川三省为拦截卡归属地最多的三个省份；从归属城市来看，重庆市、三明市（福建）、上海市三城市为拦截卡归属地最多的城市，与猫池卡归属城市存在较大的重合。

（3）2024 年上半年捕获的拦截卡中，归属国内三大运营商的占 98.29%

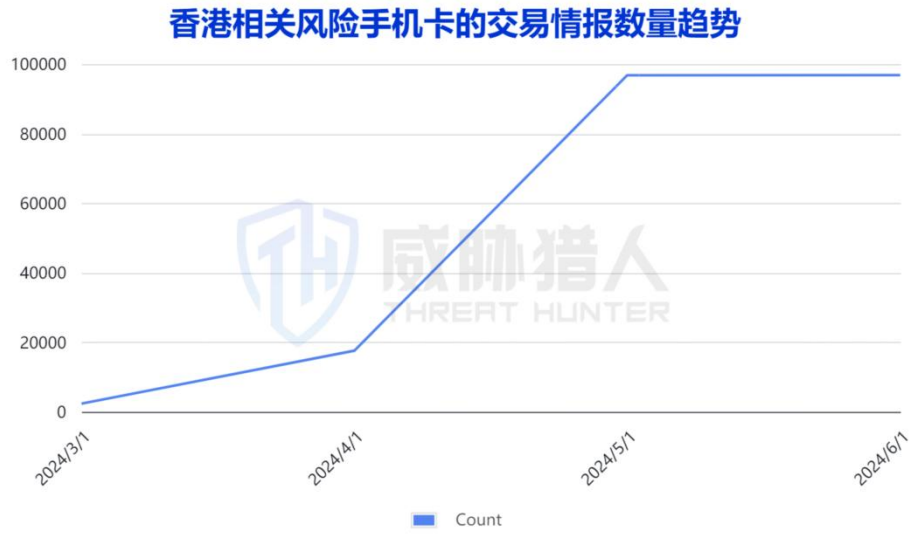
2024 年上半年威胁猎人情报运营平台捕获拦截卡 39.8 万张，归属国内三大运营商的拦截卡占比达 98.31%。

2.1.3 归属地为香港的风险手机卡大幅增加，2024 年 6 月捕获香港相关风险手机卡近 10 万

针对黑卡主要来源渠道进一步研究发现，2024 年上半年，归属地为香港的风险手机卡交易数量呈现大幅增长趋势，2024 年 3 月香港卡交易量级仅为数千张，2024 年 6 月香港卡交易量级达到近 10 万。

香港相关风险手机卡数量的大幅增长，从需求侧来看，2024 年 5 月至 6 月，香港发生多起线上诈骗事件，事件过程中，下游诈骗黑产利用香港手机卡注册 whatsapp 等境外聊天软件，对受害者展开线上诈骗，一定程度上导致了香港卡数量的大幅增长，也反映了风险手机

卡在地域上的风险趋势及供需变化。



对比其他境内手机卡，香港手机卡具备如下特点：

1、注册范围广：香港手机卡注册范围广，可注册 Telegram、WhatsApp 等海内外应用；

2、在线使用时间长：香港手机卡接码服务的在线使用时间相对境内卡更长，一般可保证一个月重复使用，而境内手机卡一般为数日；

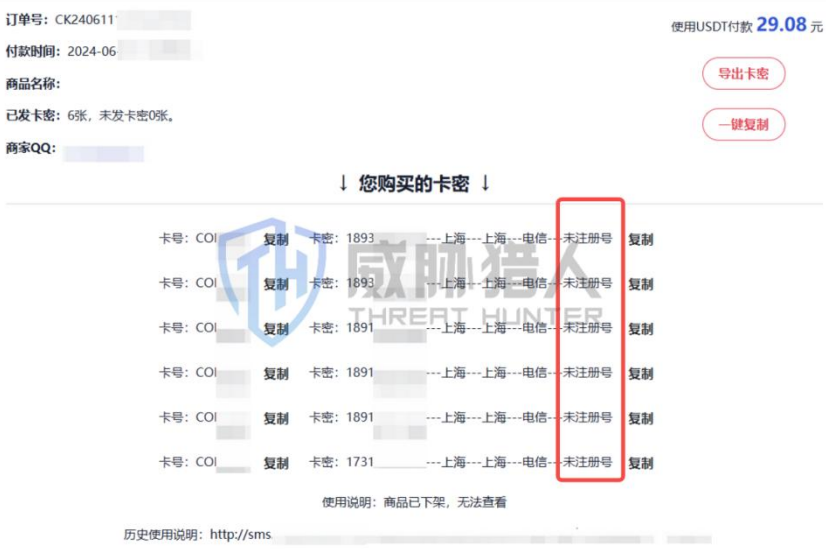
3、价格较低：香港手机卡的价格相对境内卡接码价格更低；

4、支持多种接码形式：香港卡支持多种接码形式，目前威胁猎人在接码平台、发卡网站、私域接码均发现了香港相关手机卡的作恶记录。

2.1.4 黑卡物料资源标签更加丰富，提升下游黑产筛卡效率、实现精准作恶

威胁猎人研究发现，2024 年上半年，黑产在非法交易中对黑卡物料的筛选及使用更为精细，相较于 2023 年黑卡商品描述字段，除了会提供的黑卡类别，注册情况等信息外，卡商还会标识号码“已筛选”，即卡商在购买后的订单页面中展示号码的历史账户信息，并将信息提

供给下游购买方，使其确定是否为目标卡类，减少筛卡成本，大幅提升下游黑产作恶效率。



与此同时，威胁猎人研究发现，黑灰产之所以能提供精确的账号及相关信息，主要借助了黑灰产新老号检测工具实现，该工具通过恶意调用业务相关的应用接口 API，来检测号码是否注册或存在历史绑定记录。

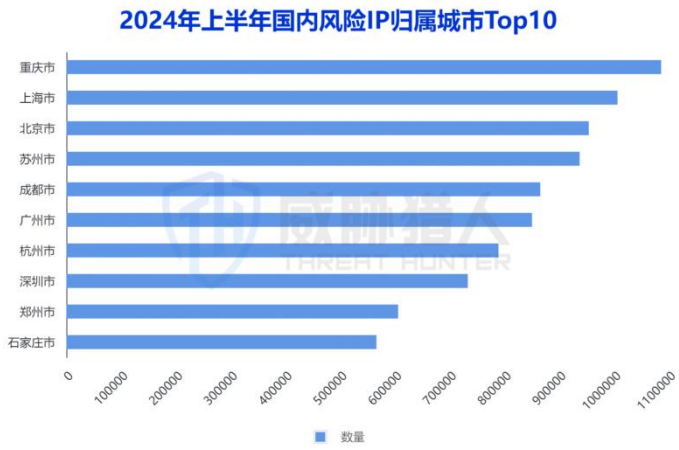
2.2 2024 年上半年风险 IP 资源分析

2.2.1 2024 年上半年风险 IP 资源变化趋势

威胁猎人持续提升国内外风险 IP 监测能力，为互联网平台优化国内外风控规则提供了有力支持，2024 年上半年威胁猎人持续监测国内风险 IP5503 万个，国外风险 IP10273 万个，较 2023 年下半年分别提升 18.62%和 22.44%。我们对国内及国外两种类型的风险 IP 分析发现：

（1）2024 年上半年国内风险 IP 归属最多的三个省份：江苏、广东、河南

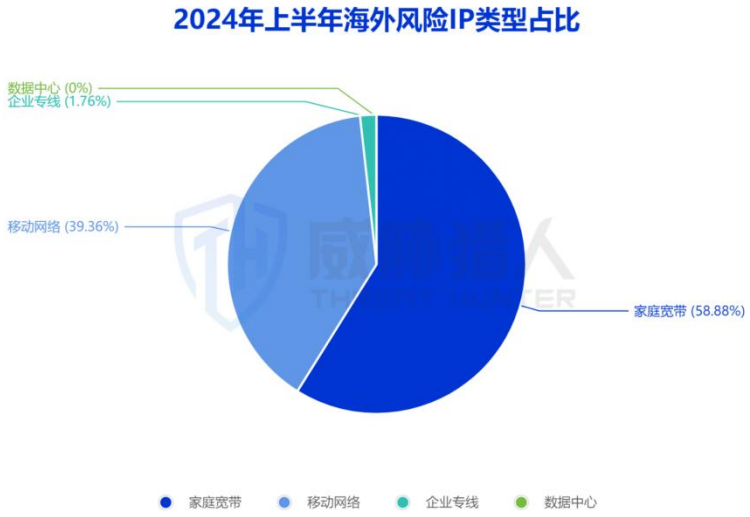
（2）2024 年上半年国内风险 IP 归属最多的三个城市：重庆、上海、北京



（3）2024 年上半年国外风险 IP 归属最多的三个国家：巴西、印度、美国

（4）2024 年上半年国内风险 IP 类型中，家庭宽带类型占比近 90%

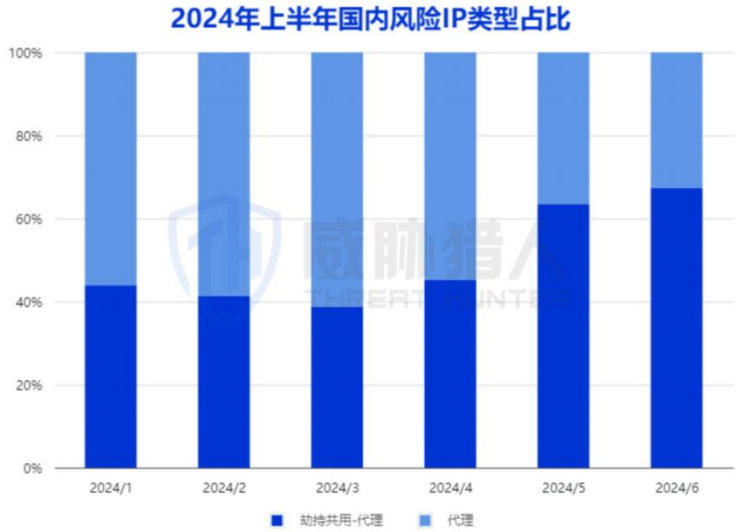
（5）2024 年上半年海外风险 IP 类型以家庭宽带、移动网络为主



2.2.2 2024 年上半年“劫持共用代理”IP 攻击占总量 67%，成为攻击者主要使用 IP 类型

威胁猎人对代理 IP 平台持续监测，发现 2024 年上半年黑产通过植入木马恶意使用正常用户 IP 的行为更加猖獗，从 2024 上半年捕获数据来看，“劫持共用代理”IP 日均捕获数量达 80 万，这一标签的 IP 攻击占比从 43.88%（2024 年 1 月）上升至 67.41%（2024 年 6 月）。

由于这类 IP 大部分时间是正常用户使用，如进行点击、充值、浏览等行为，少量时间会被黑产劫持共用，出现短暂的作恶行为，因此平台可能会认定该用户为正常用户，进而忽视其短暂的作恶行为，给黑产可乘之机。



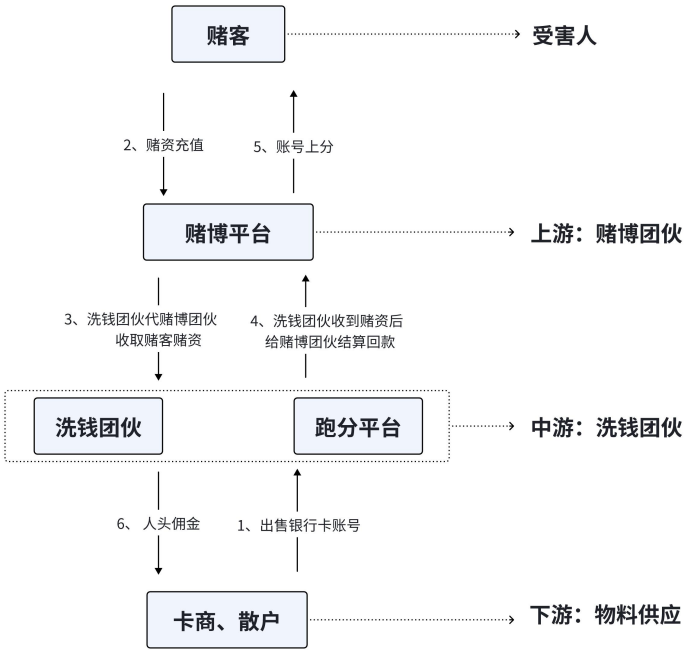
2.3 2024 年上半年网络洗钱资源分析

2.3.1 2024 年上半年涉及洗钱的银行卡资源变化

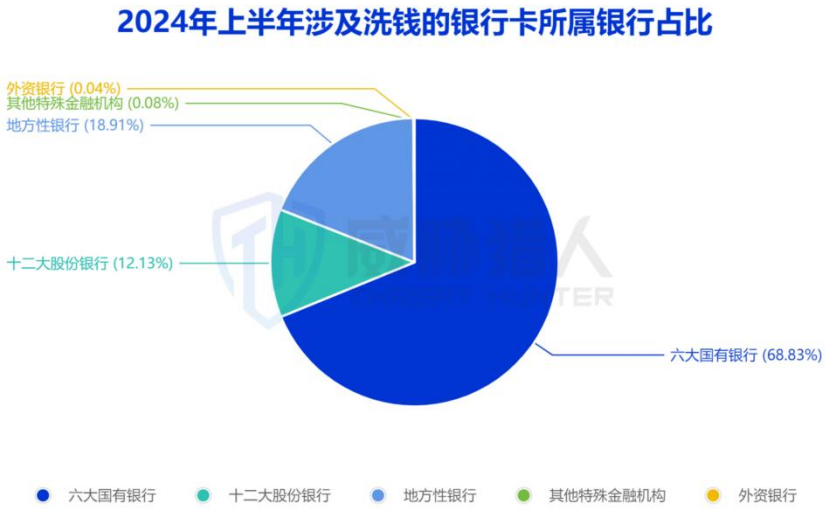
(1)涉及洗钱的银行卡数量较 2023 年下半年下降 28%，其中跑分卡数量下降 50.3%

2024 年上半年涉及洗钱银行卡数量为 19.5 万，较 2023 年下半年下降 28%。涉及洗钱银行卡主要包括跑分卡、涉赌卡、涉诈卡，其中跑分卡新增数量降幅最大，较 2023 年下半年下降 50.3%，威胁猎人针对黑产团伙的跑分方式深入挖掘发现，2024 年上半年跑分团伙逐渐由跑分平台转向 Telegaram 跑分，使得监测难度大幅提升。

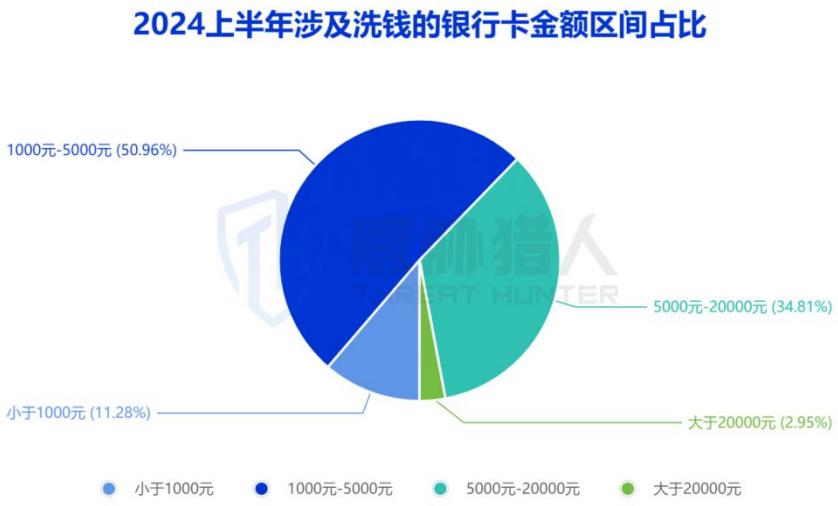
赌博平台跑分的具体流程如下：



（2）涉及洗钱银行卡归属国有银行的占比远高于非国有银行，与国有大行发卡量相关



（3）银行卡洗钱金额的主要区间为 5000 元以下



（4）超过 65%的洗钱银行卡仅在监测到的当天活跃

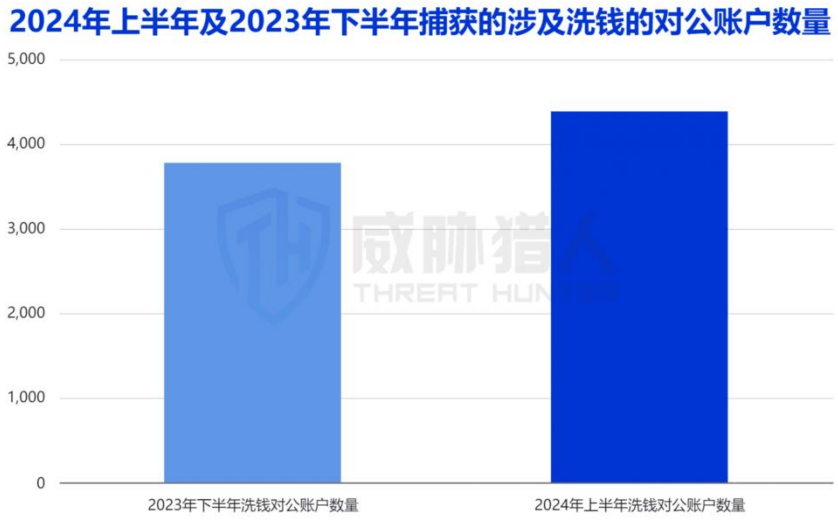
威胁猎人对近半年捕获洗钱银行卡的“首次发现时间”和“最新发现时间”进行分析，发现统计期间内，65.8%的洗钱银行卡仅在捕获当天活跃，可见，为了避免风控监测，频繁用于洗钱的银行卡较少。

2.3.2 2024 年上半年涉及洗钱的对公账户资源变化

洗钱对公账户：对公账户指以公司名义在银行开立的账户，洗钱对公账户指被黑产用于非法资金清洗的银行对公账户，因对公账户具有收款额度大、转账次数多等特点，使得“对公账户”常常作为黑钱转账的集中点及发散点。

（1）2024 年上半年监测涉及洗钱的对公账户数量较 2023 年下半年上升 16%

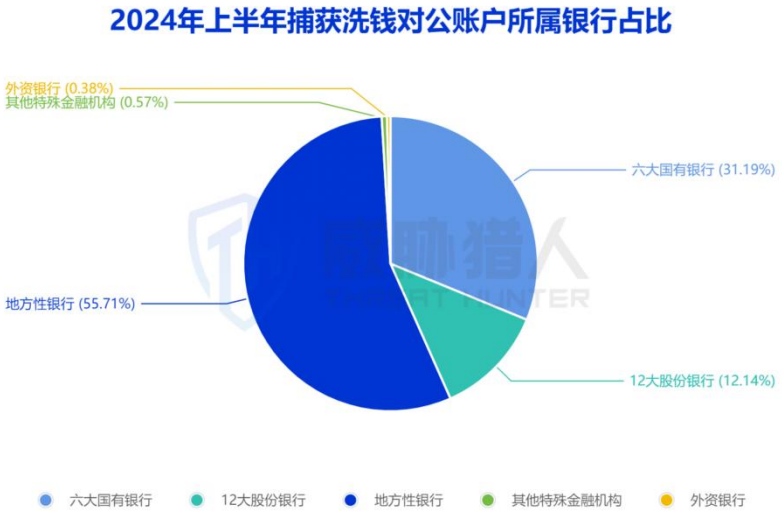
2024 年上半年威胁猎人持续监测黑产在洗钱过程中所使用的银行对公账户资源，发现涉及洗钱的对公账户数量持续上升，由 3378 个上升到 4386 个，较 2023 年下半年上升 16%。

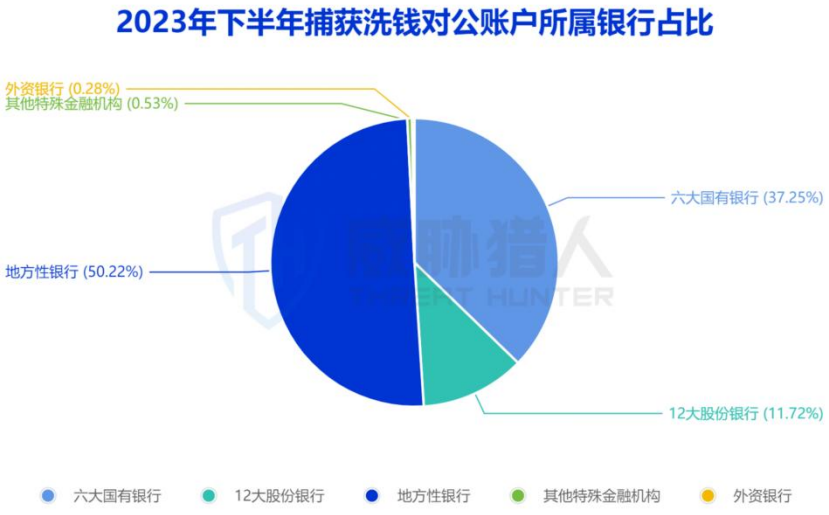


（2）2024 年上半年监测涉及洗钱对公账户的所属银行 732 家，国有银行占比 31%

2024 年上半年威胁猎人共捕获到涉及洗钱的对公账户 4865 个，涉及银行机构 732 家。洗钱对公账户所属银行中，国有银行占比 31.19%。

此外，监测到的地方性银行对公账户数量较 2023 年下半年上升 5.51%，而国有占比下降 6.06%，黑产利用对公账户洗钱的过程中，在开户行的选择上，部分开始转向地方性银行进行作恶。





(3) 2024 年上半年监测涉及洗钱对公账户归属省份中，安徽、江西、陕西首次进入 TOP10

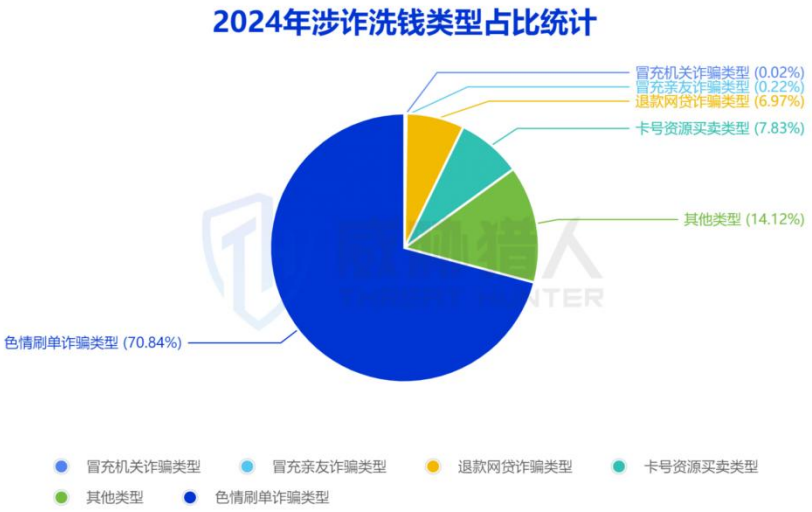
涉及洗钱对公账户归属省份 TOP5 省份较 2023 年下半年基本不变，而安徽、江西、陕西省份排名首次上升至 TOP10 行列，进一步分析发现，这类省份地方性银行对公账户的增长趋势明显，该排名变动背后，一定程度也体现了洗钱团伙逐渐使用农村信用合作社及地方性银行对公账户的趋势。

2.3.3 2024 年上半年色情刷单类型的诈骗洗钱资金占总量 70%以上

基于黑产诈骗金额和风险程度，目前监测到的黑产诈骗手法大致可以分为 6 种类型，其中色情刷单诈骗类型最多，占比超 70%。据研究调查发现，冒充机关诈骗、冒充亲友诈骗、退款网贷诈骗这几类诈骗形式风险较高，诈骗金额较大，色情刷单诈骗相对风险较低，诈骗金额较小，金额一般在 5000 元以下。

色情刷单诈骗：主要指通过通过色情网站、短信、交友软件等发布虚假信息，诱导受害者完成指定刷单任务的诈骗。

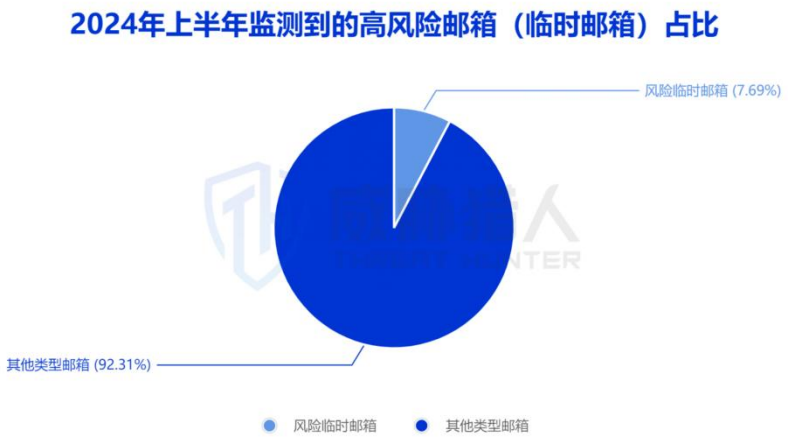
卡号资源买卖诈骗：主要指通过出售或者租借卡号协助黑产洗钱的诈骗，风险大小主要取决于黑产用途。



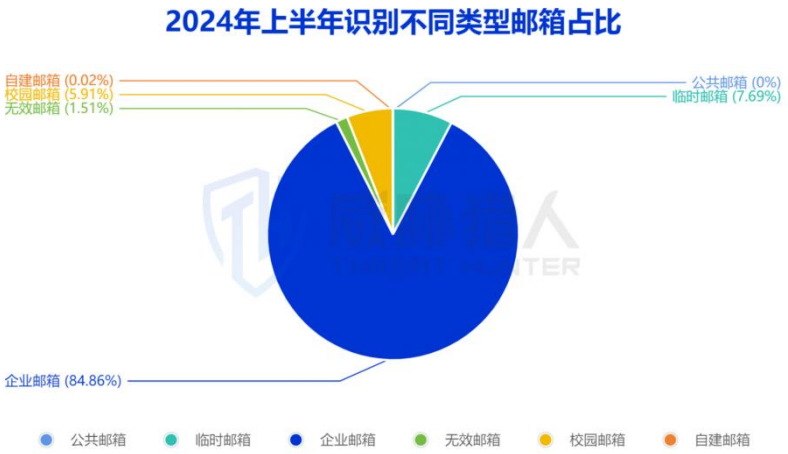
2.4 2024 年上半年风险邮箱资源分析

2.4.1 2024 年上半年风险邮箱资源变化

（1）2024 年上半年监测识别高风险邮箱（临时邮箱）占总量 7.69%

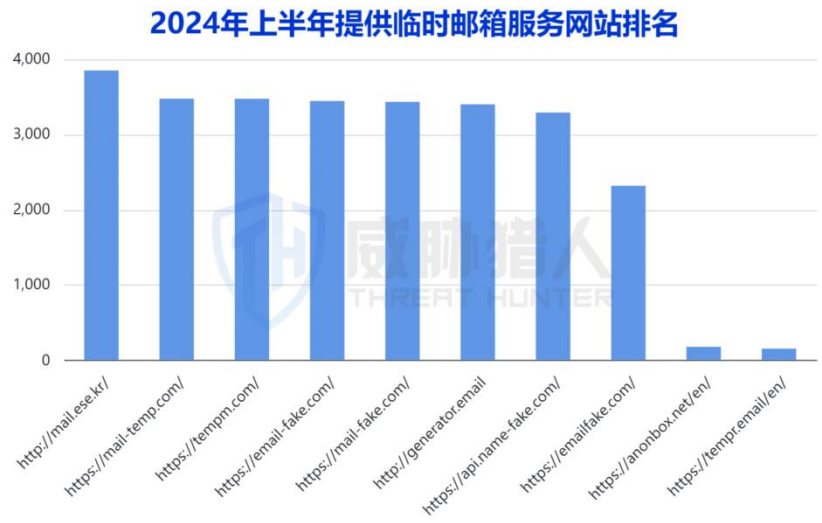


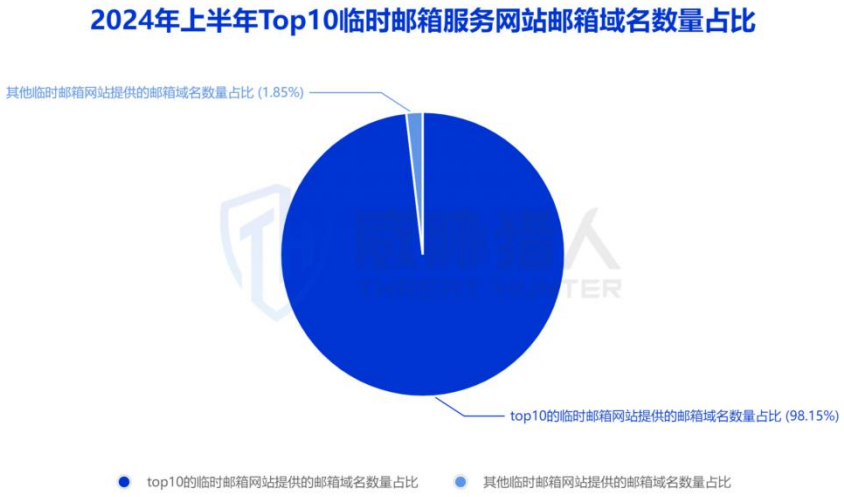
从 2024 年上半年每月不同类型风险邮箱的监测识别数量来看，2024 年上半年识别风险邮箱 35666 个，其中识别为低风险企业邮箱占总量 84%以上，高风险邮箱（临时邮箱）占比 7.69%，新增邮箱主要集中在企业邮箱。



（2）2024 年上半年，98.15%以上的邮箱域名数量来自 Top10 提供免费临时邮箱服务的网站

在风险邮箱方面，2024 年上半年我们监测发现了 8804 个临时邮箱域名，而提供免费临时邮箱服务 Top10 的网站，贡献了超过 98.15%的邮箱域名数量。





03

2024 年上半年
黑产通用型攻击技术分析

三、2024 年上半年黑产通用型攻击技术分析

3.1 黑产利用 LSPatch 技术实现快速抢单作恶，被高频利用于金融、社交、房产等平台 APP

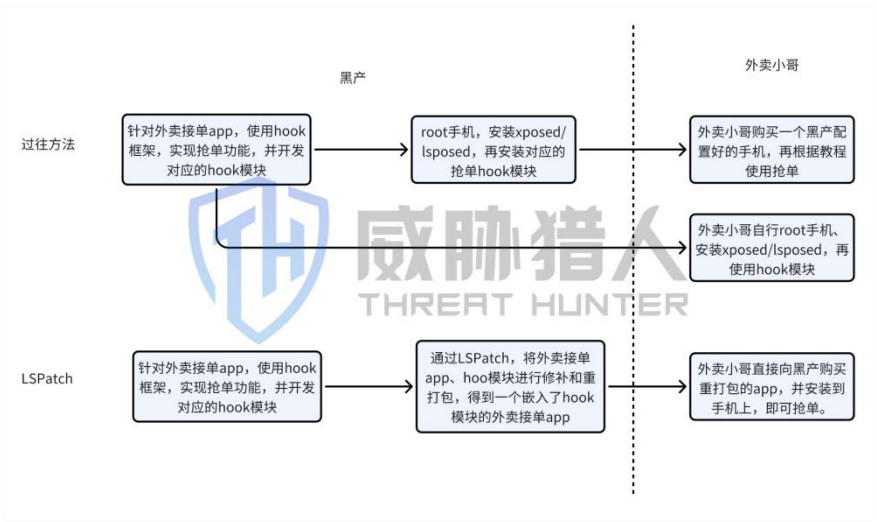
威胁猎人研究发现，2024 年上半年，不少黑产利用一款名为“LSPatch”的技术工具实现“快速抢单”作恶，同时在金融、社交、房产、本地生活等多个行业的 APP 发现了利用 LSPatch 技术快速抢单的恶意行为。

LSPatch 本质上是一款免 Root 使用 Hook 框架模块的技术，借助该技术，使用者能在非 Root 手机上使用 Hook 框架模块，实现 hook 手机系统函数，并对函数整体执行逻辑进行修改。通过该工具，黑产将具体的作恶环境及作恶工具打包到被攻击的 app，让使用者直接安装注入了恶意工具的虚假 app，即可进行快速抢单，极大降低了使用者的工具使用门槛。

在传统的 Xposed 或 Lsposed 框架中，用户通常需要获取 root 权限才能安装和使用各种模块，以实现对手机应用的个性化定制和系统优化，这一过程对于不熟悉技术的用户来说，不仅操作门槛高，还存在“手机变砖”的风险。Lspatch 的出现，无疑为这类用户打开了一扇新的大门，无需 root 权限，用户便能轻松体验到 Xposed 模块带来的强大功能。

工具	运行设备环境	使用方式	特点
LSPatch	正常手机设备	直接安装APP即可	使用门槛低，直接安装即可
Xposed	Root手机设备	（1）Root手机 （2）安装Hook框架 （3）启动Hook模块；	（1）存在一定使用门槛，需对设备进行root （2）不稳定，root过程中，手机可能会变砖；
Lsposed	Root手机设备		

以本地生活 APP 为例，黑产通过 LSPatch 技术在外卖接单 APP 内嵌入 hook 模块，从而使该 APP 具备自动抢单功能，一个外卖小哥只需要向黑产购买“外卖接单 APP”，并进行正常安装，即可进行自动抢单，外卖小哥的抢单门槛、花费均出现极大的下降。利用 LSPatch 技术的抢单工具与过往抢单工具的对比如下：



3.2 黑产利用 HID 设备进行自动化攻击，作恶更加隐蔽、监测难度大幅提升

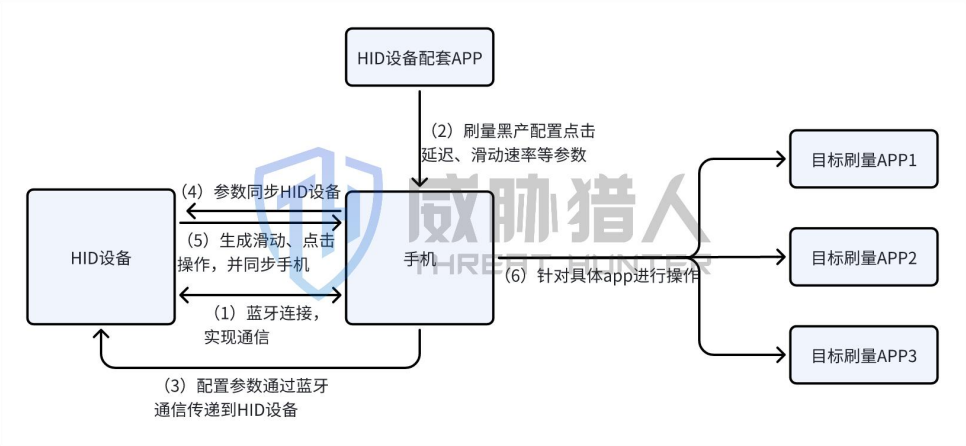
威胁猎人研究发现，除了按键精灵、auto.js pro 等自动化脚本工具外，2024 年上半年黑产利用 HID 设备进行自动化操作攻击的行为更加频繁。随着技术的发展，大部分 HID 设备开

始支持蓝牙协议的方式进行传输，使黑产可以通过“HID 设备+蓝牙协议的方式”实现简单的滑动点击操作，其中最受黑产关注的则是“短视频刷量”这一场景。

HID（Human Interface Device，人机接口设备）是 USB 设备中常用的设备类型，是直接与人交互的 USB 设备。键盘、鼠标等设备都是日常生活中最常见的 HID 设备。由于 HID 设备在软件层面并无明显的特征，使得使用该类设备进行攻击的行为更加隐秘。

以短视频刷量场景为例，短视频刷量的第一步是养号，而养号需要帐号进行不断的观看某一类型的视频，让平台的推荐算法完成对帐号的标签标记。为实现短视频刷量中自动化点击，同时尽量绕过平台风控，黑产团伙除了基于基于手机开发者权限、手机 root 权限实现自动化点击外，也有不少黑产“基于 HID 备进行自动化点击”。

以威胁猎人最近分析的一款“基于 HID 设备实现自动化点击”工具为例，主要运行流程如下：



“基于 HID 设备实现自动化点击”的方法通过代码控制硬件，硬件发送 HID 指令，实现具体的点击活动操作，与目前主流的基于代码、ADB 操作设备点击的自动化点击实现方法不同；且该方法无需配置特定环境（如开发者权限、root 环境），这使得大部分平台已有的自动化点击风控规则在识别该方法上，可能存在失效的情况，进一步增加了平台方的检测成本。

04

2024 年上半年
黑产攻击场景分析

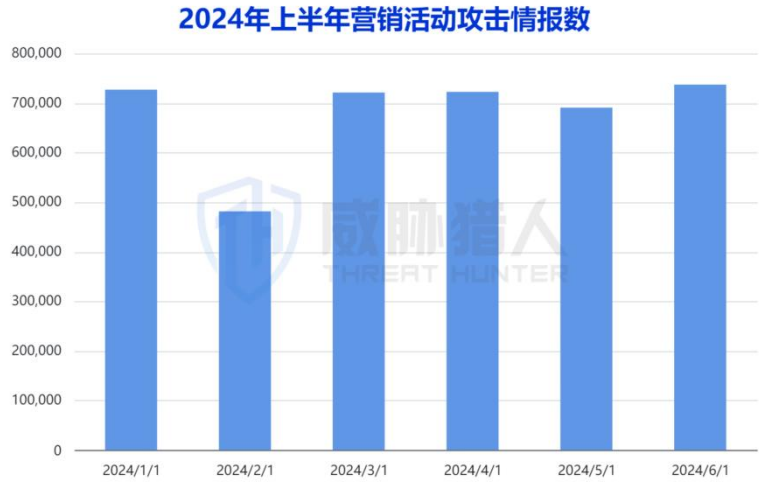
四、2024 年上半年黑产攻击场景分析

4.1 营销欺诈场景分析

4.1.1 营销活动

（1）营销活动攻击情报 408 万条，涉及作恶黑产群组 8000 个

2024 年上半年威胁猎人共捕获营销活动攻击情报 408 万条，监测到活跃的作恶社交群组 8000 个，涉及作恶黑产人数达 6.5 万名，整体较 2023 年下半年均有所下降。2 月份情报量下降，主要受春节期间黑产交易放缓的影响，节后攻击情报量逐渐回升。



（2）大量黑产针对电商平台特殊商品进行恶意赔付，有黑产表示“赔付一单够吃半年”

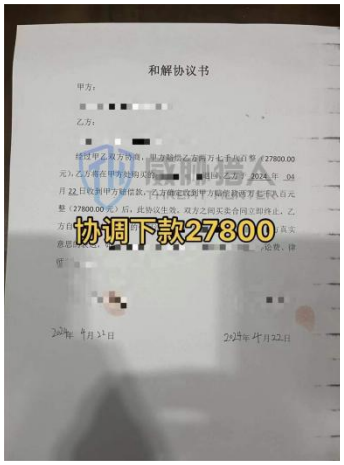
电商平台快速发展之下，不少电商平台通过客户无理由退货等宽松的退货规则，有效提升平台流量及竞争力，这一规则在无形中被黑产发掘并利用，利用平台规则进行恶意赔付的黑灰产群体不断壮大。

2024 年 4 月，威胁猎人情报平台监测到大量号称“超级维权”的黑产攻击行为，1 月份仅有零星黑产广告，4 月份讨论量增长至近 200 条。深入挖掘发现，不少黑产以“赔付一单够吃半年”的高额赔付，吸引更多黑产团伙对电商平台及相关商家发起攻击，假借“维权打假”名义进行恶意赔付及攻击的事件不断涌现。

与过去常规的“三无”、“打假”、“不发货”等赔付思路不同，“超级维权”指的是黑灰产锁定平台上售卖“有毒有害”的商品，进行药品检测和出具报告，提起行政复议、行政诉讼、信访，威胁商家进入协商调解赔付，甚至最终获得法院执行款，赔付流程涉及国家的公权机构，整体审核周期较长，小中高额赔付所需要的时间不等。

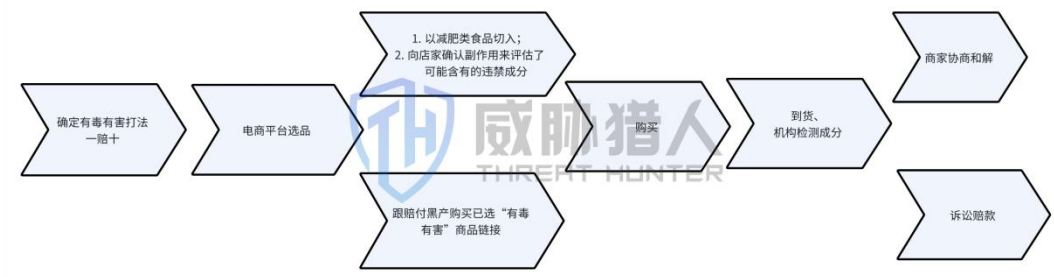
为了成功获取赔偿，赔付黑产表示有货源团队、接货检测团队、法务团队等全程陪跑，来招揽愿意付出本金和“上车费”的用户进行教学赔付，这也是“超级维权”赔付玩法升级之处。

主打商品类型包括：他达拉非（性功能障碍药品）、西布曲明（减肥类）、麻黄碱（减肥类），基本都是需要医生开处方类型药品或为国家食品药品监督管理局禁止添加成分，如产品包含即构成违反法律。



序号	检验项目	检测方法	单位	标准值	检测结果	单项判定
1	麻黄碱	BJS 201710	g/kg	/	0.920	/
备注	/					

主要赔付流程如下：



（3）黑产利用“锁单”方式联合用户套现银行立减金，作恶行为分工更加精细化

近年来，平台用户与黑灰产针对平台优惠活动联合套现的事件频繁发生，用户正常领取权益，

领取权益后黑灰产团伙进行套现，并按比例与用户分配变现利润，减少黑产团伙寻找变现买家或“被迫消费”的额外成本。这种联合套现进一步体现了对资源的高效利用，以及作恶行为的精细化分工。

不少银行机构每月或每周会推出支付立减金活动，这类活动一直是黑灰产和羊毛党高度关注的掘金项目。指定银行的大额立减活动中，黑灰产团伙和银行用户的高度协作套现分利润的行为更加猖獗，利用支付后锁单套取优惠的手法逐渐在电商平台广泛使用。

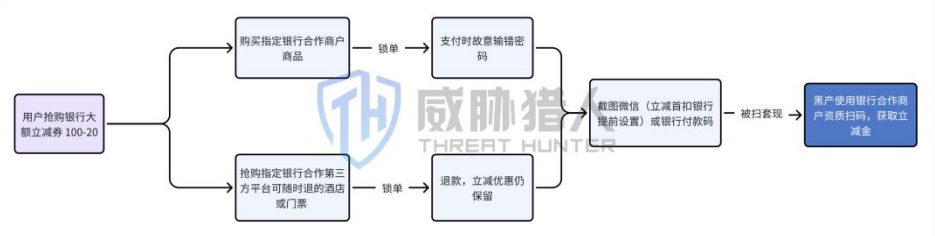
2024 年上半年，威胁猎人监测到大量黑产利用银行支付规则漏洞，通过“锁优惠”、“锁单”等与用户联合套现，具体流程及手法如下：

1、联合容易抢得银行立减金的商户下单，支付阶段故意输错密码来锁住优惠名额；

2、购买可随时退款商品（如门票或酒店）锁住本单优惠，退款后保留当月立减资格；

3、套现阶段，用户向黑产提供付款码，由黑产套取银行立减金，黑产再返回支付金额和部分立减金，与用户瓜分利润，与用户联合锁单的手法，让黑产攻击具备了充分的套现操作时间。

举个例子：某用户锁单“满 100 减 20 券”后，向黑产出示付款码，黑产利用相关资质进行扫码并扣除 100 元“订单”，用户最终支付 80 元，黑产获得 100 元，并私下返回用户 90 元，通过该套现手法，黑产与用户各获得 10 元立减优惠，银行则损失了 20 元立减权益。



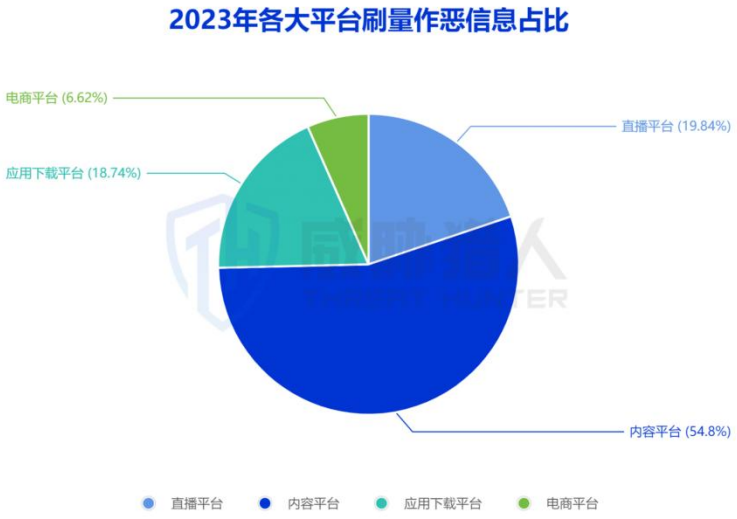
4.1.2 内容刷量

（1）内容刷量作弊情报 51 万条，涉及刷量的作恶群组 3977 个

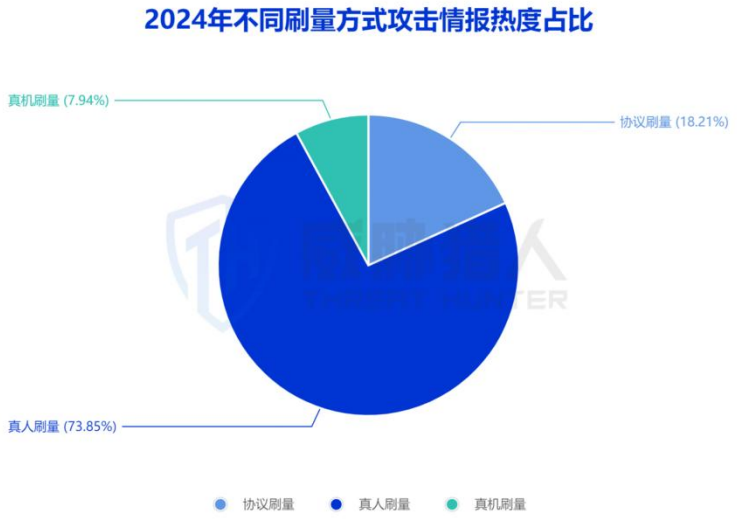
在 2024 年上半年，刷量作弊的情况依然严峻，威胁猎人安全团队在此期间监测到涉及直播平台、内容平台、电商平台以及应用下载平台的刷量作弊情报共计 51 万条。此外，监测到涉及刷量的活跃社交群组 3977 个，参与这些黑产活动的人数达到 9014 人。

（2）内容平台、直播平台遭受刷量攻击占比超 75%，真人作弊刷量仍是主流刷量方式

威胁猎人针对各平台发布的刷量作恶情报进行持续监测，发现 2024 年上半年，内容平台及直播平台遭受刷量攻击最为严重，刷量相关作恶信息占比超总量的 75%，主要体现在内容平台浏览量、评论及分享刷量，直播平台人气互动、上榜和礼物代刷等。



从刷量手段来看，真人作弊刷量仍为主流刷量方式，威胁猎人监测到，真人作弊相关情报占刷量情报总量的 74%。随着各大平台对恶意刷量行为的识别技术不断更新，许多刷量工作室已从使用协议刷量和基于真实设备的群控刷量转向采用真人刷量的方式，进一步满足平台对真实有效流量的要求，这种转变反映了平台对技术手段刷量的有效打击。



（3）“自然流刷量”等直播间新型刷量手法的应用更加普遍

数字媒体快速发展之下，直播带货已成为商业销售的一种重要模式，效果难预测、流量不稳定等问题给许多直播商家带来困扰，由于平台付费推流价格高昂，黑产团伙开始盯上自然流量刷量的商机。

直播平台自然流量的推荐机制意味着，只有特定标签用户进入直播间进行点赞评论等刷量行为才会成为高质流量，于是更精细化的真人刷量方式随之产生。

自然流量也称“推荐 feed 流”，指持续更新并呈现给用户的内容信息流，直播间自然流量的种类包括但不限于：

1.直播广场流量：通过直播间的粉丝点赞、设置吸引人的封面和标题，实现从直播广场引流的流量；

2.同城流量：利用同城定位功能，开播时打开同城定位，吸引同城的人刷到你的直播；

3.搜索流量：通过个人主页、搜索、订单中心等来源的流量，虽然占比不大，但也是自然推荐流量的一种。

2024 年上半年，威胁猎人观察到“直播广场刷量”等新型自然流刷量手法的应用更加普遍。以“直播广场刷量”为例，为了有效提升直播间热度，使其成为直播广场推荐流量，黑产利用大量手机账号及云控软件进行直播间刷量，具体行为包括：

1、提前“养号”：提前对刷量账号进行养号，刷同类型内容模拟目标用户群体，使后续直播间流量推荐更加精准；

2、推流至直播广场：通过操控大量账号，关注主账号并观看短视频 20 分钟以上，后续使直播间被推流至直播广场，获得更大的流量；

3、进入指定直播间进一步刷量：再次利用云控软件批量控制手机账号，进入指定直播间进行关注、点赞、评论、亮灯牌等一系列操作，进一步增强直播流量的真实性及活跃度。

在云控软件的操作下，几百甚至上千账号瞬时涌入指定直播间，原本无人问津的直播间忽然人气暴涨，顺势吸引更多“野生”流量，整个流程“预判”了系统对用户喜好的推送，实际上大部分是虚假流量。

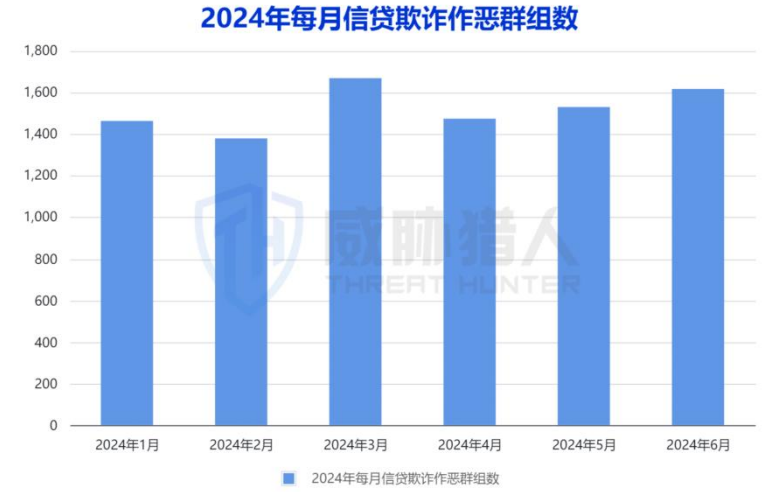
这类刷量方式流程繁琐、成本较高，威胁猎人深入调研了解到，这类模拟自然流量的刷量方式，其单个账号可在 5 元以上，是普通真人刷量账号价格至少两倍以上，这也反映了直播行业对“真实流量”的需求日益增长，与此同时平台对各类刷量手法的风控日益增强。

4.2 金融欺诈场景分析

（1）2024 年上半年信贷欺诈攻击情报 46 万条，监测到活跃作恶群组 2700 个

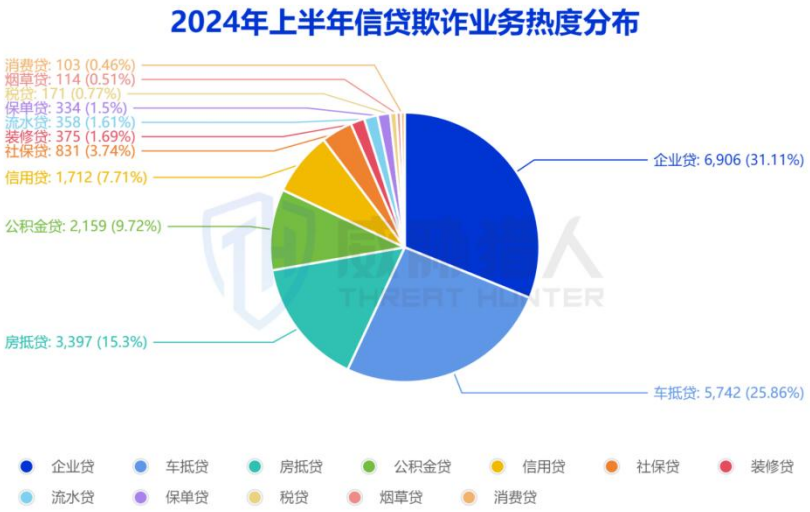
2024 年上半年，威胁猎人共捕获信贷欺诈攻击情报 46 万条，监测活跃的作恶社交群组 2700 个，涉及作恶黑产 1.4 万名。


2024年每月信贷欺诈情报数
100,000
80,000
60,000
40,000
20,000
0
2024年1月
2024年2月
2024年3月
2024年4月
2024年5月
2024年6月
2024年每月信贷欺诈情报数


2024年每月信贷欺诈作恶群组数
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
2024年1月
2024年2月
2024年3月
2024年4月
2024年5月
2024年6月
2024年每月信贷欺诈作恶群组数


2024年每月信贷欺诈作恶黑产数
6,000
5,000
4,000
3,000
2,000
1,000
0
2024年1月
2024年2月
2024年3月
2024年4月
2024年5月
2024年6月
2024年每月信贷欺诈作恶黑产数

从贷款产品类型来看，2024 年银行业信贷欺诈热度 TOP5 的贷款产品类型分别是：**企业贷、车抵贷、房抵贷、公积金贷和信用贷。**



从地域分布情况来看，2024 年上半年银行业信贷欺诈地区热度排在 TOP5 的地区是：**山东、浙江、河北、重庆、北京。**

（2）伪造包装“企业主”等虚假身份进行背债骗贷，伪造手法更加丰富逼真

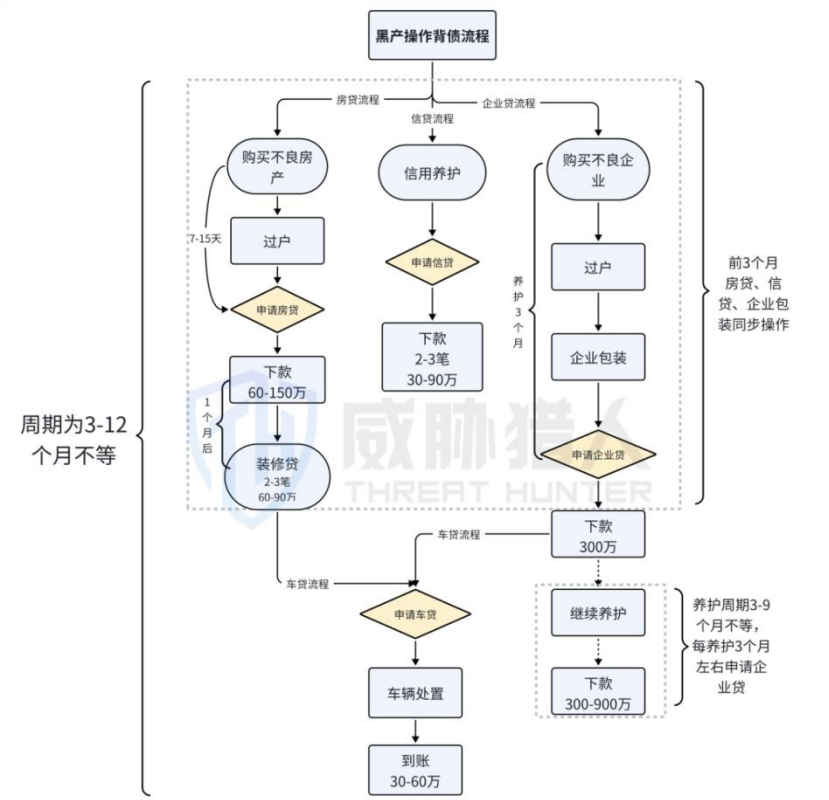
背债人往往是那些征信记录清白、急需大量资金却没有还款能力的人，通过对这些人进行个人资产情况等虚假包装，从银行套取高额贷款，获取几十甚至上百万的利润，所付出的代价是抛弃自己的征信，面临法律的制裁。2024 年 7 月，我国失信执行者达 833 万人，其中不乏大量职业背债人。

由于背债风险事件频发，引起了银行等金融机构的高度重视，针对背债骗贷行为的风控政策更加严格。为了最大限度获取利益，同时避免受到相关机构打击与法律制，相关黑产对于背债人的身份包装及材料伪造更加逼真，用接近“真实”的手段提升骗贷成功率。

为避免银行风控，确保利益最大化，黑产中介会给背债人包装“工作者、户主、企业主”等各种虚假身份，作为申请贷款的增信条件，具体手段包括给背债人真实缴纳社保、公积金、过户房产/企业、真实开票纳税、真实租赁经营场景等等。

通过一系列包装准备，黑产中介将利用背债人的各项资质，进行“房贷、信用贷、企业贷、车贷”一条龙大额融资，据了解，一个背债人骗贷总额高达 500-2000 万元不等，实际到手金额为背债总额的 40%-60%。贷款成功后，为避免被发现并被定性为诈骗，不少黑产中介不惜提高骗贷成本，帮助/叮嘱背债人还款半年甚至两年。

黑产操作背债骗贷的具体流程如下：

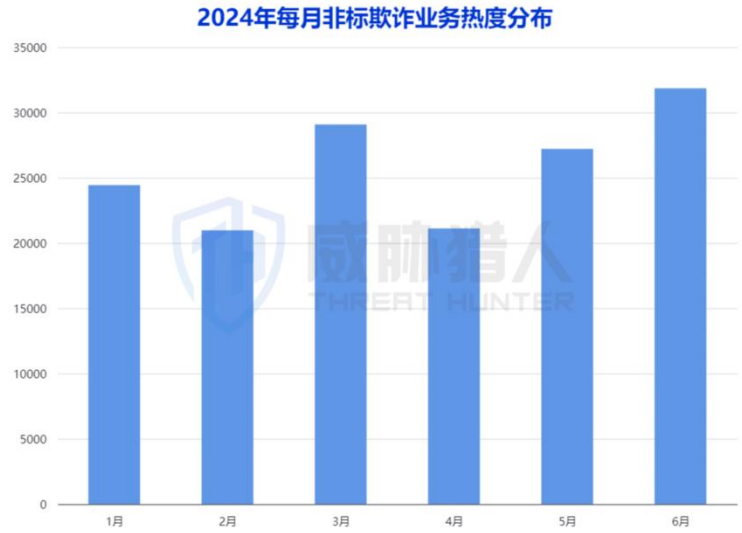


（3）2024 年上半年非标贷款的欺诈业务活跃，非标贷款相关话题热度增长近 10%

非标贷款：指客户达不到常规贷款的标准条件，黑产中介通过包装材料、美化数据、关系进行骗贷的行为。

2023 年下半年非标相关话题讨论量级达到 140780 条，2024 年上半年非标热度总值为 154685，增长率为 9.9%。

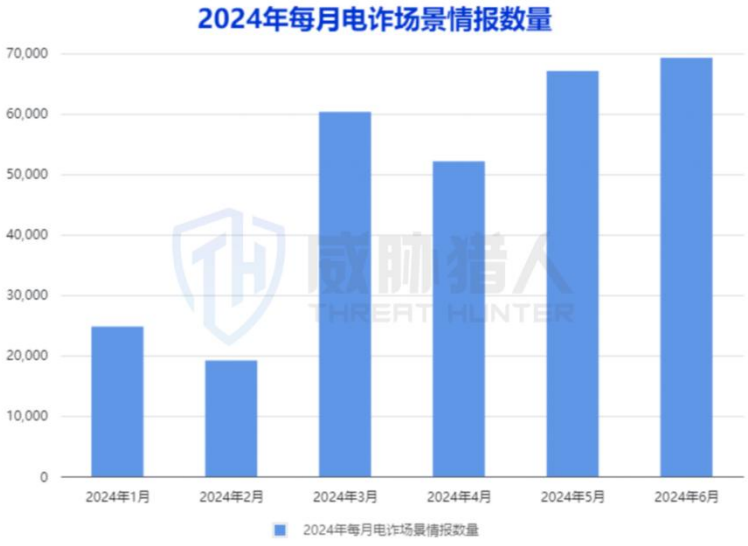
在近几年经济下行的影响下，企业、经营者、个人普遍存在收入降低、高负债等困境，使得一些企业、经营者、个人现有的资质条件不满足金融机构的放款要求。黑产、中介通过虚假流水（个人、企业）、科技提额、融车套现、虚假装修贷套现、以租代购套现等，以虚假材料、虚假需求通过审批、提额系统，实施欺诈，使得非标业务持续活跃。



4.3 电信网络诈骗场景分析

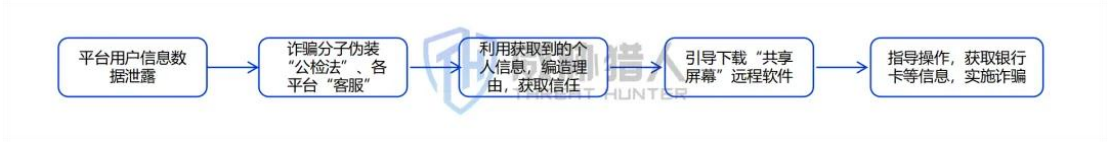
（1）2024 年上半年电信诈骗攻击情报 29 万条，监测到活跃作恶群组 10187 个

2024 年上半年，威胁猎人风险情报平台监测到电信网络诈骗相关情报 29 万条，活跃作恶社交群组 10187 个，涉及作恶黑产 1.7 万名。



（2）利用各类远程会议软件“共享屏幕”诈骗的事件高发

2024 年上半年，利用远程会议软件“屏幕共享”功能进行诈骗的事件频繁发生。诈骗分子通过一些非法渠道获取乘客个人及相关业务信息，冒充航空公司、保险机构等工作人员，通过一些特定话术（如“退费”“理赔”“改签”等为由），诱导受害人安装远程会议软件，并打开“屏幕共享”功能，以此获取到受害人的短信验证码，甚至是支付密码等，最后成功盗刷受害人的银行卡，或者成功诱导受害人把钱转到指定账户，具体流程如下：



举一个真实的案例：

李某接到陌生来电，冒充某航空公司的“客服”告知其航班需要改签同时会进行相关赔偿，要求李某点击某线上会议链接开启屏幕共享，由于对方能准确说出自己的航班信息，李某信以为真，按照其要求进行了屏幕共享的操作。

此时诈骗者利用该功能趁机获取李某个人信息，并以进行身份认证、解绑银行卡为由，要求李某提供自己的银行卡号、密码、手机验证码等信息，并进行人脸识别，最终李某银行卡里的 30000 元被对方全部转走。

以下是从电诈场景中挖掘的远程会议名称汇总：

电诈团伙使用的远程会议名称汇总	
黑产开发的远程会议软件	小艺宝、拓课宝、展讯通、会讯通、企业云、全视通、云办公、云会议、软视通、佳讯通、微易云、畅联云、微易宝、微会议、云信会议、轻会议、众会议、天翼云、音会议、恒顺宝、云服务、星客宝、Vymeet、诸视云、鸿雁视频会议、onRoom、昆仑云会议、威讯云会议、开会宝、云会通
应用商城直接搜索的远程会议软件	zoom、teams、webex、[redacted]anydesk、AirDroid Cast

（3）黑产开发各类远控软件并将其伪造成常用 APP，大幅提升诈骗成功率

在杀鱼诈骗的过程中，诈骗团伙会通过诱导受害人安装远控软件（如 ready.apk），黑产通过将这类软件伪装成正常的 APP（如**反诈中心 APP** 等），套取受害人的信任，使其放心开

启无障碍服务授权，从而控制受害人手机并采集手机信息，远程操控手机进行转账，成功盗刷受害人的银行卡，或者成功诱导受害人把钱转到指定账户。

仿冒成各类日常应用的“远程控制”APP，黑产在后台操控受害者手机，使不少受害者完全无法察觉、难以防备，极大提升了黑产团伙的诈骗成功率。2024 年 3 月，连云港的张某在家中玩手机游戏和平精英时认识一陌生人以送皮肤的方式，被通过“ToDesk”APP 控制手机，通过手机银行充值未知游戏账号 7 次 648 元和平精英套餐，损失人民币 4536 元。

为了诱导受害人下载安装远程控制软件，黑产团伙会针对不同人群及心理特点设计不同的手法和话术，受害者往往在毫无戒备心、获取“回报”的情境下完成下载，堕入骗局。

部分推广话术如下：

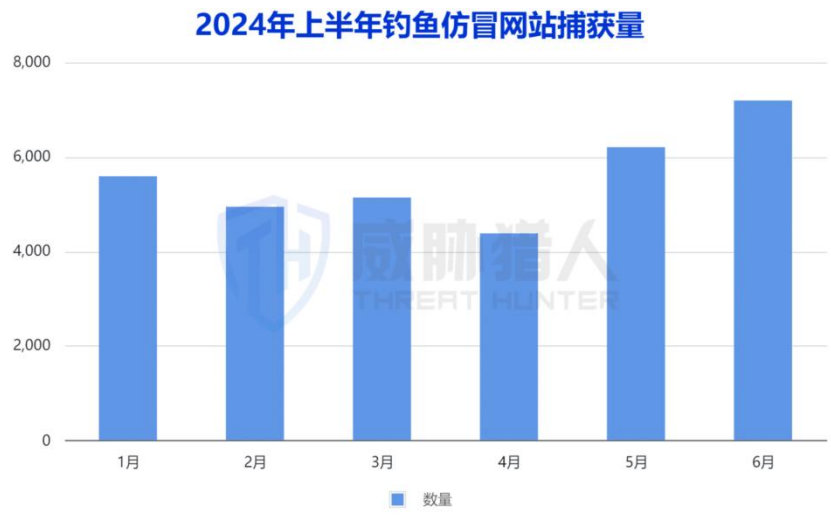
推广对象	手法及话术
朋友	跟身边的朋友试着多聊聊家常，然后以开玩笑的方式让朋友去下载软件
游戏平台用户	在游戏平台发布免费领取皮肤或账号买卖的广告，当游戏平台的用户主动联系领取皮肤或账号交易时，告知对方需要有反诈APP软件在手机上才可以交易，如果互相有欺诈行为反诈APP软件会有提示，这样就可以让用户掉以轻心地去下载
有贷款需求的人群	联系有贷款需求的用户，简单聊天以后直接告诉他，这边需要查看信誉分，让对方下载国家反诈APP，再去截图信誉分，这样一般对方都不会怀疑
路人	投资100-200元去买一些小礼品，然后在路边遇到人就这样说：“帅哥\美女，你好我们是单位出来实习的，我们的单位是销售部门领导我了考验我们的能力，让我们出来推荐一下国家反诈APP，不管新老用户都可以参加的，你看你这边能不能帮我完成一个任务，完成任务以后我们会有一个精美小礼品赠送。”

4.4 钓鱼仿冒场景分析

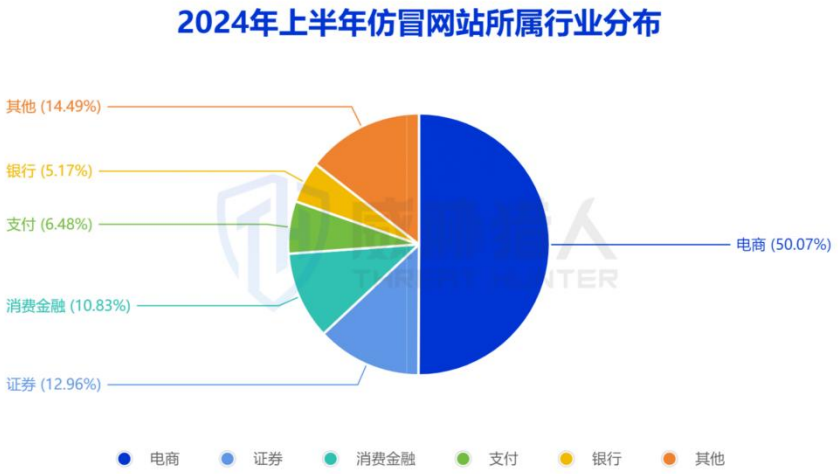
（1）2024 年上半年监测钓鱼仿冒相关事件 33453 起，涉及 243 家企业

2024 年上半年，威胁猎人共监测到钓鱼网站及仿冒 APP33453 例，涉及 243 家企业，较 2023 年下半年监测总量下降 8.97%，整体保持增长趋势。此类网站及 APP 都是通过仿冒

正常网站及 APP，获取用户信任并骗取用户的个人信息及钱财。



（2）遭受钓鱼仿冒情况最为严重的 Top3 行业：电商、证券、消费金融



从上半年的行业分布数据来看，钓鱼网站仿冒行业占比 TOP3 为电商、证券行业和消费金融行业，其中电商行业超过金融行业，成为遭受钓鱼仿冒攻击最为严峻的行业，电商行业仿冒案例占总量的 50%以上。

针对电商行业相关仿冒数据研究发现，主要有以下三个特征：

1、电商行业的仿冒网站通常以仿冒购物商城平台的形式出现；

2、仿冒电商平台一般会有 1-4 种仿冒模版，模版完整地仿冒了现购物商城必备的网页端、APP 端下载界面、客服系统和商城管理后台，仿冒效果十分逼真；

3、黑灰产团伙倾向于批量注册同一仿冒网站作恶，广撒网的同时，最大限度绕过风控。主要体现在，一般黑产团伙设置的仿冒网站二级域名和 URL 路径一致之外，域名注册时间基本一致。

（3）投资盘诈骗多发，以仿冒“证券”行业网站为主

经济下行时期，不少人想要通过有效投资在短期内快速获益，黑产利用这类人群想要短期获益的心理进行投资盘诈骗，投资盘诈骗类型主要攻击金融行业，其中以仿冒证券行业网站最为普遍。

投资盘：主要指以仿冒投资属性较强的金融行业企业为目标的仿冒网站或 APP

“投资盘”主要流程及角色分工如下：

上游黑产搭建仿冒网站：黑产一般会在源码平台购买仿冒网站的源代码，并安排开发人员部署仿冒目标网站的环境；

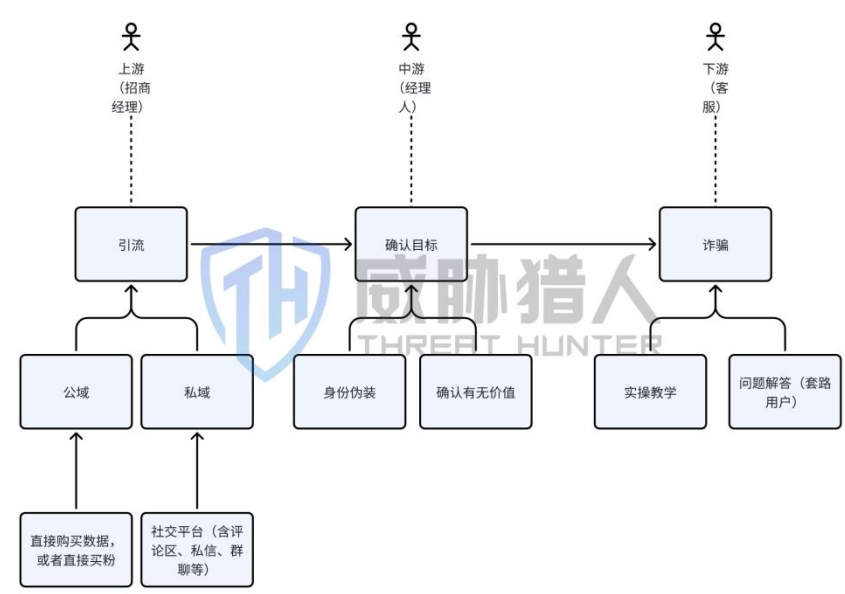
上游“招商经理”引流获客：通过购买目标人群数据，或者通过主流社交平台及短视频平台

进行引流获客；

中游“经理人”联系目标客户：以某公司回馈客户、介绍理财产品、活动邀约等话术联系目标用户。“经理人”一般会在社交软件上打造精英人设，增强可信度来减少受害者的防备心理。

下游“投资平台客服实施诈骗：即进行诈骗操作的人，证券行业仿冒网站通常涉及资金投入、提现等操作环节。

“投资盘”中，黑产通常会设定具体规则，例如将初始资金投入设定为 10 万元，封盘资金为 50 万，在未封盘前用户可以随意在盘口进行操作，如投资、提现等，进一步套取用户信任，待用户投入资金达到 50 万，黑产将取消用户提现并跑路。

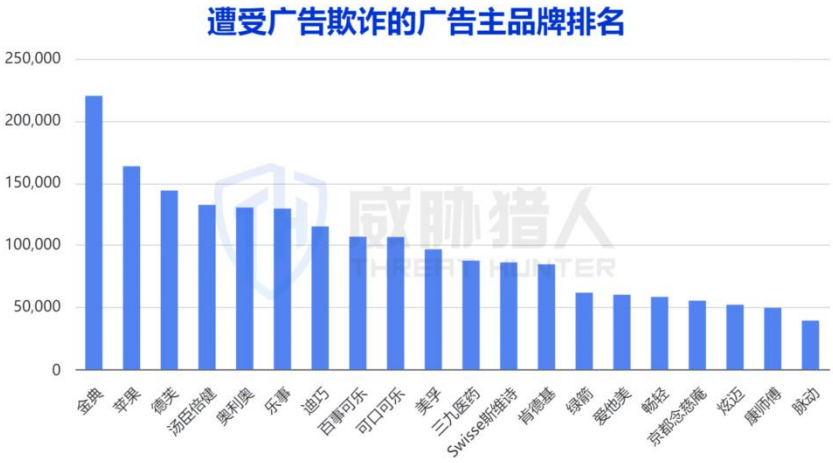


4.5 品牌广告欺诈场景分析

（1）遭受欺诈的品牌广告主中，食品饮料类成为遭受广告欺诈占比最大的广告主

威胁猎人基于广告暗刷流量监测捕获到大量广告欺诈数据，涉及到多个行业，食品饮料类成为遭受欺诈占比最大的广告主。

遭到广告欺诈的广告主品牌排名如下：

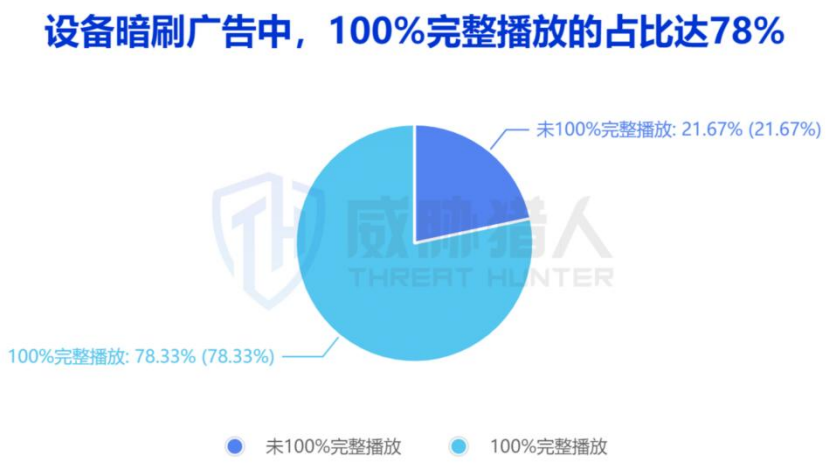


（2）从欺诈广告形式来看，100%播完欺诈广告占比达到 78%

从捕获数据中的欺诈广告形式来看，欺诈广告中以 15 秒的视频广告为主，这类广告占捕获欺诈广告总量的 99%以上。

从欺诈广告的播放情况来看，设备暗刷伪造并上报的广告中，大部分都是完整播放完毕的，100%播完的占比达到 78%，这一数据明显不符合正常用户的行为，现实情况下有耐心将广告看完的用户并不多。

视频广告包括开始播放、播放中、完成播放等阶段，不同阶段都会进行广告追踪，并将流量上报至广告监测平台，实际上这些广告并未播放，仅仅是通过设备暗刷伪造了虚假的广告播放情况，并将虚假追踪情况上报。



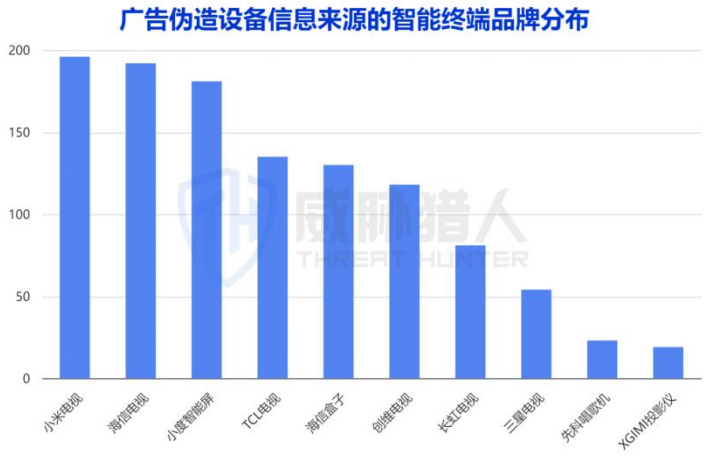
（3）品牌广告伪造的终端情况

在广告欺诈刷量的作弊链路中，上报的作弊广告流量往往会包含动态变化的伪造设备参数信息，模拟真实的设备信息及其展现广告的数据情况，以欺骗广告主。

威胁猎人针对伪造的广告播放数据进行分析发现，伪造并上报的虚假广告数据里，覆盖了三大类终端：

广告伪造的移动端中包含了手机及平板，其中以手机为主，覆盖以下多个手机品牌：

广告伪造的互联网智能终端中，包含了智能电视、电视盒子、智慧屏、智能音箱（带屏）、唱歌机、投影仪等智能终端品牌：



4.6 数据泄露场景分析

（1）2024 年上半年数据泄露事件共计 16011 起，较 2023 年下半年增长 59.58%

据威胁猎人数据泄露风险监测平台数据显示，2024 年上半年（1-6 月）全网监测到的 1.1 亿条情报中，基于真实性验证引擎及 DRRC 人工分析验证有效的数据泄露事件共计 16011 起，较 2023 年下半年增长 59.58%，9539 起。

威胁猎人发现，在 2024 年 2 月数据泄露事件量出现大幅下降，较 2024 年 1 月下降 36%（898 起），进一步分析了解到，主要有以下两个方面所致：

从数据泄露源头来看，第三方泄露、短信通道泄露等不同原因所引发的数据泄露事件量均在2024 年 2 月出现下降的情况，可以看出主要是受到春节期间黑产放假带来的交易行为放缓的影响。

从贩卖数据（中间商）的黑产团伙数量来看，2024 年 2 月非法数据交易黑产团伙数量出现下降。

（2）银行、电商、消费金融成为数据泄露事件数量 Top3 行业，银行事件数量 2961 起位列第一

从行业分布来看，2024 年上半年数据泄露事件涉及 85 个行业，1524 家企业，数据泄露事件数量 Top5 行业分别为银行、电商、消费金融、保险、快递。其中，银行行业数据泄露事

件数量高达 2961 起，成为数据泄露事件数最多的行业。

2024 年上半年 TOP10 行业排名变化情况如下：

行业	2023年下半年排名	2024年上半年排名	排名变化
银行	2	1	↑1
电商	5	2	↑3
消费金融	1	3	↓2
保险	4	4	-
快递	3	5	↓2
在线票务	7	6	↑1
证券	8	7	↑1
汽车品牌	9	8	↑1
支付	6	9	↓3
本地生活	15	10	↑5

排名靠前的数据泄露行业中以金融、电商行业为主，金融行业的数据泄露事件主要体现在银行、消费金融、保险等企业的客户信息倒卖，通常被下游黑产团伙用于精准营销及诈骗，因涉及大量高价值用户数据，且靠近交易环节，成为了个人信息泄露的重灾区。

近年来线上购物发展更加火热，据 2024 年 3 月发布的《中国互联网络发展状况统计报告》显示，截至 2023 年 12 月，我国网络购物用户规模达 9.15 亿人，占网民整体的 83.8%。线上购物的持续稳定增长下，电商平台产生了海量购物订单及物流信息，这些购物订单及物流信息由于暴露面较大，成为了黑产团伙的重点目标，同样被用于营销或诈骗。

同时，在公安部近期公布的“十大高发电信网络诈骗类型”中，刷单返利、虚假网络投资理财、虚假购物服务、冒充电商物流客服、虚假征信等 10 种常见的电信网络诈骗类型发案占比近 88.4%。

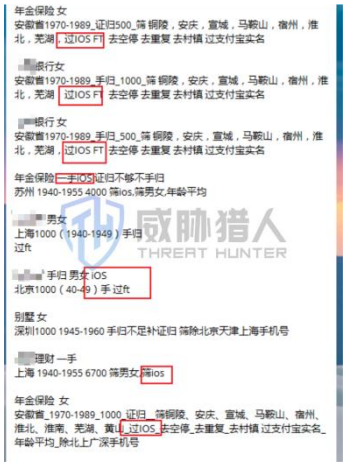
其中刷单返利类诈骗是发案量最大和造成损失最多的诈骗类型，虚假网络投资理财类诈骗的个案损失金额最大，虚假购物服务类诈骗发案量明显上升，已位居第三位，而金融、电商类用户群体正是此类诈骗案件的受害群体。

（3）2024 年上半年出现多起利用 Facetime 诈骗活动，“IOS”字段相关风险事件共 1237 起，较 2023 年下半年增长 8 倍

威胁猎人安全研究员发现 2024 年上半年泄露的数据中，“设备信息”字段信息出现频率逐渐增多，尤其是“IOS”类数据字段，从数贩卖黑产团伙与下游数据购买者的聊天记录来看，下数据购买者对于数据的复购要求中多次提及“IOS”设备数据的筛选要求。

0		订单号	姓名	身份证号	手机号	出生日期	年份	性别	保障到期	投保日期	公司分部		设备信息
9	某险创建订单	34	34 石	211	195	27/81	1981	女	2/2/24	232/3/23 0:		公	iOS
9	某险创建订单	90	60 潘	232	360	5/71	1971	女	4/25/24	24/26/23 (		支	iOS
9	某险创建订单	11	32 胡	230	458	/71	1971	女	7/25/24	27/26/23 (		支	iOS
9	某险创建订单	65	66 衣	210	097	0/80	1980	女	4/24/24	24/25/23 (		公	iOS
9	某险创建订单	60	41 王	220	008	/75	1975	女	10/4/24	210/5/23 (		公	iOS
9	某险创建订单	81	14 邢	210	332	4/70	1970	女	4/16/24	24/17/23 (		公	iOS
9	某险创建订单	25	35 朱	239	543	25/79	1979	女	2/21/24	22/22/23 (		支	iOS
9	某险创建订单	12	05 王	230	578	3/67	1967	女	7/14/24	27/15/23 (		支	iOS
9	某险创建订单	84	35 吕	220	707	5/75	1975	女	8/25/24	28/26/23 (		公	iOS
9	某险创建订单	77	04 顾	210	135	5/73	1973	女	1/6/24	31/7/23 0:		公	iOS
9	某险创建订单	55	74 单	211	210	5/69	1969	女	7/5/24	237/6/23 0:		公	iOS
9	某险创建订单	31	17 杨	211	083	4/70	1970	女	12/11/24	12/12/23		公	iOS
9	某险创建订单	92	21 牛	210	235	14/73	1973	女	4/14/24	24/15/23 (		公	iOS
9	某险创建订单	97	39 李	232	398	9/73	1973	女	6/12/24	26/13/23 (		心	iOS
9	某险创建订单	96	11 曲	220	511	5/79	1979	女	3/12/24	23/13/23 (		公	iOS
9	某险创建订单	80	28 姚	230	583	1/78	1978	女	7/1/24	237/2/23 0:		支	iOS
9	某险创建订单	49	84 杜	230	334	1/69	1969	女	12/26/24	12/27/23		中	iOS
9	某险创建订单	84	44 李	220	111	/76	1976	女	11/4/24	211/5/23 (		公	iOS

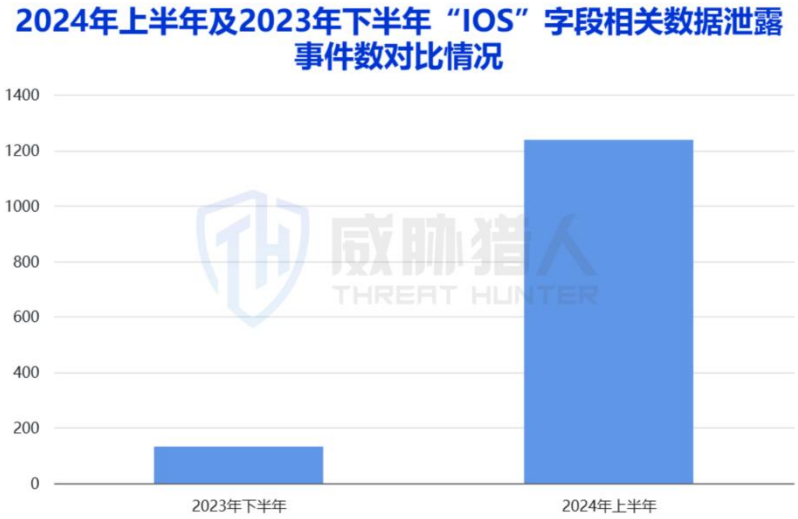
（威胁猎人捕获的泄露数据中包含设备信息）



（下游作恶团伙以及数据售卖方反馈需过 IOS、FT 等要求）

威胁猎人统计发现，2024 年上半年泄露的数据中包含“IOS”字段的相关风险事件高达 1237 起，较 2023 年下半年增加 8 倍。

随着国家公安机关对传统电话诈骗的打击加大、运营商监管加强，而 Facetime 日渐普及，不法分子开始盯上 Facetime 通话功能，试图通过这一功能实施诈骗活动。“IOS”类数据字段的大幅增加，以及黑产沟通验证，进一步佐证了利用 Facetime 进行诈骗的现状使得上游数据清洗产业链发展更加猖獗。



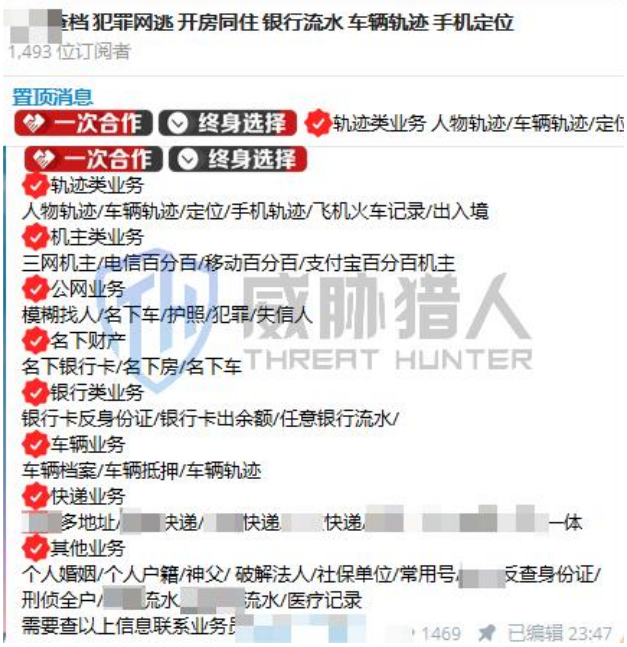
自 2024 年起，威胁猎人发现不少诈骗分子冒充“金融平台客服”、“国家征信中心工作人员”等身份，使用 FaceTime 功能向苹果手机用户发起通话，以“开通百万医疗保险需要关闭”、“有未结清的贷款需要处理”等为由进行诈骗，告知手机用户如不取消会被强制扣款，或个人征信受损，从而诱骗手机用户将相关款项转移至指定账户，给受害者带来巨额损失。

（4）2024 年上半年“查档”信息事件共 657 起，事件数呈现快速上升趋势

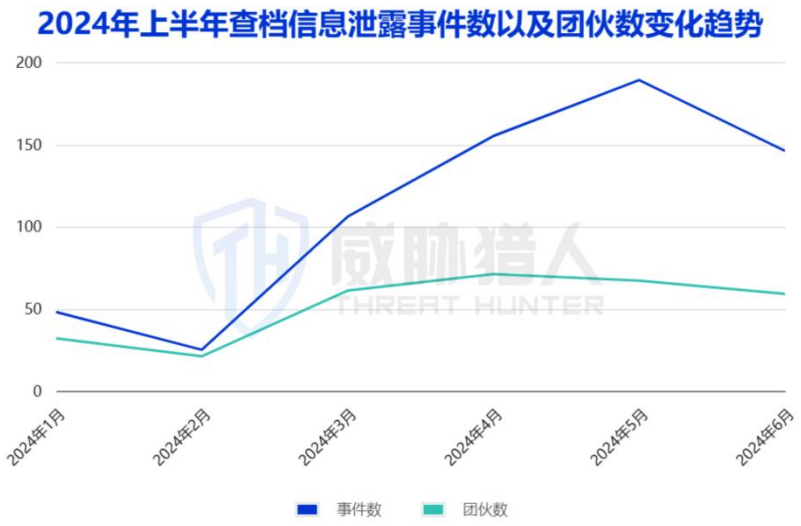
黑产在 Telegram 等渠道社工查档的事件屡见不鲜，例如通过一个手机号，就可以查询这个手机号相关的所有身份信息，如地址、银行卡号、名下资产等等。

查档：指提供对指定人员信息的资料档案进行调查或相关数据提取服务。

常见的查档服务有：轨迹类（人物轨迹、车辆轨迹）、名下财产（名下卡、名下车、名下房）、快递业务（快递地址、物流信息）、个人信息（婚姻、户籍、社保）等。



在 2024 年上半年发现的数据泄露事件中，威胁猎人累计发现 657 起“查档”信息泄露事件，占整体数据泄露事件的 4.10%。从每月变化趋势来看，查档类的相关风险事件数呈上升趋势，相关黑产团伙数量也不断增加。一定程度上反映出通过查档进行非法收益的形式更加普遍，背后收益更加可观。



05

总结

五、总结

2024 年上半年，网络黑产运作逐渐智能化和链条化，企业需要重点关注以下问题：

1、在攻击资源方面，2024 年上半年黑灰产资源除洗钱银行卡外，其余资源量级均呈现上升趋势

2024 年上半年风险 IP 数量较 2023 年下半年增长 44.8%，国内作恶手机号较 2023 年增长 8.8%，涉及洗钱银行卡新增数量有所下降，较 2023 年下半年下降 28%。

在攻击资源应用方面，黑卡物料资源标签更加丰富，如提供黑卡类别，业务信息、下机时间、标识号码“已筛选”等提升下游黑产筛卡效率、实现精准作恶；2024 年上半年黑产通过植入木马恶意使用正常用户 IP 的行为更加猖獗，“劫持共用代理”IP 攻击占总量 67%以上，成为攻击者主要使用 IP 类型。

2、在攻击技术方面，不少黑产利用 LSPatch 技术快速抢单作恶，基于 HID 设备的自动化攻击更加隐蔽

2024 年上半年，不少黑产利用“LSPatch”技术工具实现“快速抢单”作恶，在金融、社交、房产等多个行业的 APP 发现了利用 LSPatch 技术快速抢单的恶意行为。

此外，部分黑产开始利用 HID 设备进行自动化操作攻击，通过“HID 设备+蓝牙协议的方

式”实现简单的滑动点击操作，其中“短视频刷量”场景受到黑产团伙的重点关注。

3、在攻击场景方面，黑产作恶手法快速更新，作恶流程上出现精细化分工的趋势

营销欺诈场景上，利用平台规则进行恶意赔付的黑灰产群体不断壮大，威胁猎人情报平台监测到大量号称“超级维权”的黑产攻击行为，2024 年上半年恶意赔付相关话题量持续上涨。

金融欺诈场景上，背债骗贷相关的风险事件频发，伪造手法更加丰富逼真，黑产中介利用背债人进行“房贷、信用贷、企业贷、车贷”一条龙大额融资，一个背债人骗贷总额高达 500-2000 万元不等。

品牌广告欺诈场景上，威胁猎人基于设备暗刷流量持续监测，发现品牌广告暗刷的情况十分普遍，其中食品饮料类成为遭受广告欺诈占比最大的广告主。

数据泄露场景上，2024 年上半年出现多起利用 Facetime 诈骗活动，“设备信息”字段信息出现频率逐渐增多，尤其是“IOS”类数据字段，“IOS”字段相关风险事件共 1237 起，较 2023 年下半年增长 8 倍。

针对层出不穷的作恶事件，企业应及时了解其作恶流程及细节，并结合自身业务场景建立具体的风控规则。与外部黑产的对抗是动态的、持续性的，企业可以**依托基于全网多渠道监测的黑灰产情报数据**，快速识别风险并进行针对性防御。

威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

关注“威胁猎人”

深圳永安在线科技有限公司（品牌名：威胁猎人）

官方服务热线：400-809-3699

官方合作邮箱：marketing@threathunter.cn

官网地址：www.threathunter.cn