威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

# 黑产大数据

## 2025年上半年互联网黑灰产趋势年度总结


THREATHUNTER

# 关于威胁猎人

威胁猎人 Threat Hunter（深圳永安在线科技有限公司）成立于 2017 年，以黑灰产情报能力和反欺诈技术为核心，专注于及时、精准、有效的业务欺诈风险的发现和响应。

公司围绕不同行业在数字化发展过程中面临的业务欺诈、数据泄露、钓鱼仿冒、API 攻击等风险场景，提供成熟多样的产品与服务，并多次入选 Gartner 技术成熟度曲线报告、IDC 威胁情报领域代表厂商。

公司总部在深圳，在北京、上海、重庆、新加坡等地设有分公司，并在深圳和重庆两地建立数字风险应急响应中心（DRRC），为客户提供 7*24 小时全天候数字风险应急响应和及时、优质的服务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85%头部互联网企业，每年帮助客户减少数十亿资金损失。

# 前言

2025 年上半年，互联网黑灰产攻击持续演化，呈现出更隐蔽、更智能、更产业化的趋势。黑灰产从业人员数量继续增长，攻击资源、技术与作案场景全面升级。整体来看，2025 年上半年黑灰产行业发生的几大事件，也时刻印证了黑灰产市场的核心规律——黑产永不眠，当主要交易平台被打击时，黑产及其作恶需求会迅速迁移至现有或新兴替代渠道。

**报告内容关键点总结：**

**在攻击资源方面，**威胁猎人捕获日均活跃风险 IP 达 1382 万例，环比上升 15.02%，“劫持共用代理”IP 攻击更加猖獗，计费模式更多元；黑卡渠道受监管打击后收缩明显，同时新型“链接接码”方式兴起，提升攻击隐蔽性；洗钱银行卡环比上涨 28.60%，其中涉赌卡占比 70.25%，环比上涨 141%，与赌博平台新型充值方式“挂单充值”相关；洗钱对公账户环比下降 40%，黑产目标逐渐从六大行转向城商行和农信社；商户洗钱数量上涨，行业集中于终端零售业、批发零售业、餐饮业。

**在攻击技术方面，**AI 能力被黑产深度滥用，分钟级 AI 换脸、语音克隆已广泛应用于电诈与认证绕过场景，显著提升攻击效率与欺骗性。与此同时，“拉码工具”等洗钱技术工具流入黑产交易链，可直接将黑钱转入正规平台交易路径中进行清洗。

**在攻击场景方面，**营销欺诈、金融欺诈、电信诈骗、钓鱼仿冒、数据泄露、API 攻击等典型场景依旧高发，攻击模式由单点操作向链式协同演进。整体来看，黑灰产已渗透至各行业业务链条，作案模式不断翻新，威胁持续扩大，防御体系亟需系统性升级。

面对不断演进的黑灰产威胁，威胁猎人发布《2025 年上半年互联网黑灰产研究报告》，基于平台捕获的海量风险数据和典型案例分析，从攻击资源、技术演化、重点场景等维度全景呈现当前黑产发展态势，旨在为各行业风控建设提供实战情报支持，助力提升对新型黑产的洞察力与防御力。

# 目录

# 01

# 2025 年上半年黑产攻击资源分析

# 一、2025 年上半年黑产攻击资源分析

## 1.1 2025 年上半年作恶手机号资源分析

### 1.1.1 2025 年上半年新增国内风险手机号总量较 2024 年下半年环比下降 26.16%

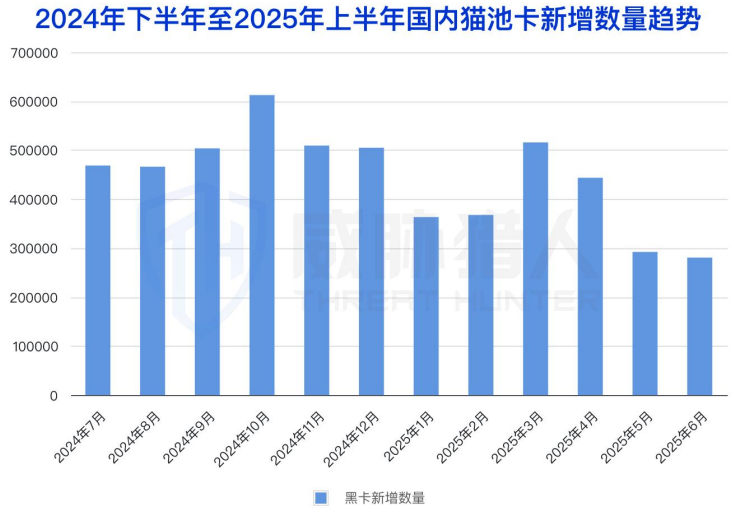
2025 年上半年，威胁猎人监测发现新增国内风险手机号总量出现下滑趋势，新增数量为 226 万，较 2024 年下半年环比下降 26.16% 。


### 1.1.2 2025 年上半年猫池卡资源变化趋势

**（1）2025 年上半年国内猫池卡较 2024 年下半年减少 26.16%**

据威胁猎人情报平台数据显示，2025 年上半年捕获新增猫池卡 226 万例，较 2024 年下半年环比下降 26.16% 。

**猫池卡：**指黑产 “猫池” 设备中，可被批量操控以实现收发短信等功能的手机 SIM 卡，常被不法分子用于违法活动。




**经威胁猎人情报专家分析，出现这一趋势的主要原因是：**

1、1 月及 2 月因农历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；这一现象为黑灰产业的年度周期性规律。

2、2025 年上半年猫池卡数量在 5-6 月呈下降趋势，主要原因为上游黑卡卡商供给收缩，2025 年 4 月底起，供卡源遭受监管打击，卡商停止供卡，导致 2025 年上半年整体数据量下降，详细见 2.1.3。

**（2）2025 年上半年新增猫池卡归属最多的三个省份为：上海、重庆、广东**

威胁猎人对 2025 年上半年新增国内猫池卡进行统计分析，发现上海、重庆、广东三省（含直辖市）为猫池卡归属地最多的三个省份。

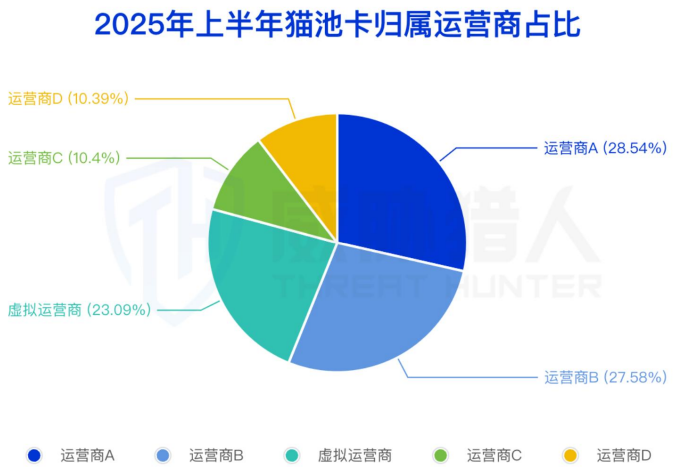

| 省份 | 2025年上半年猫池手机卡新增数量排名 | 年度趋势 |
|---|---|---|
| 上海 | 第一 | 维持 |
| 重庆 | 第二 | 上升8位 |
| 广东 | 第三 | 上升3位 |
| 湖南 | 第四 | 2024年未进入Top10 |
| 山东 | 第五 | 下降1位 |
| 湖北 | 第六 | 上升2位 |
| 辽宁 | 第七 | 下降4位 |
| 福建 | 第八 | 上升1位 |
| 浙江 | 第九 | 2024年未进入Top10 |
| 江苏 | 第十 | 下降3位 |

### （3）2025 年上半年新增猫池卡归属最多的三个城市为：上海、重庆、长沙

威胁猎人对 2025 年上半年新增国内猫池卡进行统计分析，发现上海、重庆、长沙三地为猫池卡归属地最多的三个城市。

**（4）2025 年上半年捕获的新增猫池卡中，归属国内三大运营商的占 66.51%**

威胁猎人情报数据显示，2025 年上半年监测到新增猫池卡 226 万例，其中归属国内三大运营商的猫池卡占比 66.51%




## 1.1.3 2025 年国内拦截手机卡资源变化趋势

**拦截卡：**黑产通过病毒木马劫持手机短信收发权限，从而控制的手机号码，号码主人为正常用户。

**（1）2025 年上半年国内拦截卡较 2024 年下半年减少 83.51%**

据威胁猎人情报平台数据显示，2025 年上半年，威胁猎人捕获新增拦截卡达 15.5 万，较 2024 年下半年减少 83.51%。对黑灰产拦截卡供给情况的进一步分析显示：

2024 年下半年至 2025 年上半年，主流拦截卡平台持续受到监管力量打击，导致供卡侧规模大幅下降。

- 1-4 月期间，原本活跃的 6 个拦截卡平台（供卡渠道）中，仅剩余 2 个处于半停滞状态；

- 而 5 月下旬，监测发现新增 4 个供卡渠道，此前处于半停滞状态的 2 个供卡渠道，黑产更换了域名、接码工具后恢复活跃。

截止 25 年上半年，现存 6 大活跃供卡渠道，但上述平台的号码供给量级和质量均呈现不稳定波动状态。


**（2）2025 年上半年拦截卡归属最多的三个省份为：山东、河南、四川**

针对 2025 年上半年捕获到的国内拦截卡统计分析发现，山东、河南、四川三省为拦截卡归属地最多的三个省份。

| 省份 | 2025年上半年拦截手机卡新增数量排名 | 年度趋势 |
| --- | --- | --- |
| 山东 | 第一 | 上升1位 |
| 河南 | 第二 | 上升2位 |
| 四川 | 第三 | 维持 |
| 广东 | 第四 | 下降3位 |
| 河北 | 第五 | 上升3位 |
| 安徽 | 第六 | 维持 |
| 湖南 | 第七 | 下降2位 |
| 江苏 | 第八 | 上升1位 |
| 江西 | 第九 | 上升1位 |
| 广西 | 第十 | 下降1位 |

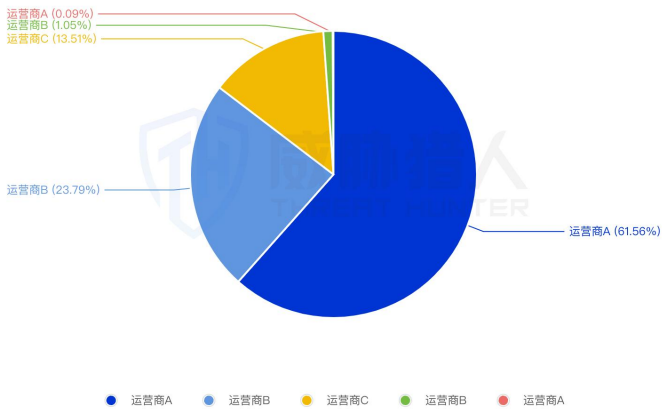
**（3）2025 年上半年新增拦截卡归属最多的三个城市为：重庆、菏泽、临沂**

威胁猎人对 2025 年上半年新增国内拦截卡进行统计分析，发现重庆、菏泽、临沂三地为拦截卡归属地最多的三个城市。


**（4）2025 年上半年捕获的新增拦截卡中，归属国内三大运营商的占 98.86%**

2025 年上半年威胁猎人情报运营平台捕获新增拦截卡达 15.5 万张，归属国内三大运营商的拦截卡占比达 98.86%。

2025年上半年拦截卡归属运营商占比

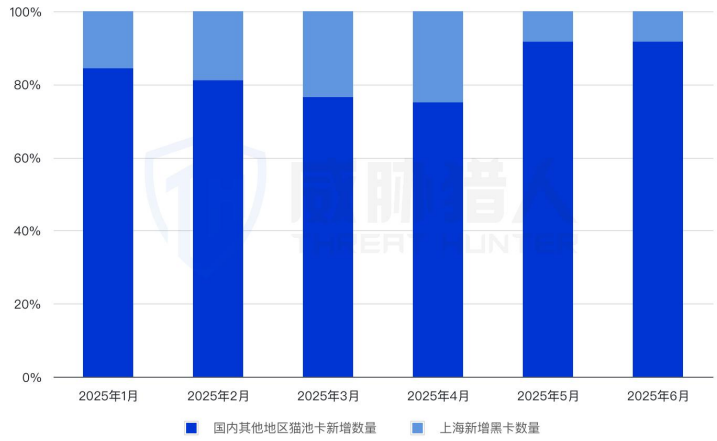



## 1.1.4 监管打击供卡源：上游供卡源波动影响黑产作恶全链条

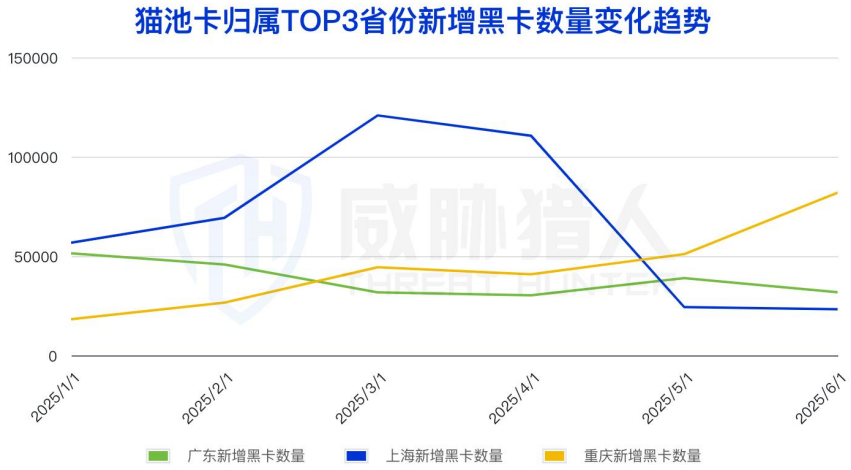
### （1）头部供卡源上海卡商监管重创，国内猫池卡上半年锐减

威胁猎人监控数据分析，上海卡商近年跃升为猫池卡供应的头部卡源。2024 年以来，提供号码归属为上海市的猫池卡卡商持续高度活跃，2024 年新增上海猫池卡占全年新增总量的 11.77%；2025 年 1 到 4 月期间仍保持上升趋势，于 4 月达到峰值，当月新增国内新增猫池卡中 24.93% 来自上海。2025 年 5 月监管打击行动中，上海卡商首当其冲受创，该卡源 5 月份新增占比全国的比重迅速下滑至月均占比 8.29%。这也是上半年国内猫池卡出现大幅下降的主要原因。

国内新增猫池卡，上海号码占比情况



上海新增黑卡数量监管打击期间大幅下降，导致全国猫池卡整体数量下滑，在下图可见，上海新增黑卡数量在 5 月出现锐减并在本年度首次低于广东、重庆黑卡，该格局目前仍保持。

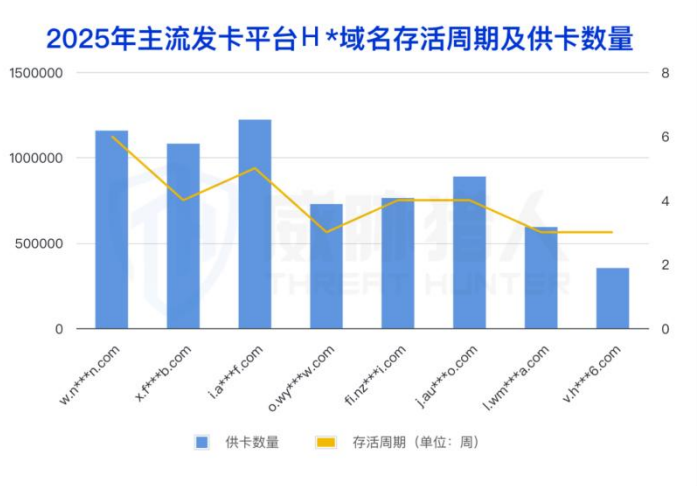



2025 年上半年黑卡产业链监管打击时间线如下，上游上海、重庆卡商相继遭受打击。

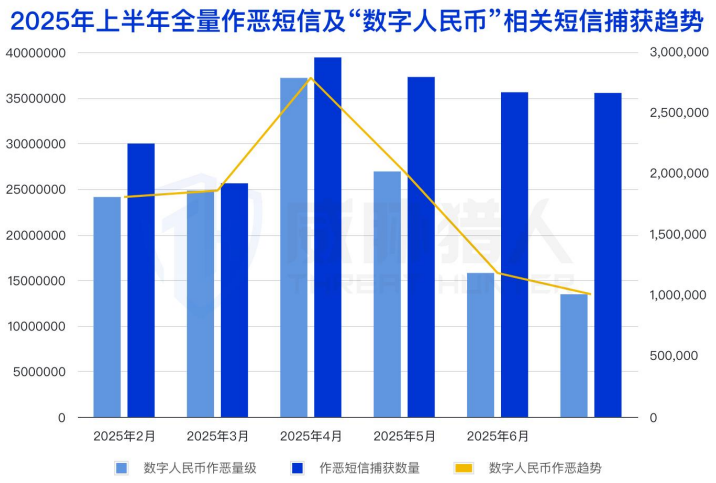

**（2）上游供卡源的波动传导至黑产中游环节**

作为黑产中游环节的发卡平台和接码平台，2025 年 5 月到 6 月期间频繁出现迁址、关停维护或注销等情况，这进一步阻断下游黑卡供给链路。

以长期监控的黑产主流发卡平台团伙 A 为例，短期频繁更改使用的域名 8 次以上，域名存活周期缩短到 15 到 21 天不等，供卡数量亦呈现下滑趋势，从 115 万降至 6 月底 35 万。

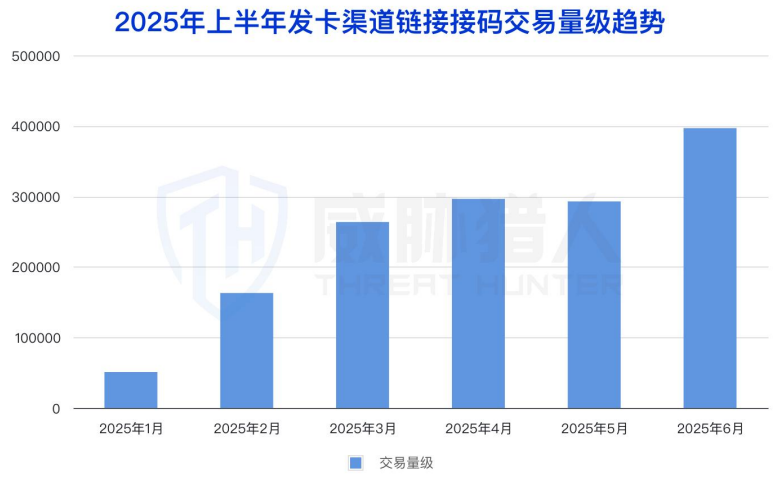



而作为黑灰产主要作恶渠道之一的群接码渠道，观察捕获的接码短信记录亦呈现下降趋势——2025 年 5 月至 6 月捕获的短信记录数量，较同年 3 月至 4 月下降了 556 万例，环比降幅约为 7.26%。以黑产作恶重点目标 “数字人民币” 接码为例，其作恶短信数量变化趋势，便是这一影响的典型例证。




## 1.1.5 链接接码：黑灰产新型接码方式兴起

2025 年上半年，被称为“链接接码”的新型接码方式在发卡渠道兴起，黑产当前主要用于北美地区和中国香港地区的接码服务。截止 6 月份，已监控 146 万余条交易记录，涉链接接码相关域名 140 个，每周新增约 8 个分销商独立域名。




“链接接码”的显著特征为“一对一”的模式，具体而言，下游黑产用户购买某个项目后会分配到一个专用接码手机号，并通过独占链接接收该项目的短信验证码。每个恶意手机号仅服务单一项目，每个链接仅展示对应项目的验证码。链接接码流程如下：


相较于传统接码方式，链接接码具备更高的隐私性与反溯源能力，其有效规避了传统接码中常见的三类风险：

**一是养号成果被窃取**——传统接码通常共享对接码或转码房间，导致号码明文或掩码被其他黑产读取，已养成的恶意账户被劫持；

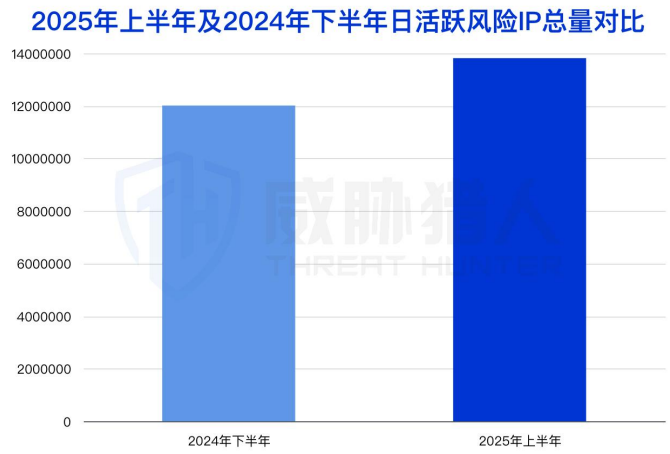
**二是资源冲突问题**——同一号码在多个黑产项目中重复使用，造成数据污染，需额外过滤流程。

**三是监管溯源追踪**——卡商通常将链接接码使用的接码域名设置为不同于黑产平台的域名，或出售给分销商使用独立域名，难以通过域名溯源到黑产平台。


## 1.2 2025 年上半年作恶 IP 资源分析

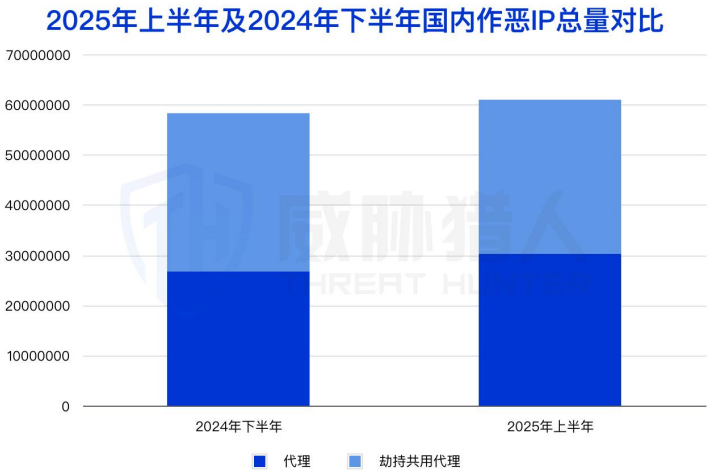
### 1.2.1 2025 年上半年日均活跃风险 IP 总量较 2024 年下半年环比增长 15.02%

2025 年上半年，威胁猎人监测发现日均活跃风险 IP 数量持续上升，风险 IP 数量达到 1382 万，较 2024 年下半年增长 15.02%。



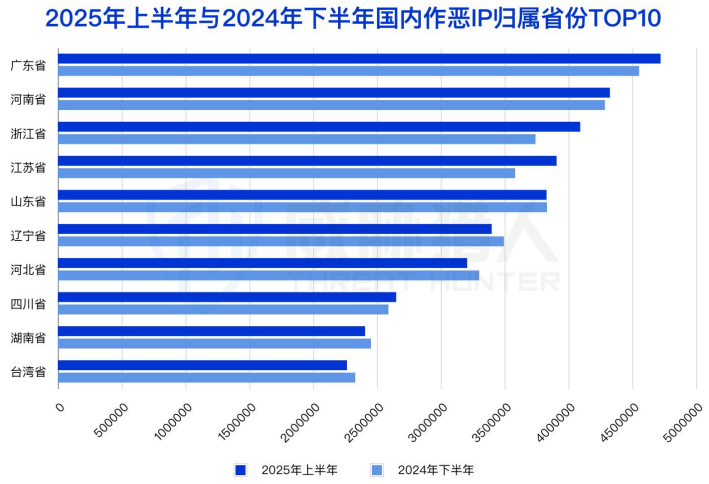

## 1.2.2 2025 年上半年国内作恶 IP 资源分析

**（1） 2025 年上半年国内作恶 IP 有 6096 万个，环比 2024 年下半年增加 4.61%**




**（2）2025 年上半年国内作恶 IP 归属省份 TOP3：广东、河南、浙江**

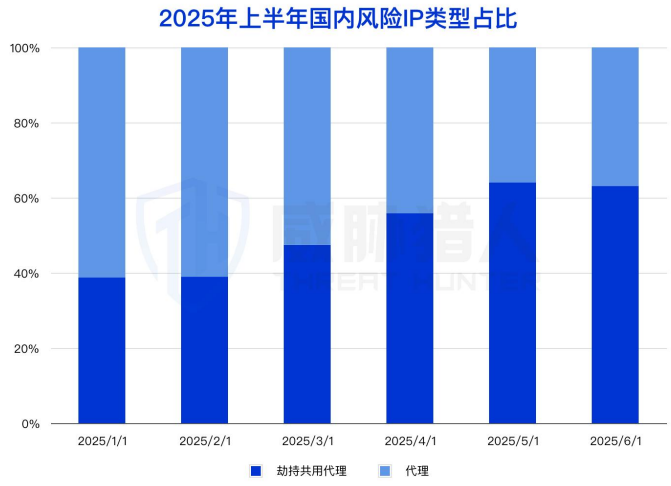
威胁猎人情报数据统计显示，2025 年上半年国内活跃的作恶 IP 归属省份（含直辖市）主要集中在广东省、河南省和浙江省。




**（3）2025 年上半年“劫持共用代理”IP 攻击占总量 50.37%，IP 资源供应更稳定、计费模式更多元**

威胁猎人对代理 IP 平台持续监测，从 2025 上半年捕获数据来看，“劫持共用代理”IP 日均捕获数量达 120 万，同时从国内风险 IP 类型占比来看，黑产使用劫持共用 IP 攻击占比从 1 月的 38.80%上升至 6 月的 63.10%，说明黑产通过植入木马恶意使用正常用户 IP 的行为更加猖獗。

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。



劫持共用代理从兴起到稳定，为满足黑产群体多类型的攻击需求，收费模式从之前单一的按 IP 计费模式发展成适应于不同攻击场景使用的计费模式，产品逐渐趋于成熟。

| 代理IP类型 | 2024年下半年 | 2025年上半年 |
| --- | --- | --- |
| 代理 | 按IP计费<br>按流量计费<br>按并发计费<br>不限量IP池 | |
| 劫持共用代理 | 按IP计费 | 按IP计费<br>按流量计费<br>按并发计费 |

**（4）2025 年上半年静态 IP 仍是重要作恶资源之一**

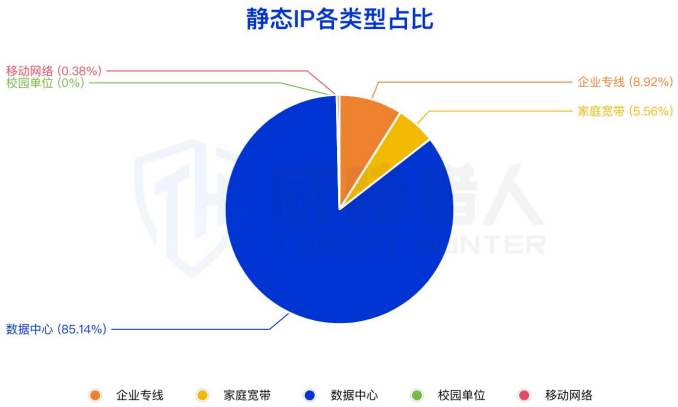
威胁猎人对代理 IP 持续监测，针对近期黑产使用的资源情况，我们发现部分黑产仍会使用静态长效代理 IP 进行作恶。从 2025 上半年捕获数据来看，“长效静态代理”IP 捕获数量达 140 万。

与威胁猎人过往监控的短效动态代理 IP 不同的是，这类长效静态 IP 地址长期不变，其特征较为固定和明显，易被网站和网络安全系统识别并与恶意活动关联起来，且一旦被平台检测封禁 IP，就无法继续使用，导致黑产的攻击行为难以持续进行。然而在一些不需要频繁更换 IP 的作恶场景，黑产通常会使用静态 IP，主要用于如下场景：

**社交平台养号：**利用长效静态 IP 注册的虚假账号进行养号，之后发送大量的垃圾私信、评论、群发广告等，进行恶意营销推广，干扰正常用户的社交体验，引流到其他非法平台或网站。

**低频爬虫：**利用长效静态 IP 模仿普通用户进行数据爬取的一种爬虫，其在 User-agent、频率、时间轴等特征上与普通用户较为接近，进而爬取社交媒体、新闻网站、论坛等平台上的信息。

同时我们发现，这类长效静态代理 IP 的来源类型以数据中心为主，占比 85.14%，而短效动态代理 IP 则主要来源于家庭宽带。



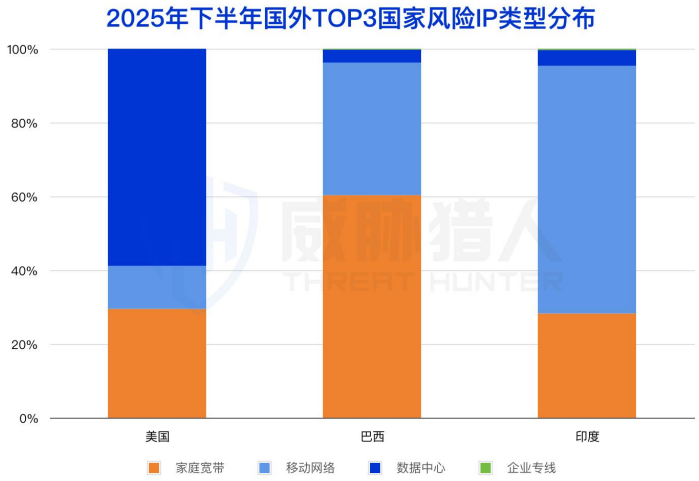

## 1.2.3 2025 年上半年国外作恶 IP 资源分析

（1）2025 年上半年捕获国外作恶 IP 1.1 亿个，环比 2024 年下半年增加 6.56%


**（2）2025 年上半年国外作恶 IP 归属国家 TOP3：美国、巴西、印度**

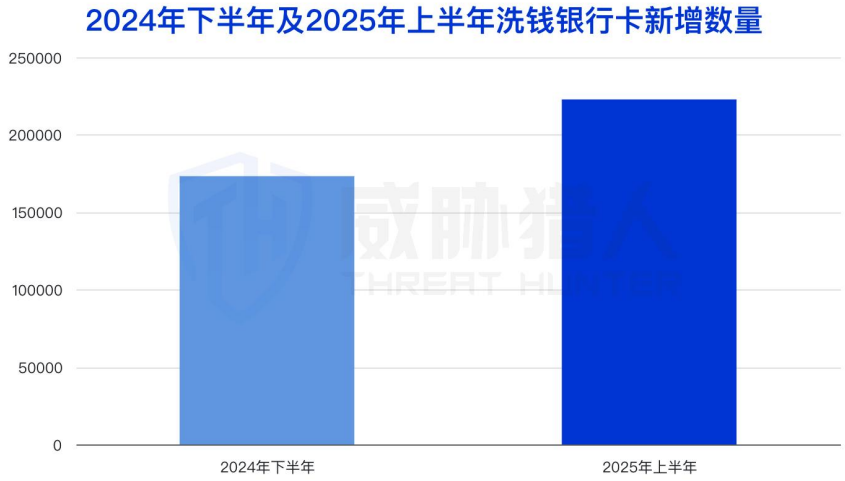
威胁猎人情报数据统计显示，2025 年上半年国外活跃的作恶 IP 国家主要集中在美国、巴西和印度。


威胁猎人发现不同国家的黑 IP 作恶资源也不尽相同，如下是国外 top3 国家的黑 IP 类型分布。




## 1.3 2024 年网络洗钱资源分析

### 1.3.1 2025 年上半年涉及洗钱银行卡较 2024 年下半年环比上涨 28.60%



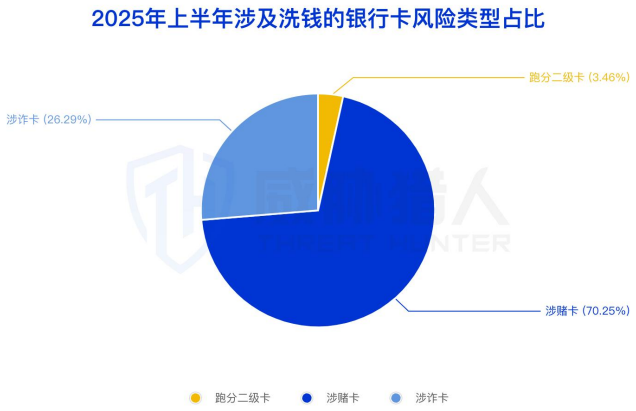

**涉赌卡：**活跃在赌博平台中，为赌博平台内收款使用的银行卡，常被用于赌博平台内进行充值收款行为，关联的资产涉及到赌博洗钱行为。威胁猎人通过人工和自动化结合的方式，从各类赌博平台中采集用于收款行为的银行卡账号信息。

**涉诈卡：**在各类匿名社交黑产群聊中，被诈骗团伙购买用于洗钱的银行卡，常用于诈骗类黑资金转移。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的记录中，提取出诈骗团伙所使用的银行卡账号信息。

**跑分二级卡：**活跃在跑分平台，用于收取洗过一遍资金的二级银行卡。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。

**（1）2025 年上半年洗钱银行卡中涉赌卡占比 70.25%，环比上涨 141%**

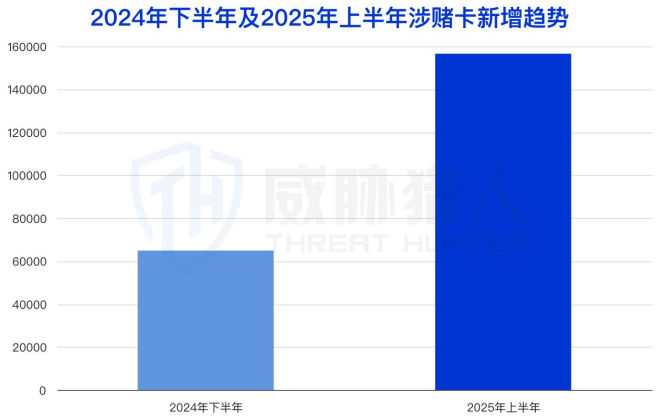
威胁猎人对 2025 年上半年捕获到的 22.28 万张参与洗钱的银行卡进行分析，主要分为涉赌卡、跑分二级卡和涉诈卡三种类型，其中涉赌卡占比最大，达到 70.25%。




**①2025 年上半年赌博平台挂单充值渐成规模，涉赌卡环比上涨 141%**

威胁猎人观察发现，出现涉赌银行卡环比上涨 141%这一显著增长的核心原因是赌博平台新型充值方式——“挂单充值”的发现和规模监控。威胁猎人于 2024 年 11 月份首次在赌博平台中发现此类赌资充值方式，该方式利用充值赌客与提现赌客之间的点对点充值方式，进行洗钱活动。

相比早期跑分模式，“挂单充值”无需招募专业跑分人员，直接利用赌客银行卡即可低成本获取大量账号分散转移诈骗资金。因赌客卡前期无明显洗钱特征（如小额高频转账），极大提升了资金转移的隐蔽性。

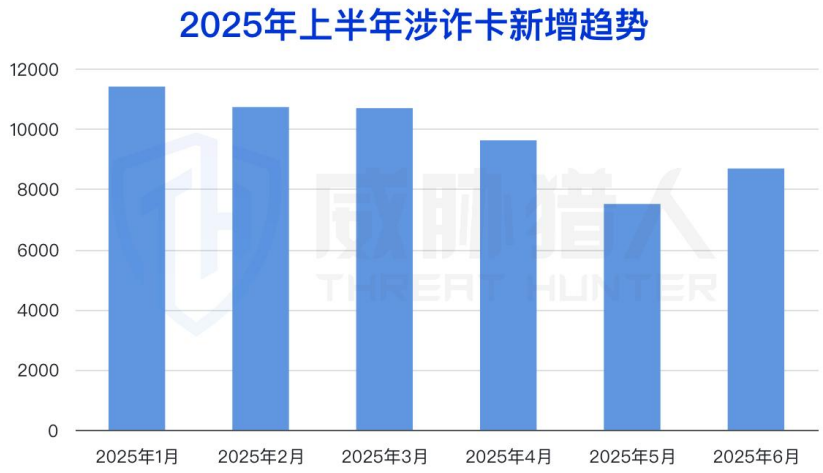



赌博平台挂单充值洗钱模式，即是将赌客 A 的提现需求与赌客 B 的充值需求实时进行匹配，引导赌博资金在赌客间点对点直接流转。让赌客在不知情的情况下成为洗钱通道，帮助完成赃款转移。

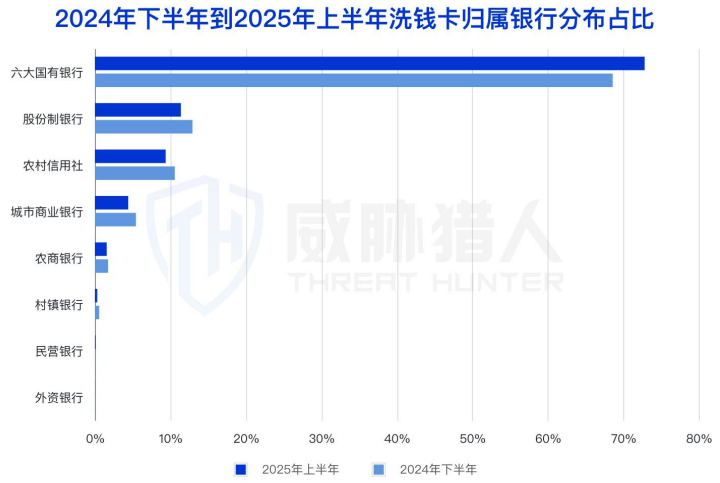

**②2025 年上半年最大黑产担保“好旺”崩盘，洗钱团伙发生转移，涉诈卡数据 5 月份出现短暂下降**

威胁猎人观察发现，涉诈卡新增数量在 5 月出现明显的下降，但在 6 月又迅速回升。其背后原因，是美国在 5 月对 Huione 集团（汇旺）实施制裁，导致其在 TG 上的黑灰产担保平台“好旺”崩盘。这一制裁行动似乎遏制了黑产活动，实则仅造成洗钱团伙的短暂转移，黑产迅速迁移至“土豆”、“火币”等新兴担保平台，洗钱活动并未受到实质性打击。

这一变化清楚反映出，当前的打击手段并未从根本上切断黑产洗钱链条。黑产组织具备极强的适应性和转移能力，一旦某个平台受限，便迅速转向其他渠道继续运作。因此，仅依赖个别平台的制裁难以形成持续有效的遏制力，黑产洗钱产业链仍在不断演化与扩散，打击工作面临巨大挑战。




**（2）2025 年上半年涉及洗钱的银行卡中，六大国有银行的洗钱卡占比依旧是最多的，达到 73%**




**（3）2025 年上半年涉及洗钱的银行卡中，三种类型洗钱卡排名 TOP1 省份均为广东省**

威胁猎人研究发现，2025 年上半年三种风险类型的洗钱银行卡归属省份 TOP10 均涵盖广东、江苏、四川，其中 TOP1 均为广东。

不过，不同类型的洗钱银行卡 TOP10 省份存在差异性：

如跑分二级卡的 TOP10 省份中，福建和江西是独有省份；而涉诈卡的 TOP10 省份中，山东是独有省份。

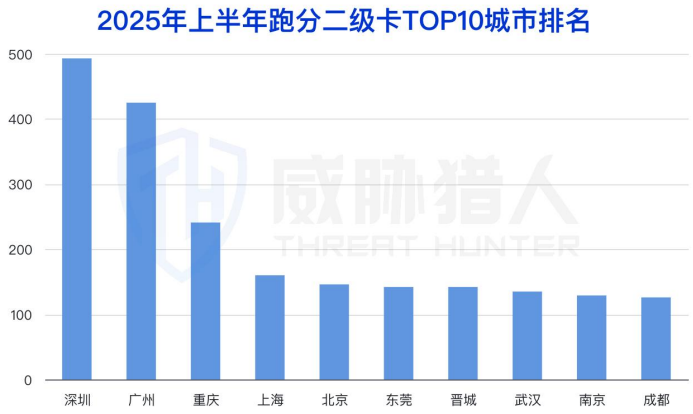



**（4）2025 年上半年涉及洗钱的银行卡中，三种类型洗钱卡排名 TOP1 城市均为深圳市**

威胁猎人研究发现，2025 年上半年三种风险类型洗钱卡的 TOP10 归属城市均涵盖深圳、广州、重庆、上海、北京、东莞、成都，其中 TOP1 均为深圳。

不过，不同类型的洗钱银行卡 TOP10 城市存在差异性：

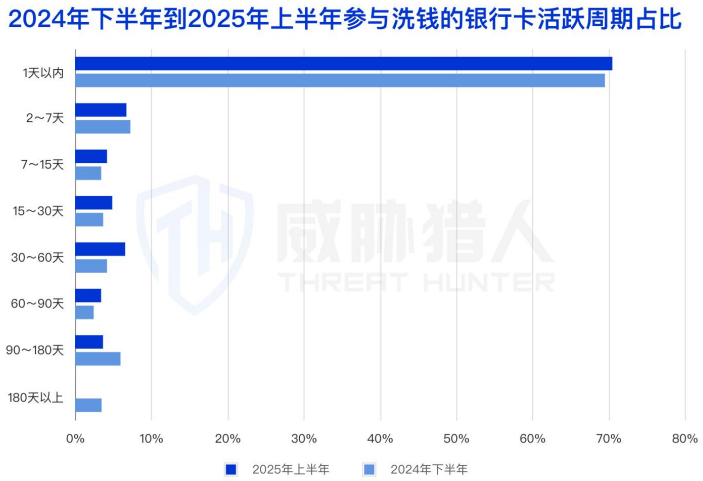
如跑分二级卡的 TOP10 城市中，晋城和南京是独有城市；涉赌卡的 TOP10 城市中，银川是独有城市；而涉诈卡的 TOP10 城市中，郑州和西安是独有城市。





**（5）2025 年上半年涉及洗钱的银行卡中，活跃周期在“一天以内”的占比，基本维持在 70%左右**

威胁猎人分析发现，洗钱卡活跃时间依旧呈现短期化特征。2025 年上半年单日活跃卡占 70%，长期活跃卡（180 天以上）占比则低于 1%。




## 1.3.2 2025 年上半年对公洗钱账户资源变化分析

**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。

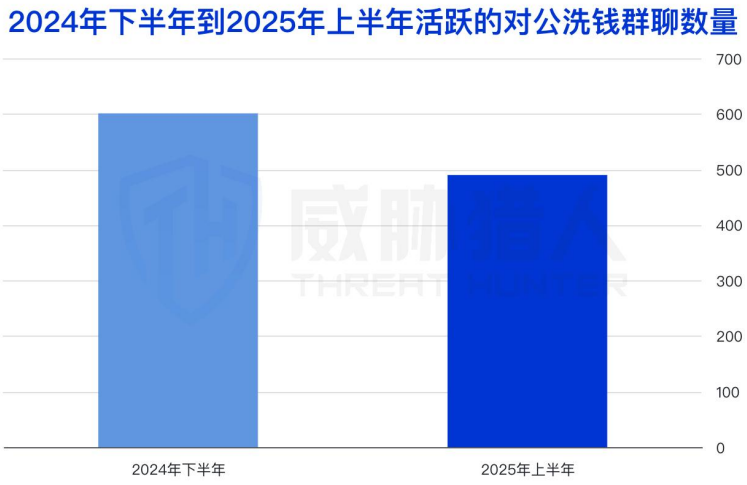
**（1）2025 上半年新增洗钱对公账户环比下降 40%**

2025 年上半年，威胁猎人监测数据显示，洗钱对公账户新增数量环比下降 40%，分析发现导致量级下降的因素主要有三个：

1. 提供洗钱对公账户的洗钱团伙数量在减少，2025 年上半年，提供对公账户的洗钱团伙数量环比下降了 18%。

2. 对公洗钱需求在每年年初都会短暂的下降，根据对洗钱黑产团伙研究发现，黑产每年在接近春节前的 1-2 个月对公洗钱的需求都会减少，对应的提供对公账户的黑产提供对公账户数量也在减少。

3. 5 月份美国对 Huione 集团（汇旺）实施制裁，导致其在 TG 上的黑灰产担保平台“好旺”崩盘，活跃在 TG 上的对公洗钱黑产团伙在 5 月份之后又进一步下降 26.25%。

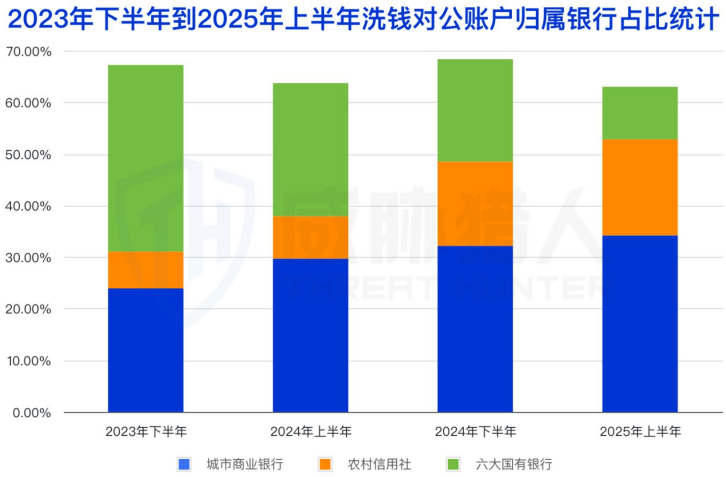




**（2）2025 年上半年涉及洗钱的对公账户中，黑产目标逐渐从六大行转向城商行和农信社**

威胁猎人近两年数据显示，涉洗钱对公账户的归属银行发生了显著变化。2023 年下半年至 2025 年上半年，六大国有银行的洗钱对公账户占比从 36%下降至 20%，与此同时，城市商业银行和农

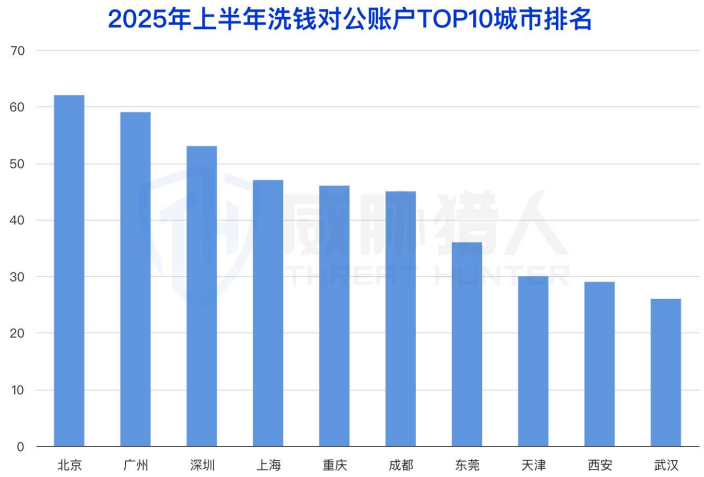
村信用社的占比则呈现持续上升趋势，城市商业银行从 23%增至 34%，农村信用社也从 7%升至 18%。

这一现象明确揭示了黑产洗钱活动正在将目标从监管更为严格、获取成本更高的六大国有银行，逐步转向城市商业银行和农村信用社。这或侧面反映出，相比国有大行，城市商业银行和农村信用社的对公账户获取门槛相对较低，且在洗钱风险管控方面可能存在一定的薄弱环节。、




**（3）2025 年上半年涉及的洗钱的对公账户中，TOP3 省份是广东、山东、江苏**


**（4）2025 年上半年涉及洗钱的对公账户中，TOP3 城市是北京、广州、深圳**




**（5）2025 年上半年涉及洗钱的对公账户中，TOP3 行业是批发零售业、终端零售业、商务服务业**

威胁猎人近两年数据显示，涉及洗钱的对公账户中，TOP10 的所属行业均未发生变化，且渠道批发业长期位于榜首，这表明此类行业的对公账户更容易被黑产用来洗钱。

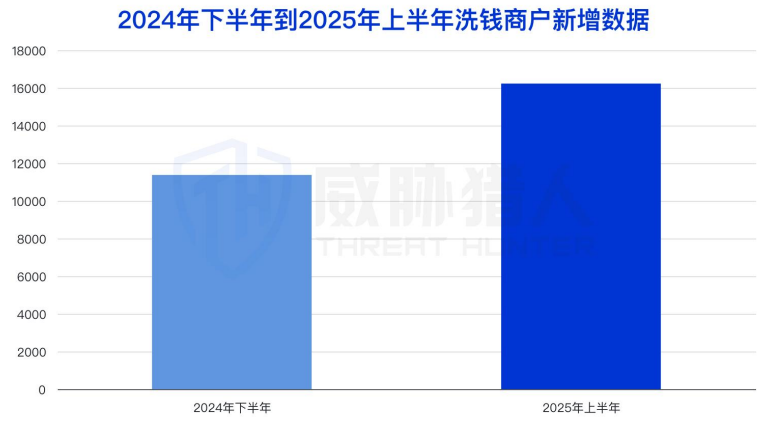

## 1.3.3 2025 上半年参与洗钱的商户资源变化分析

**“商户”**通常指具有合法营业资格的商户及商户账号。近年来，诈骗或洗钱团伙开始利用商户账户收取“黑钱”来洗钱，使用商家资质开通的收款账户基本没有收款额度限制，可支持花呗、信用卡等多种付款方式，相比传统洗钱方式会更隐蔽和高效

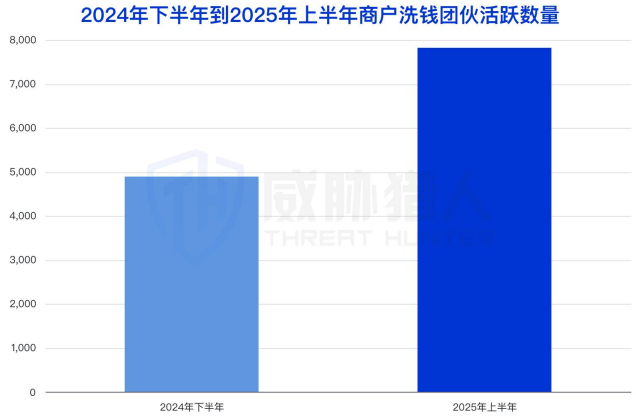
### （1）商户洗钱团伙活跃数量持续上升，被黑产用来洗钱的商户数量环比上涨 43%

2025 年上半年，用于洗钱的商户账户数量环比上涨 43%，呈现出快速增长态势。这一显著增长背后的主要推手是黑产获取商户的成本及门槛较低，以及商户交易特征与洗钱交易特征相似。

一方面，黑产通过伪造材料、资质交易、代办开户等非法手段，以极低成本绕过审核。一旦得手，这些账户便会大量出售或租赁给到洗钱团伙。另一方面，商户本身具备高频交易、大额资金流动以及支持多种支付方式的特征，为非法资金的流转和掩护提供了天然通道。这种“易获取、高适配”的特性，使商户成为黑产洗钱链条中的重要节点。




威胁猎人监测数据显示，2025 年上半年，活跃的商户洗钱黑产团伙数量环比增长了 60%。这一数据反映出商户洗钱风险扩张，该模式正在向组织化、规模化方向演变，进一步表明商户洗钱模式对反洗钱工作的挑战性。



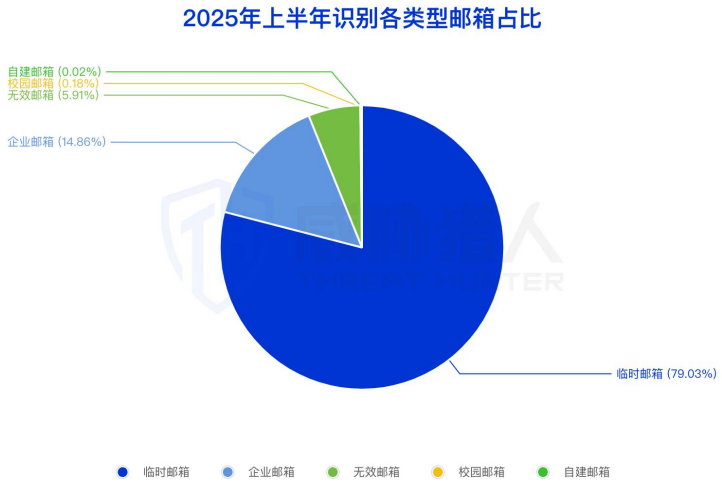
**（2）2025 年上半年涉及洗钱的商户中，TOP3 省份是广东、浙江、湖北**


**（3）2025 年上半年涉及洗钱的商户中，TOP3 城市是广州、武汉、昆明**

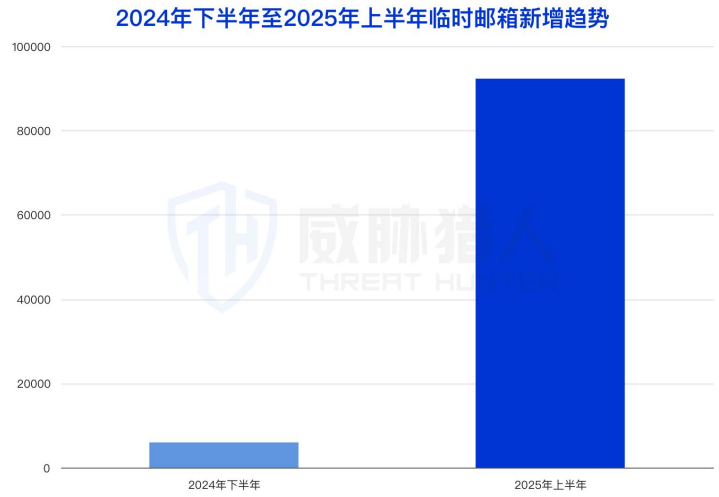

**（4）2025 年上半年涉及洗钱的商户中，TOP3 行业是终端零售业、批发零售业、餐饮业**

## 1.4 2025 年上半年风险邮箱资源分析

2025 年上半年，威胁猎人识别邮箱域名数量 11.68 万个，其中高风险临时邮箱占比最大，达到 79.03%。




2025 年上半年，高风险临时邮箱域名数量环比上涨 14 倍。威胁猎人通过邮件服务器反查技术，加强了对共用同一个邮件服务器的临时邮箱域名群组的监控能力，捕获未被完全覆盖的、属于同一批临时邮箱服务商的衍生域名，极大地拓宽了风险邮箱的监测范围。



02

# 2025 年上半年

# 黑产通用型攻击技术分析

# 二、2025 年上半年黑产通用型攻击技术分析

## 2.1 AI 技术助力黑产实现分钟级攻击

“妈，8000 元不够，给我转 1.5 万元吧。”一位母亲正和女儿视频聊天，听着在外地上学的女儿在视频里撒娇抱怨“生活费不够用了”，她心疼不已打算立刻给孩子转账。就在这时，家门打开了，她的“真女儿”走了进来。而另一头，视频里的“假女儿”还在央求妈妈“给生活费”。

这是一则 AI 反诈视频。在这条反诈视频评论区中，不少网友反映自己也有过类似的被骗经历，“骗子来电，声音容貌和我家人一模一样”。

在上述的例子中，诈骗分子使用了实时换脸+语音克隆的技术实施了诈骗。实时换脸技术为诈骗分子假扮受害者亲人提供了第一道便利，而语音克隆技术则为诈骗分子取信受害者亲人打上了第二道保险，让诈骗分子能最大限度的取信受害者亲人，从而实施诈骗。

得益于 AI 技术的发展，黑产也逐渐将 AI 技术应用到其攻击中。这在一定程度上降低了黑产的攻击门槛，提升了黑产的攻击效率，提高了黑产的攻击质量；这也导致受害者在面对黑产的攻击时防不胜防。

### 2.1.1 AI 换脸技术进化-借助少量图片实现分钟级 AI 换脸

在 2023 年，威胁猎人展示了黑灰产基于视频进行 AI 换脸的攻击技术；而经过两年时间的技术发展，基于图片进行 AI 实时换脸的攻击技术也逐渐成熟，并开始被黑产用于攻击中。

**（1）新旧技术对比**

通过对比不同时期的攻击技术，可以知道：

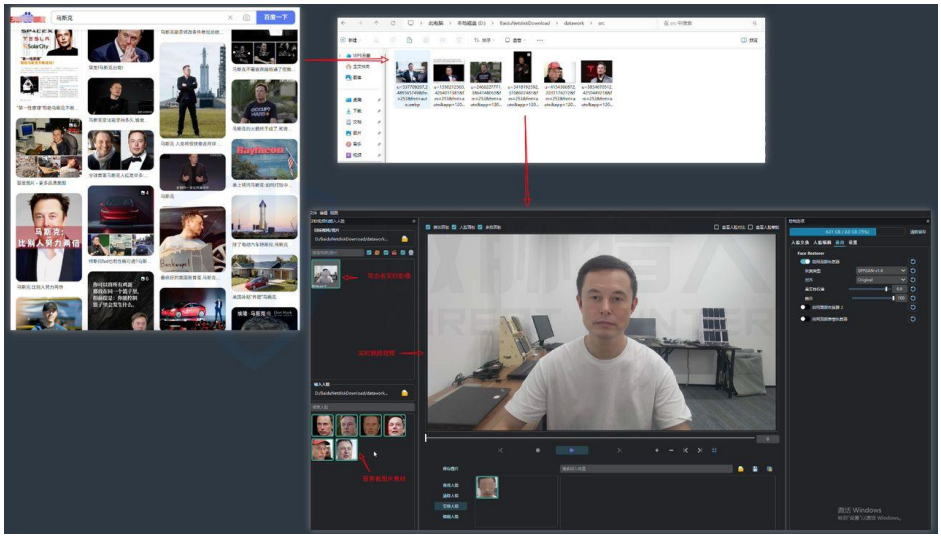
① 新技术在素材要求更低、训练时长更短的作恶优势；

② 换脸效果存在受限条件，需要脸型相近，相近程度直接影响成功率。

| | 早期 | 中期 | 现在 |
|---|---|---|---|
| 实现效果 | 基于模型训练的非实时换脸 | 基于模型训练的实时换脸 | 无模型限制的实时换脸 |
| 素材要求 | 10-20秒的受害者人脸视频 | 10-20秒的受害者人脸视频 | 3-5张受害者人脸照片 |
| 训练时长 | 几小时-几天 | 几小时-几天 | 实时换脸 |
| 换脸效果 | 好 | 好 | 取决于攻击者与受害者面型。越像，效果越好 |
| 硬件要求 | 30系、40系、50系显卡均可 | | |

**（2）新技术演示**

过程十分简单：首先从公开渠道，获取目标人物 2-3 张图片；随后直接用换脸软件加载图片，实现实时换脸。



**（3）风险**

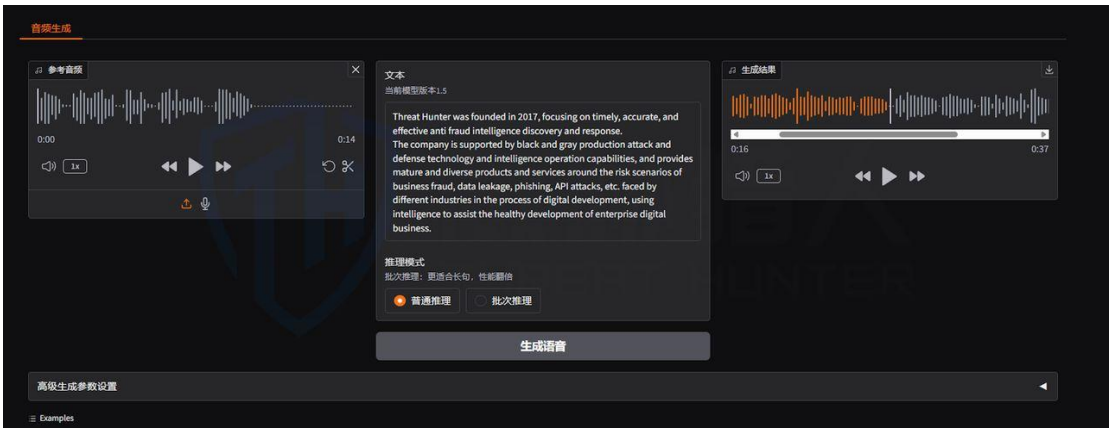
AI 换脸技术的发展，使得攻击者实施攻击所需的素材越发简单、速度越发快速。以 app 的人脸认证绕过场景、电信诈骗场景为例，这导致攻击者能在更短的时间内实施攻击，留给受害者思考的时间也越来越短；往往在受害者还未反应过来的时候，攻击者便已发动攻击，让受害者防不胜防。

### 2.1.2 语音克隆技术-基于 10 秒音频克隆声音

得益于技术的发展，除了上面提及的 AI 换脸技术外，基于少量音频实现的语音克隆技术也变得成熟，并被黑产用于攻击中。

**（1）技术演示**

以受害者一段 10 秒的音频作为克隆样本，在短短的 10 几秒内即可完成克隆，并能以受害者的语音进行任意内容的输出。




**（2）风险**

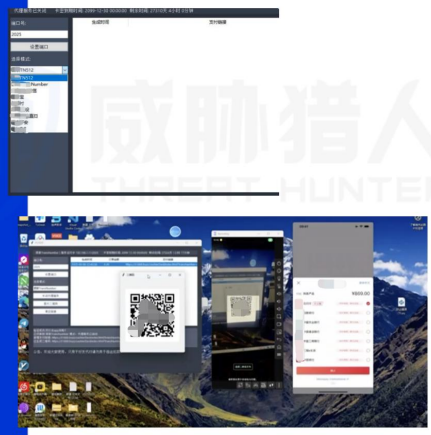
与 AI 换脸不同，语音克隆往往被用于电信诈骗场景中。常见的如电话诈骗、视频会议诈骗等诈骗场景中，都可能会使用到语音克隆技术。语音克隆技术的发展，必然会使得攻击者的攻击越发逼真、越发迅速。

## 2.2 拉码工具-抓取平台支付订单链接进行洗钱

### （1）工具信息

威胁猎人于 2025 年 4 月捕获到黑产洗钱常用的拉码工具。该工具功能为抓取电商平台、支付平台生成的支付订单链接，并将链接转化为二维码供其同伙扫码使用。

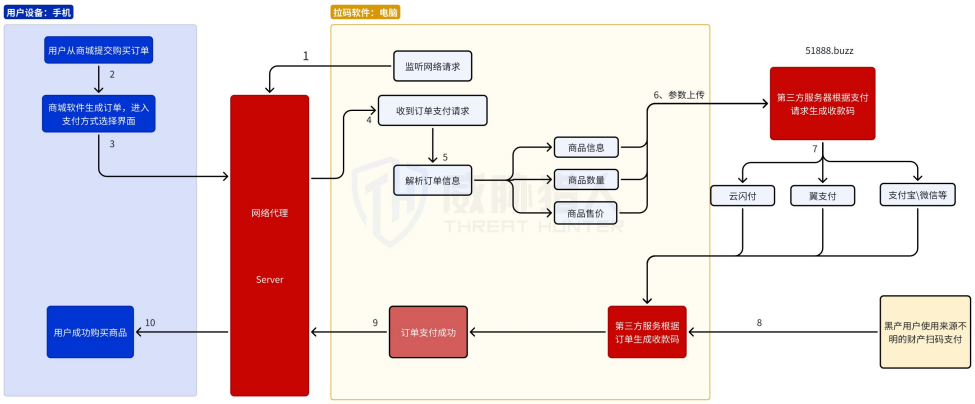
该工具的信息如下：

| | |
|---|---|
| 应用名称 | 皇朝代付 |
| 应用类型 | 拉码工具 |
| 应用环境依赖 | root、VPN代理 |
| 应用界面 |  |

### （2）工具流程介绍

该类工具利用抓包技术，抓取支付订单链接，供黑产在洗钱过程中支付使用。具体运行流程如下：

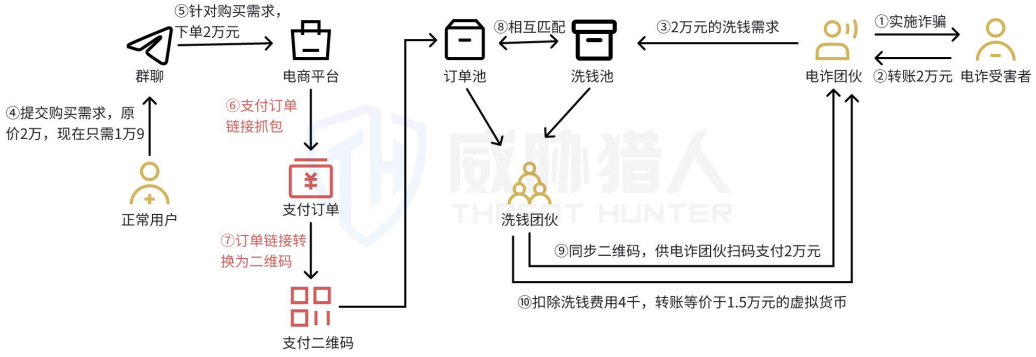
1. 手机端设置 VPN 端口转发
2. 电脑端开启软件，监听手机端转发的信息
3. 手机端在软件中选择商品下单，电脑端会弹出收款二维码
4. 利用其他手机扫码付款即可。




经调研，该类工具常被用于黑产代付、洗钱、刷单诈骗等场景，以下文电诈团伙 A 寻找洗钱团伙 B 进行洗钱为例，在洗钱流程中，洗钱团伙通过拉码工具，将正规平台的支付订单裹挟到洗钱流程中，使得黑钱直接流向的正规平台中，使得洗钱流程波及的范围更大，追查难度亦更高。

**洗钱团伙 B 提供的服务及主要流程如下：**

1. 电诈团伙诈骗得到 2 万元，寻找洗钱团伙进行洗钱；
2. 洗钱团伙创建社交群聊并持续运营，以优惠购买商品为噱头，吸引正常用户；
3. 正常用户 A 购买电脑设备，原需 2 万；现在群聊中购买，只需 1.9 万；
4. 洗钱团伙将 2 万元的洗钱需求与正常用户的 2 万元购买需求相匹配，让洗钱团伙用诈骗来的 2 万元支付正常用户的购买订单；这个过程中，电诈团伙正是借助洗钱团伙通过拉码软件生成的二维码或链接，完成正常用户 2 万元商品订单的支付。
5. 正常用户 A 向洗钱团伙转账购买费用 1.9 万，洗钱团伙再扣除 4 千元的洗钱服务费后，把余下 1.5 万元以等价的虚拟货币转给电诈团伙；



# 03

# 2025 年上半年
# 黑产攻击场景分析

# 三、2025 年上半年黑产攻击场景分析

## 3.1 营销欺诈场景分析

2025 年上半年，威胁猎人系统共捕获营销活动攻击情报 5.8 亿条，环比 2024 年下半年（4.6 亿条）增长超 26%，呈现持续高压态势。

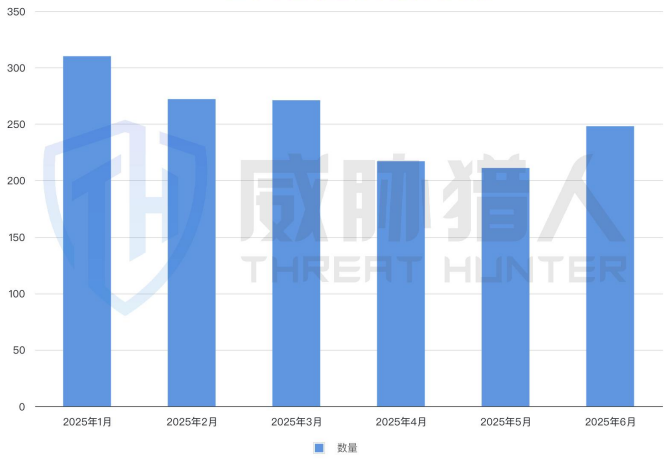
2025 年 1 月起攻击量明显攀升，1-3 月线报量从 6800 万级别上升至 9600 万+，5 月线报量飙升至 1.37 亿条，为半年峰值，大量黑灰产借助五一促销节点、品牌 618 预热期集中投放营销诈骗内容。


2025 年上半年威胁猎人共计预警同步风险事件 1510 个，从行业分布来看，电商行业仍是风险最为集中领域，占比高达 27.55%，其次为本地生活 (11.99%) 、银行 (9.07%) 、兴趣社交 (8.82%)、在线票务（7.88%）等行业，整体呈现以下特征：

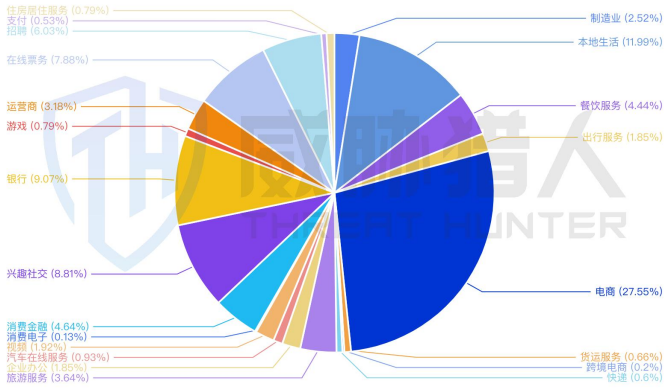
- 平台属性强的行业风险更高：如电商、生活服务、票务等行业，由于其依赖用户活跃、订单交易和营销活动，成为黑产重点目标；

- 资金交互频繁的行业同样高发：如银行、消费金融、支付类行业，风险关注点更偏向于营销引流下的转化路径篡改、薅羊毛行为；

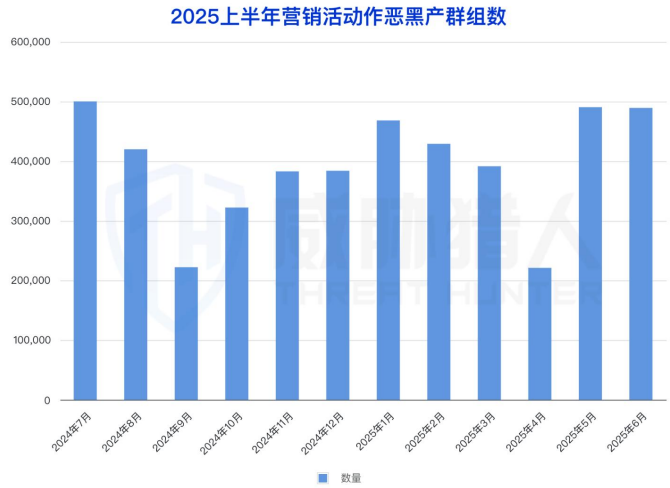
2025上半年营销活动事件量级态势




2025上半年营销活动攻击事件行业分布




根据威胁猎人平台监测数据，2025 年上半年平均每月捕获涉及营销活动的黑产作恶群组约为 37.5 万个，其中 5 月与 6 月为半年高点，整体群组数量相比 2024 年下半年同期略有上升

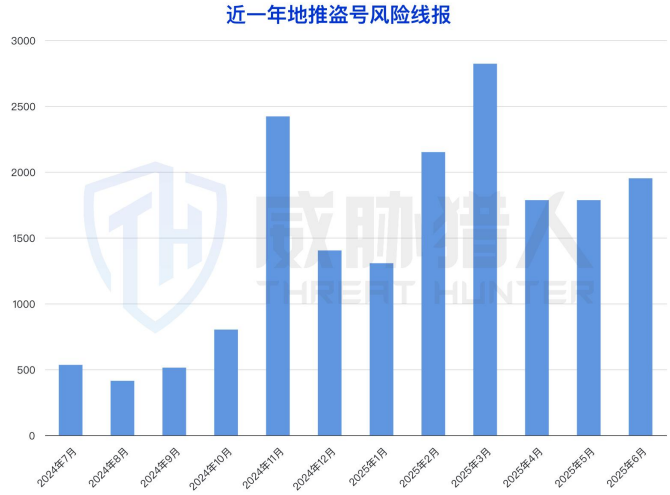



2025 年上半年，威胁猎人平台平均每月捕获营销欺诈相关黑灰产从业账号超过 130 万，其中 6 月达到 143.6 万，为近一年新高，整体对比 2024 年下半年月均水平（约 117 万）上涨 11%。


### 3.1.1 黑产“嫁接”传统地推手段至盗号欺诈

今年上半年以来，盗号风险逐渐上升，黑灰产团伙手法不断翻新，逐渐从“技术型劫持”向“社交工程诱导”演进，最终形成“技术劫持+社交工程”的复合攻击模式。这类被盗取的账号经盗号黑产交易后，最终会被用于各类非法引流、诈骗等作恶用途。

威胁猎人数据显示，2025 年上半年共计捕获 11798 条地推盗号风险线报，2024 下半年共计捕获该类线报 6080 条，环比上涨 94.05%。其中今年 2 月起明显增长，表明春节期间是地推盗号行为的高发阶段；后续三个月数据回落，但整体仍处于高位，说明风险尚未解除。




**（1）传统地推方式受黑产团伙关注及利用**

所谓“地推”，即“地面推广”的简称，原本是企业通过摆摊、扫街、派发传单、面对面讲解等方式在线下接触用户、推广产品的一种营销方式。其核心特征是真实接触+现场转化，多见于地铁口、商圈、校园、展会等人流密集区域。

黑灰产团伙正是借助这一形式，将传统的线下推广手法“嫁接”到欺诈攻击中。通过主流社交平台配合使用，黑产人员以“扫码登录”“刷单返利”“中奖领奖”等话术诱导用户扫码、下载 App 或交出手机，诱使其主动提交授权信息或执行敏感操作，进而获取账号控制权。

**（2）两大类高发地推盗号路径**

威胁猎人识别出两类高发盗号路径：

**一类**是单点式作案，由地推人员手持接码卡，通过话术诱导用户扫码并实施账号换绑，流程简单，盗号后直接出售变现，组织结构松散。

**另一类**是链条化作案，由上游开发木马工具，中游地推执行植入，下游专门负责账号流转和变现，分工明确、作案规模更大、隐蔽性更强。

**① 地推引流+账号换绑：黑产高效盗号路径**

黑产在与受害者当面接触时，往往通过线下拉新活动、扫码抽奖等方式引导受害者扫码或交出手机，再以“辅助操作”为名，实则快速完成账号密码重置和换绑手机号的操作，该类地推盗号简易、高效。但是账号极易掉线。黑产可获取其账号短期的使用权（1-2 天），因此黑产往往是提前对接好买家，获取到账号后便快速出售获利

1. 黑产在街头通过地推摆摊的方式吸引用户参与等活动（扫码注册领礼品、下载 app 等等）

2. 黑产使用话术取得用户信任，并借机拿到手机，迅速为该账号设置登录密码（如 aa123456），并使用手里的换绑卡资源，将目标 app 账号原绑定的手机号进行更换；

3. 黑产使用新换绑的手机号登录该账号，此时系统可能触发新设备风控：

- 若是需要原手机验证码验证：黑产诱导受害者提供短信验证码

- 若是密码验证：则使用统一设置的弱密码完成验证；

4. 确认可以正常登录后，黑产便快速将账号出售，并离开摆摊地点，寻找下一个人群密集地继续行骗


**② 地推引流+诱导安装木马 App 实现盗号**

黑产通过线上或线下地推，以“扫码领奖”“参与活动”等话术诱导受害者安装木马 App，从而在后台静默提取用户在目标 App 中的登录凭证（如 token、cookie、session_id 等），并实时上传至黑产服务器。该手法在业内被称为“提参”，即“提取参数”的简称，实质上是绕过传统密码验证，直接复用用户的登录会话，实现远程克隆登录。获取凭证后，黑产可借助上号器、模拟器等工具还原账号使用环境，进行批量登录、自动化操作与变现。这类账号通常以“数据号”形式出售，具备可直接登录、无需验证的特点，极易被用于刷量、引流、推广等黑产行为。

下图为盗号黑产上游提供给中游地推团队的二维码，地推人员只需要让用户扫描二维码其账号登录凭证便会被盗取


下图为地推上游黑产使用的软件界面，中游地推人员每成功诱骗一个用户扫码或者下载 app，其登录数据凭证便会传回后端显示在软件里面，黑产则可以批量导出数据进行售卖


黑产操作链路详解：

1. 黑产在街头通过“扫码送礼”“邀请拉新得红包”等方式，吸引路人参与活动。

2. 地推人员在“社交诱导”下，引导用户完成如下行为之一：

- 下载带有提参功能的木马 App（通常伪装成活动 App 或优惠工具），App 安装后在后台静默运行，抓取目标 App 的登录凭证数据；

- 扫码登录钓鱼页：地推人员出示二维码，诱导用户用某 App 扫码登录，通过接口监听或缓存劫持提取其登录凭证；

- 诱导提供验证码：谎称需要验证身份，诱骗用户提供短信验证码，黑产后台借此登录账号并同步提取 token 等参数。

3. 一旦成功获取，登录凭证数据会实时上传至黑产后台服务器


## 3.1.2 刷单团伙产业链升级

### （1）刷单行为的产业化演变路径

威胁猎人监测和分析，电商刷单正经历从“零散化”向“平台化”“工具化”的快速演进早期刷单主要依托 QQ 群、微信群，以“熟人+鱼塘”的模式发布任务，个人用户通过垫付购买商品获得佣金返现。这种方式高度依赖人力协调，操作繁琐、成本高、效率低。而近年来，刷单模式已显著升级。黑产团伙开发并销售自助式刷单工具系统，转至由商家主导刷单全流程的阶段。

| 阶段 | 典型特征 | 组织形态 | 技术手段 |
| --- | --- | --- | --- |
| 1. 零散刷单期 | QQ群/微信群内手工刷单 | 个体操作，鱼塘兼职 | 人工手动，无技术含量 |
| 2. 机刷过渡期 | 利用模拟器/多开工具实现部分自动化刷单 | 黑产脚本群体 | 模拟器+手动调控 |
| 3. 鱼塘平台化期 | 出现小型任务派单平台，如“单多多” | 小团体组织 | 简单网页/脚本工具 |
| 4.系统化协同期 | 刷单平台具备任务调度、账号筛选、设备联动等能力，刷量流程趋于自动化和模块化 | 工厂化运作，半自动平台接单 | 平台工具 + 风控逃避机制 + 账号/设备标签化 |

### （2）刷单产业升级：从鱼塘模式到商家自运营闭环

商家可通过黑产开发的刷单平台自行选择账号、配置设备，并远程控制刷单流程，实现从任务发起、下单操作到数据反馈的自主化操控。刷手不再是重要执行角色，只需要执行付款的动作，整个过程不在高度依赖人工对接，极大降低了操作门槛和对接成本，刷单效率和隐蔽性也大幅提升。

当前刷单生态已不是过去的“找几个群、做几单任务”那种粗放玩法，而是从组织架构、设备资源到执行方式都完成了产业级跃迁。威胁猎人总结其演变路径，呈现出三大核心升级趋势：

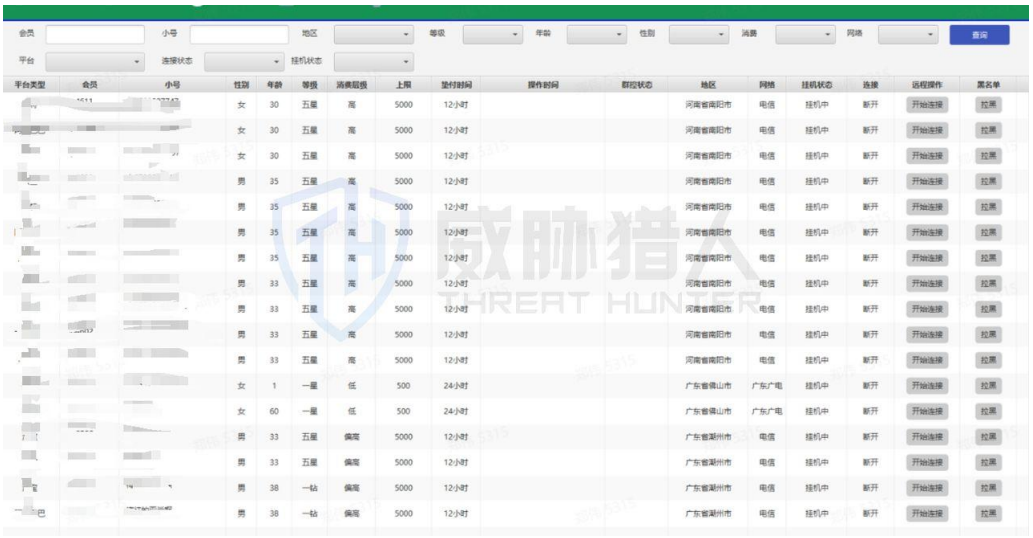
#### ① 商家主导刷单，拟真度提升至“运营级别”

相比以往交由“刷单刷手”随意操作，现如今越来越多商家开始自建刷单方案并主导执行策略。商家深谙平台流量逻辑，知道什么样的用户行为能带来真实流量、权重加持，因此他们会：

- 按照人群画像精准选设备；
- 模拟搜索、浏览、收藏、停留、下单、评价等全链条行为；
- 并结合自身商品在转化、加购率、复购等运营指标的需求，做出高度拟真的任务参数配置。

**结果：**刷单不再是“刷销量”，而是“刷全指标”，几可乱真，风控识别难度急剧上升。

下图为商家端刷单的软件页面，可根据自己的实际需求进行相应设备和平台进行连接



**② 黑产设备体系演进：上万真实刷手设备形成刷单调度网络**

平台化刷单系统背后，是一张由黑产精心构建的真实设备网。平台已对接超 4 万个真实刷手的手机，通过远控或挂机系统统一调度使用。这些设备：

- 具备长期使用记录，权重高、可信度强；
- 被打上行为标签（如地域、性别、品类偏好）；
- 被纳入刷单任务调度系统，可根据商家需求精准调用。
- 本质：刷单已由“人力协调”变成“算法+设备调度”，进入自动化生产阶段。

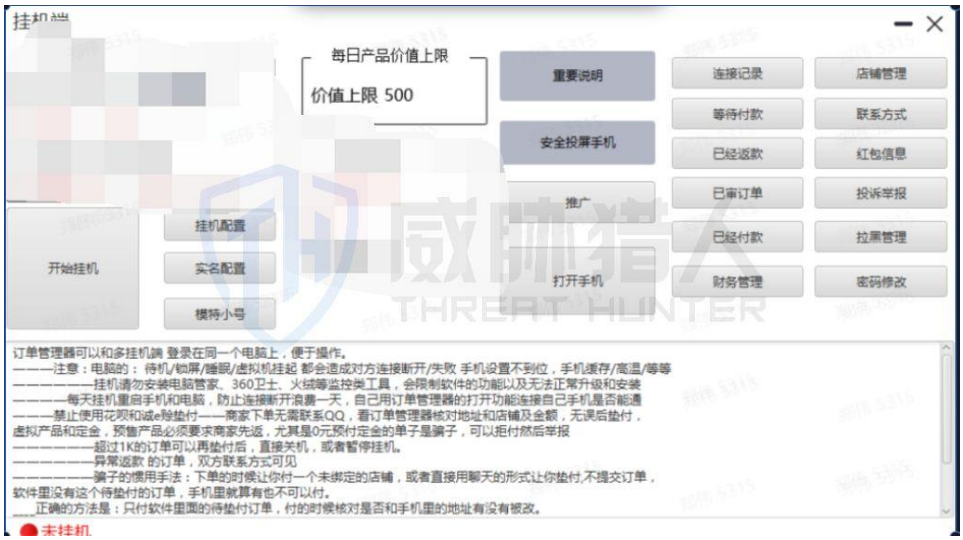
下图为刷手开始挂机前，进行个人信息配置的软件页面


**③ 刷手参与模式转变：从“全流程”到“轻参与”**

在传统刷单体系中，刷手需从接任务、浏览、下单、确认、评价全流程参与，时间成本高、协作复杂。而在当前平台化模式中：

- 刷手仅需在系统提示时完成“付款动作”，无需理解任务全貌；
- 平台系统化分配任务、自动化操作设备，刷手只需出租账号和设备即可收益；
- 参与门槛降低、操作压力减轻，吸引大量普通用户“兼职变刷手”，为黑产提供海量底层执行资源。
- 趋势预测：随着平台功能日益完善、回报机制简化，未来将有越来越多的刷手加入平台，刷单人力逐步平台化、泛职业化。

下图为刷手端的挂机页面：




### 3.1.3 水军产业从舆情干扰到商业竞争打击

随着黑灰产组织的不断演进，水军操控行为已不再局限于简单的刷量操作，而是被用于商业打压、内容控评、热点引流等场景。任务通常通过群组或小型众包平台集中发布，涵盖“点赞、评论、转发、控评”等舆论操控操作，水军按照预设要求执行任务，并提交截图等反馈材料。整个流程隐蔽性强、响应速度快，已形成从任务发起到资金结算的完整闭环。

#### （1）水军任务的接单模式与对接方式

水军任务的分发方式已形成多元化结构，主要通过社群渠道+众包平台+私密执行群三类路径完成。为了保障任务的执行率与统一性，水军组织在任务对接流程上进行了系统化设计。任务发布者不再直接与所有水军沟通，而是通过特定渠道，将操作要求精准传递给稳定的执行人群。任务对接

通常具备以下特征：

- 有明确的评论话术或图片要求；
- 有执行时间窗口或互动规则；
- 有截图或账号 ID 作为任务反馈凭证；
- 有统一的回收、审核与结算流程


**（2）捕获商业品牌水军抹黑案例**

**① 私域渠道招募水军刷差评引导舆论攻击**

通过截获一组聊天记录截图，显示有组织方通过社群方式招募水军，实施定向评论攻击国内某知名车企。任务以发布引战评论、复制粘贴内容刷差评为主，通过大量账号在特定社交平台帖子评论区发布统一差评内容，营造产品争议、制造质量负面舆情，引导公众对品牌产生质疑。

1、任务说明明确

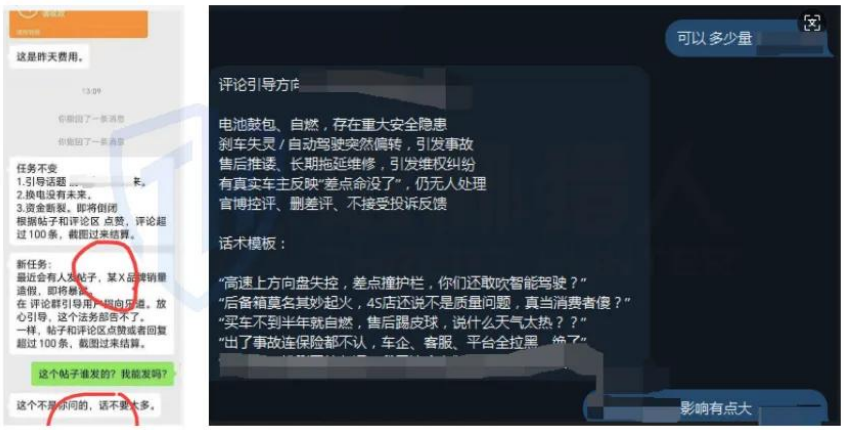
- 引导话题、换电争议、资金断裂等关键词已预设；
- 评论/点赞数超过 100 条即结算，执行门槛低；
- 明确“截图回传”作为核验机制。

2、差评内容批量提供

- 招募方提供统一文案，要求水军直接复制粘贴；
- 每条评论价格为 0.5 元，按量计费；
- 评论中包含捏造事实、夸张指控、仿冒技术人员视角等手法，增强“真实性”。

3、执行群内管控

- 禁止追问任务来源或贴主身份；
- 强调“话不要太多”，明显具备信息隔离意图；
- 群内形成“单向发单+截图结算”闭环。




### ② 众包渠道招募水军刷差评引导舆论攻击

根据监测发现，有黑产或营销团伙通过众包平台组织水军执行定向评论任务，意图在短视频平台操控舆论、引导用户对目标品牌或产品产生负面认知。这类任务往往以“点赞+评论”+“负面引导”为核心操作，雇佣大量水军在评论区展开集中发言，呈现出“真实用户吐槽”的假象，背后却是精心策划的情绪操控行为。

**任务目标：**进入指定视频，发布带有贬损语气的评论，引导舆论关注品牌问题（如续航差、产品虚标、售后差等）。

**评论方式：**首评+附评模式，即首个水军发布主评论，后续多个账号进行点赞、互动和扩散。

**示例话术：**

- “谁买谁后悔，续航虚到离谱”
- “上次都快刹不住了，电池是真不行”
- “质量真的不敢恭维”


## 3.2 金融欺诈场景分析

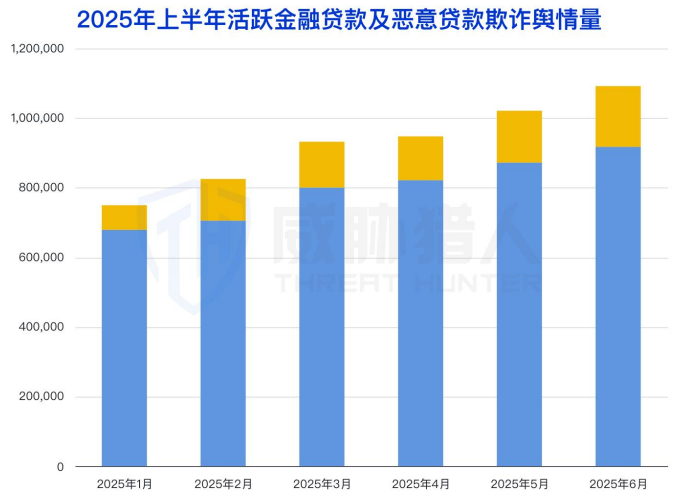
金融欺诈场景下，金融贷款风险舆情和信贷渠道中介动态受到银行等金融机构广泛关注，其中潜藏的恶意贷款风险舆情更是用于识别研判信贷欺诈、进而调整风控策略的重要情报来源。

**恶意贷款欺诈：**指金融从业人员或黑产团伙通过虚假宣传、伪造材料、诱导欺骗等手段，以非法牟利为目的实施的各类违规贷款活动。其典型行为包括：背债、融车套现、科技提额、美容贷骗贷、债务重组、AB 贷、制作假流水、征信修复、债务优化等违规业务以谋取私利。

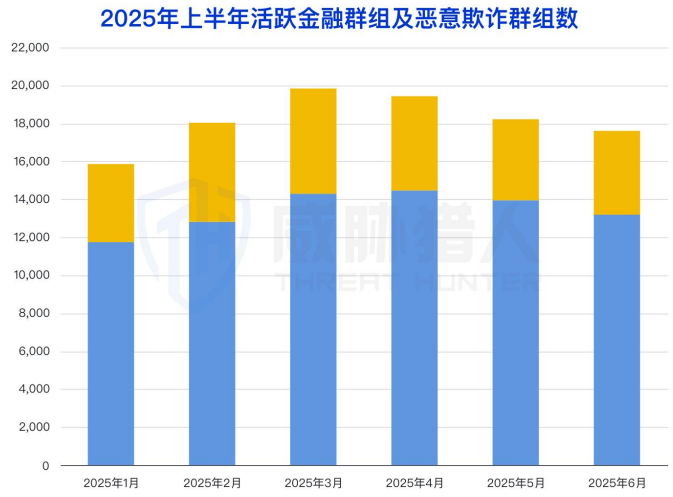
### 3.2.1 2025 年上半年金融贷款恶意欺诈攻击有增无减，依旧严峻

**（1）金融贷款恶意欺诈舆情和黑灰产规模持续扩张**

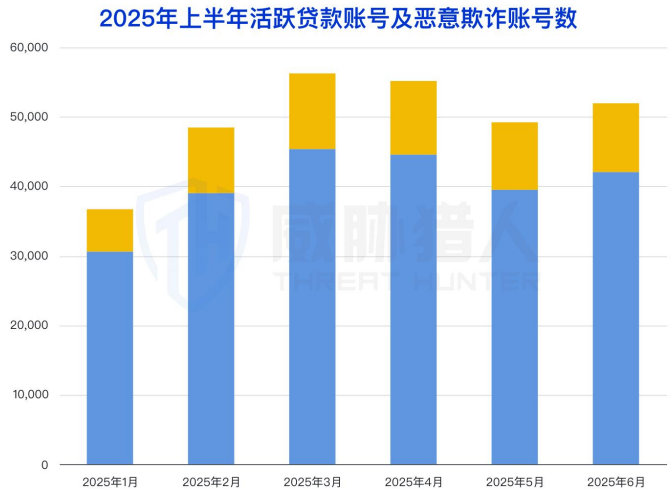
2025 年上半年威胁猎人监控捕获金融贷款风险舆情达 479 万条，其中恶意贷款欺诈舆情 77 万条，占总量 16%，金融贷款风险舆情较 2024 年下半年下降 14%，恶意贷款欺诈舆情较 2024 年下半年增长 12%。在每月的风险舆情趋势上，均呈现持续增长态势。




2025 年上半年威胁猎人监控活跃贷款群组 3.3 万个，其中恶意欺诈群组 1.3 万个，占总量 39%，活跃贷款群组较 2024 年下半年下降 4%，恶意欺诈群组较 2024 年下半年增长 5%。



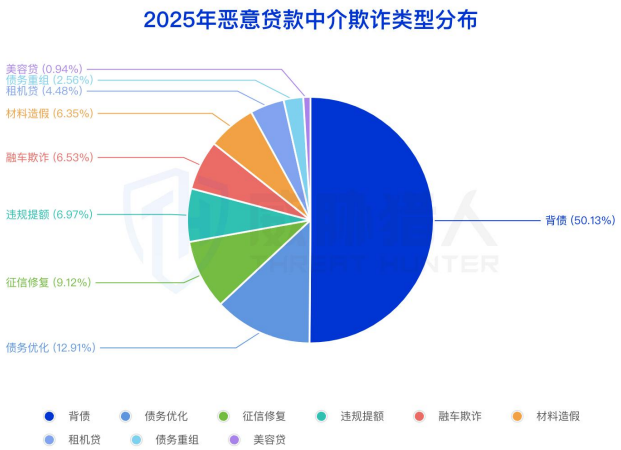

2025 年上半年威胁猎人监控捕获活跃贷款服务账号 11.8 万个，其中提供恶意贷款服务的欺诈账号（信贷黑中介/黑产）3.5 万个，占总量 29.6%，较 2024 年下半年均增长 6%。




**（2）2025 年上半年恶意贷款主要欺诈类型 TOP3：职业背债、债务优化、征信修复**

2025 年上半年数据显示，恶意贷款主要涉及职业背债、债务优化、征信修复、违规提额、融车欺诈、材料造假等超过 9 类欺诈行为，其中职业背债占比高达 50%，居首位，成为黑产核心攻击手段；债务优化、征信修复分别位列第二、第三位，相关代理投诉类业务依然保持较高活跃度。

注意：债务优化包含：反催收、代理维权、代理投诉、退息退费等债务处理场景。



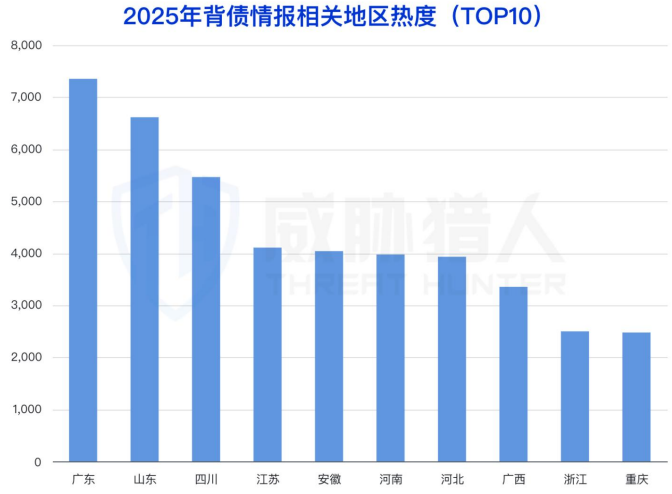

## 3.2.2 职业背债现状风险面扩大，防御压力持续攀升

### （1）职业背债热度上升、已成为黑灰产常规主营业务

2025 年上半年捕获“背债”相关攻击情报呈上升趋势，背债热度上升，2025 年上半年较 2024 年下半年增长 65%，职业背债已成为黑灰产常规主营业务，传播面越来越大。


### （2）2025 年上半年背债地区热度 TOP3 省份：广东、山东、四川

威胁猎人情报数据显示，2025 年上半年“背债”相关的贷款欺诈，活跃热度 TOP3 的省份（含直辖市）是广东、山东、四川。

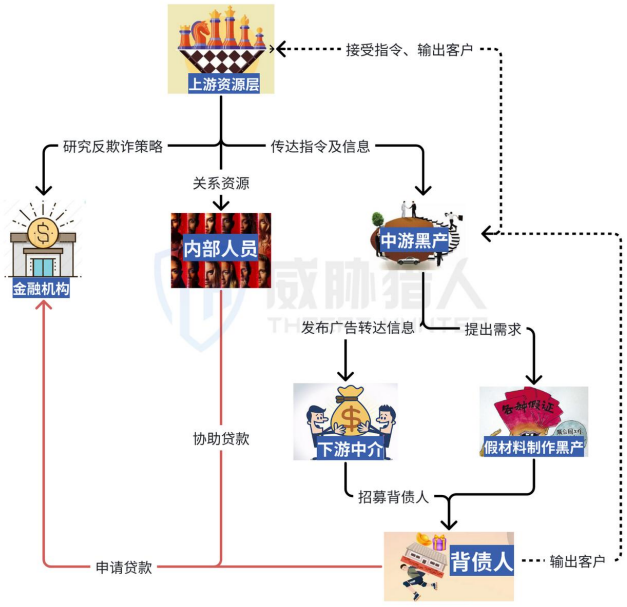



### （3）2025 年上半年背债城市热度 TOP3：重庆、上海、成都

威胁猎人情报数据显示，2025 年上半年“背债”相关的贷款欺诈，活跃热度 TOP3 的城市（含直辖市）是重庆、上海、成都。


### （4）职业背债多角色产业链解析

当前背债黑产链条已形成精密的分工体系，从资质包装、骗贷操作到债务转移均呈现高度专业化特征。背债类黑产角色主要分为上游资源层、中游黑产、下游中介、假材料制作黑产四个角色，加上内外勾结的“内鬼”和背债人，形成一个多方参与且分工明确、环环相扣的非法利益链条。



### （5）企业贷成背债最大风险点

威胁猎人针对背债风险场景深入调研发现，房贷、信贷、车贷和企业贷呈现出差异化的风险特征：车贷因资产易变现、处置链条短，风险暴露迅速且欺诈特征明显；房贷凭借抵押物增信和处置周期长的特性，风险具有较强隐蔽性；企业贷则因“先息后本、“无本续贷”等还款方式，风险呈现明显滞后性，往往积累至集中爆发阶段才显现。

黑产当前的背债搭配模式主要为组合式搭配，如常见的房信企、房企、信企、车企、房信车企等组合模式，不同的骗贷搭配模式取决于背债人的基本情况及黑产的渠道资源好坏。

以下是房贷、信贷、车贷、企业贷四类贷款场景中，职业背债黑产的核心操作环节及风险特征的专项分析，其中企业贷在背债环节中至关重要，成为当前职业背债风险场景下，金融机构面临最大风险点。

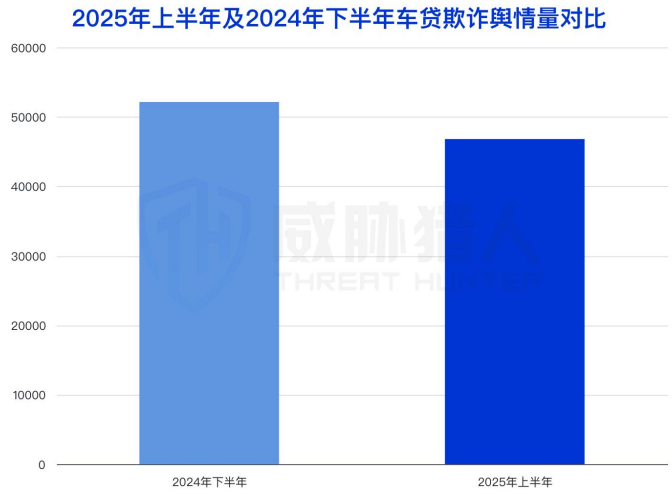
背债环节重要性，是指某一贷款场景在黑灰产背债链条中所处的功能与被利用频率，综合反映其对整条链条成败的影响程度。重要性越高，说明该环节在链条中越关键，既可能是黑产套利的主要资金来源，也可能是资产增信关键点。

对于金融机构来说，重要性高的贷款产品通常面临更高的欺诈攻击频率与更复杂的操控路径，反映出可被利用的业务漏洞更多，防控难度与风控压力也更大。

| 场景 | 涉及贷款类型 | 背债环节重要性 | 背债环节作用 | 风险表现 |
| --- | --- | --- | --- | --- |
| 企业贷 | 税票贷、经营贷 | 至关重要 | 整个背债的核心，利润来源（额度高） | 企业主体主要为有限公司、个体<br>掺杂着真实经营+刷数据<br>多笔、多次贷款<br>企业贷一般为背债最后一类贷款 |
| 房贷 | 按揭房贷、抵押房贷 | 很重要 | 为后续其他贷款场景起资产增信作用 | 按揭房后再次办理二押、三押<br>开发商新房代持套现<br>一人多贷<br>房贷很多时候为背债首笔贷款 |
| 车贷 | 按揭车贷、抵押车贷 | 重要 | 车贷门槛低、套现快、周期短 | 一人多贷、一车多贷<br>按揭车后再次办理二押、三押并处置套现<br>强免抵等非法处置车辆，易暴雷<br>车贷可以为背债首笔贷款 |
| 信贷 | 装修贷、消费贷 | 重要 | 信贷是后续企业贷的“前期费用”主要来源 | 房贷还款1个月后操作信贷、装修贷<br>消费贷可以为背债首笔贷款 |
| 农户贷 | 农户贷 | 一般重要 | 非必要搭配，但会涉及 | 利用农村户籍身份，套场地、套附着物<br>种植、养殖业 |

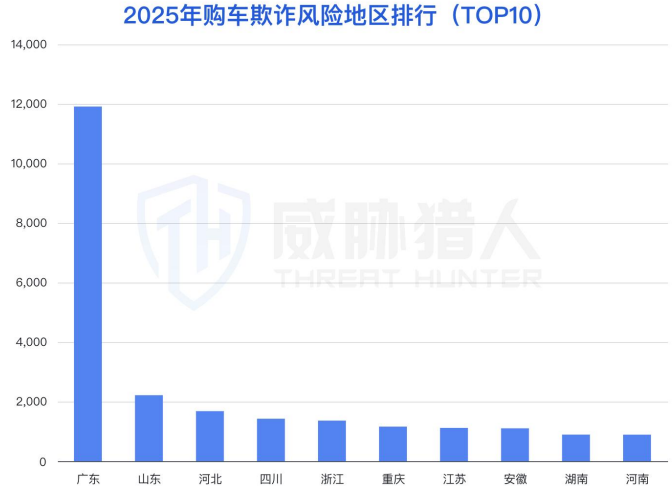
## 3.2.3 车贷欺诈风险：融车套现黑产链解析与区域态势预警

### （1）2025 年上半年购车欺诈风险有所波动，2025 年上半年比较 2024 年下半年下降 10%

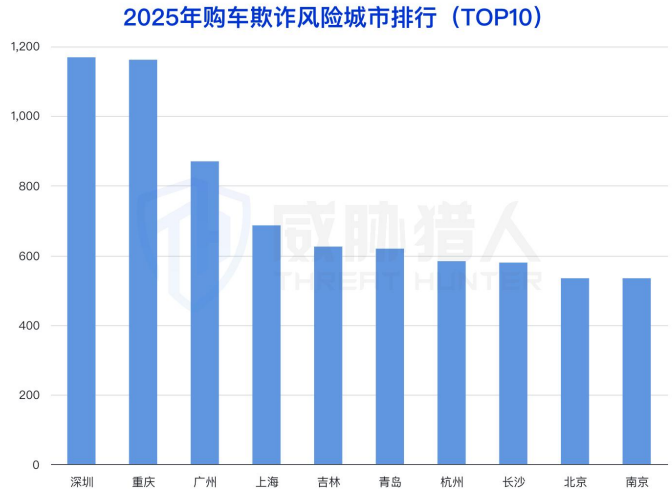



### （2）2025 年上半年购车欺诈风险地区 TOP3：广东、山东、河北

2025 年上半年购车欺诈风险地区最高的是广东省，且远高于其他省份。经深度分析，广东省购车欺诈风险高主要源于新型融车套现模式的区域性泛滥，而这类模式在其他地区较少应用。该模式具有两个显著特征：一是精准筛选具有真实购车资质（征信良好、收入稳定）且存在资金需求的用户；二是以"重真实资质、轻包装造假"的手法提升隐蔽性。

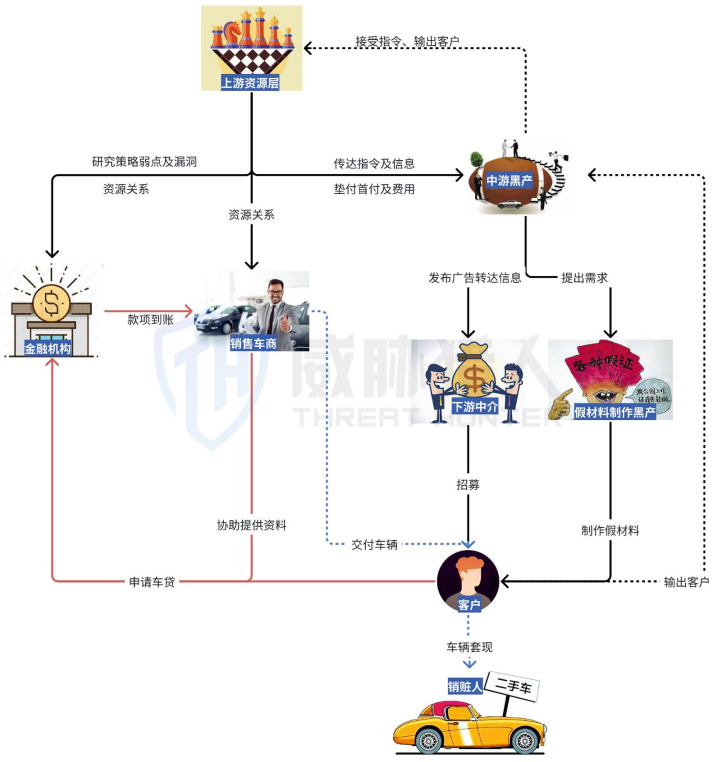


### （3）2025 年上半年购车欺诈风险城市 TOP3：深圳、重庆、广州




### （4）购车欺诈黑产链解析

购车欺诈已形成一套分工明确、流程清晰、环环相扣的黑产运作模式。黑产从筛选目标人群、招募客户贷款购车、迅速变现车辆，已构建出完整的黑产操作链条，呈现出高度组织化与成熟化特征。



**（5）车贷黑产模式固化但风险持续高位**

车贷业务中存在包括融车套现、传销购车、顶名车、买车包活等在内的多类风险。其中，融车套现风险构成最突出的威胁。

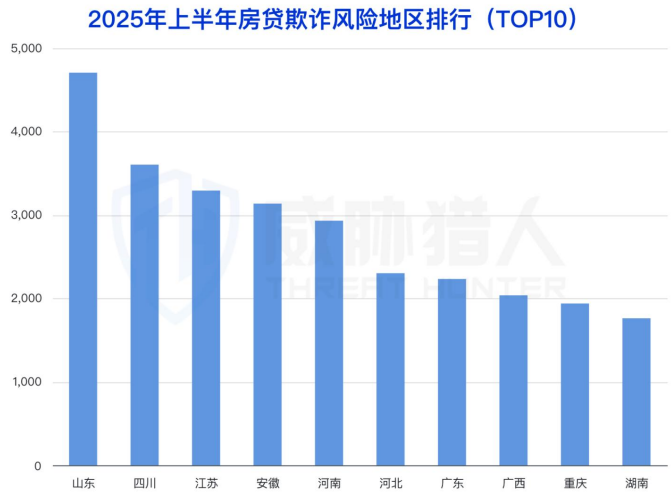
以下为车贷场景各欺诈风险模式的风险表现：

| 风险模式 | 风险表现 | 购车意图 | 风险值 |
| --- | --- | --- | --- |
| 融车套现 | 一人多贷、一车多贷<br>要钱不要车，车辆随即被变卖<br>背债环节中的一环 | 套现换资金 | 极高 |
| 传销购车 | 购车者为传销组织分子<br>传销组织以“消费积分优惠”、“0首付购车”、“低月供”等噱头引诱下级人员分期购车<br>所谓的“优惠”是与高额消费捆绑 | 真实用车 | 高 |
| 顶名车 | 一人多贷<br>以个人名义有偿帮第三方购车<br>第三方以‘真实用车’为名义骗取车辆，实则违规转卖套现 | 有偿代购 | 高 |
| 买车包活 | 买车包活：以买车提供工作为幌子，掉入分期购车的骗局高薪招募司机：<br>提供高薪司机岗位，引诱司机分期购车<br>前期承诺的“岗位”与实际不符，购车者受骗 | 购车是为了获取工作岗位 | 高 |

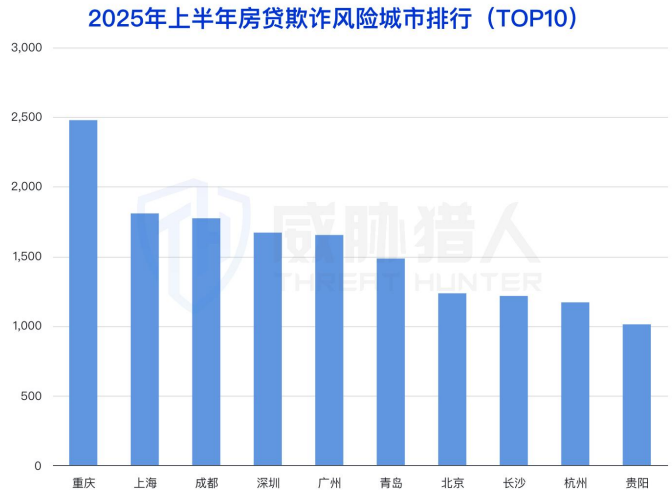
## 3.2.4 2025 年上半年房贷欺诈风险持续增长

**（1）2025 年上半年房贷欺诈风险持续增长，2025 年上半年比 2024 年下半年增长 63%**

### （2）2025 年上半年房贷欺诈风险地区 TOP3：山东、四川、江苏




### （3）2025 年上半年房贷欺诈风险城市 TOP3：重庆、上海、成都




### （4）房贷欺诈风险类型

在购房欺诈风险场景中，风险集中于两大核心欺诈类型。其一为购房按揭贷款欺诈，购房者以非真实居住需求购房，根本目的为融房套现或作为背债增信资产；其二为房产抵押贷欺诈，如常见的经营性抵押贷款转贷换贷、背债融资等。在这两类房贷场景中，实际申请贷款者均面临较大资

金缺口，特别是融房及背债的用户自身既无偿还贷款的能力，也无还款的意愿，风险直接转嫁给了银行机构，使得银行机构直接面临风险冲击。

## 3.3 电信网络诈骗场景分析

### 3.3.1 2025 年上半年电信诈骗数据趋势

2025 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 51 万条，环比 2024 年下半年下降 27.39%。但并非电诈退潮，而是多重因素叠加导致的阶段性“表象”：如各类社交、短视频平台打击涉诈话术、好旺担保等大型团伙被端、部分传播渠道切换至加密平台等。与此同时，黑灰产活跃群数量和涉诈账号规模仍在上升，表明电诈生态正加速向更隐蔽、更垂直的方向演化。


2025 年上半年，威胁猎人风险情报平台共监测到活跃作恶社交群组约 2.9 万个，环比 2024 年下半年上升 2.46%，月均活跃群数稳定在约 5000 个。在活跃群聊渠道中，以匿名群聊和社交群聊为主要大量级用户群的社媒平台，黑灰产持续依托社交平台进行组织化作案，涵盖推广仿冒链接、分发话术包、发布钓鱼页面等非法行为。


2025 年上半年，威胁猎人风险情报平台监测到涉及作恶黑产 4 万个账号，环比 2024 年下半年上升 7.61%，在持续打击下，黑灰产通过分散化、多账号操控等手段提升存活率，作恶行为反而更加隐蔽高频。


### 3.3.2 “无感盗刷”三重陷阱：技术引导、验证漏洞与仿冒伪装正在重构诈骗方式

随着支付系统和身份验证机制日趋智能化，黑灰产诈骗手法也在悄然升级。相比过去的“骗你点链接、输密码”，如今的不法分子更倾向于绕过你的感知与判断，用技术流程引导你“配合完成”或“被动失控”地完成支付操作。

2025 年上半年，威胁猎人风险情报平台监测到三类典型的新型诈骗手法正在广泛传播，它们构成了当下“无感盗刷”的三大模式：

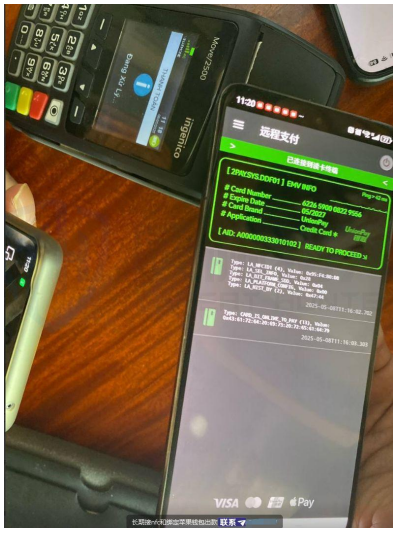
1.利用 NFC 技术实现远程传卡：本质上是利用通信技术突破物理验证场景，实现非接触式盗刷，用户并不知卡片信息已被“复制”。

2.企业代付骗局：利用验证漏洞操控支付流程：利用身份验证流程中的逻辑漏洞，绕过支付意图确认，让用户在“以为别人付款”的场景下，完成真实扣款。

3.仿冒 App 伪装诈骗：本质是利用仿冒官方权威形象伪装可信环境，诱导用户主动交出资金或信息。

**（1）滥用 NFC 免密，诱导“主动贴卡”，异地盗刷**

2025 年上半年，威胁猎人监测到多起涉及 NFC 盗刷的诈骗事件。犯罪分子利用“远程传卡”技术，诱导受害人将银行卡贴近手机，盗取 NFC 数据后远程仿真卡片，在境外或其他设备上完成盗刷，整个过程无需用户输入密码，即使卡未脱离本人掌控，仍可能被盗刷。



典型诈骗流程：

1. **冒充银行或金融平台客服**

诈骗者通过电话、短信、社交平台等方式，冒充银行风控人员，声称“你名下银行卡存在异常交易”，要求立即进行安全验证。

2. **引导安装伪装 App**

受害人被要求下载一个名为“账户安全助手”或“NFC 验证中心”的 App。该 App 仿冒正规银行界面，实则内嵌了 NFC 读卡模块和数据上传接口。

3. **诱导贴卡读取信息**

骗子指导用户“将银行卡贴近手机背面，配合完成芯片验证”，实则是诱导用户主动将卡片信息通过 NFC 方式上传给诈骗团伙。

4. **远程仿真盗刷**

诈骗团伙使用另一部支持 NFC 卡模拟的手机，在 POS 机上完成盗刷交易，等同于拥有一张“你本人的银行卡”。

5. **快速资金转移**

成功交易后，资金迅速被转入多个账户或用于虚拟币交易，受害人往往在数小时后才发现银行卡被盗刷。

### （2）“企业代付”被黑产滥用为支付引流入口，平台验证机制成漏洞入口

“企业代付”、“公司福利”、“免费充值”……看似是好事，其实正是骗子设下的“自掏腰包”陷阱。2025 年上半年，威胁猎人监测到一类以“企业代付”为幌子的新型诈骗正加速扩散。骗子伪装成平台客服、运营人员，打着企业补贴、员工福利的旗号，引导用户进入支付流程，并借助平台支付验证机制中的漏洞——如刷脸验证、快捷支付、免密授权等环节默认触发支付而非确认操作，最终让用户在未察觉自身正在执行真实支付操作的情况下完成扣款，等发现资金异常流出时，才意识到所谓“企业代付”根本不存在。


典型诈骗流程：

#### 1. 福利引流，放长线钓鱼

骗子在 QQ 群、微信群、短视频评论区发布“企业赠送会员”、“手机充值补贴”等广告，吸引用户添加他们的微信号或私信账号。

### 2. 伪装企业代付，引导充值

骗子伪装成客服、运营，称“为了匹配企业账户，需要你配合测试支付流程”，诱导用户进入某支付 App 的“手机充值”、“优惠券领取”、“订单付款”等页面。

### 3. 诱导点击验证，实为触发支付

骗子可能以“流程验证”、“支付测试”为由，引导你反复输入错误密码、刷脸认证，或让你在 App 中点击“免密开通”、“快捷支付模拟”等按钮。你以为只是配合操作，但由于平台验证流程存在漏洞，这些动作实际上触发了真实的扣款行为，导致资金在你毫不知情的情况下被转走。

### 4. 无感盗刷完成转账

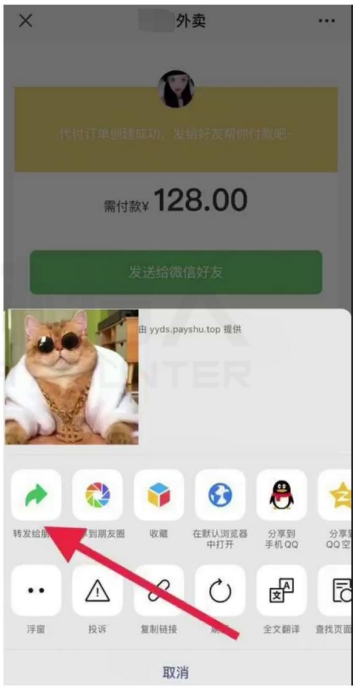
在某些支付平台或旧版客户端中，只要人脸识别成功、点击动作完成，系统便会默认执行支付操作，而没有弹窗确认或密码环节。

### 5. 盗刷完成，资金立刻被转移

用户毫无察觉地完成了支付，付款对象是骗子控制的账户，随后资金被迅速转出或通过虚拟币平台洗出，受害者往往在事后查看账单才发现异常。

### （3）仿冒 App 包装成正规平台，骗你一步步走进支付陷阱

在网络诈骗持续演化的趋势下，“仿冒”已经成为黑灰产高频使用的关键手段之一。从仿冒银行、快递、政务 App，到仿冒成人商城、社交平台、内部商城，诈骗者通过高度拟真的伪装界面和诱导话术，让用户在不知情中主动交出钱财、权限甚至隐私。


**仿真平台 + 情绪诱导：2025 年高发仿冒诈骗类型一览**

| 仿冒类型 | 场景描述 | 核心目标 |
| --- | --- | --- |
| 色敲诈骗App | 仿冒社交/私密聊天类App，诱导用户安装并上传私密信息 | 敲诈勒索、控制支付权限 |
| 情感操控型代付诈骗 | 诈骗团伙搭建仿冒电商、外卖、情趣用品平台，结合“网恋”、“情趣用品”等话术操控，引导受害人代付商品。平台页面高度仿真，付款流程与真实平台一致，但实际收款人为诈骗账户，用户付款即遭财产损失。 | 情绪操控 + 代付诈骗 |
| 电商优惠钓鱼页 | 仿冒拼多多、京东等优惠页面，以“员工内购”“隐藏补贴”等名义传播 | 窃取支付信息、引导付款 |
| 仿政务/快递App | 仿冒官方政务/物流App，发送“逾期未缴、快件异常”等提醒 | 社工欺诈 + 恶意程序植入 |

**典型案例剖析：仿冒商城引发的“代付诈骗”**

诈骗流程如下：

### 1. 感情养成，引导信任

黑产组织代聊人员在交友平台）注册女性账号，通过长时间聊天与受害人建立“线上恋爱”关系，稳定后引导“男方”履行“情侣义务”，提出买奶茶、水果、饭菜、药品等小额需求。

### 2. 下单仿冒商城，生成代付链接

代聊人员进入黑产提供的仿冒电商平台，平台页面几乎完全复刻某知名电商外卖首页，支持选择商品分类（如鲜花、水果、奶茶、药品等），填写虚假收货地址后生成“代付链接”或代付二维码。

### 3. 代付流程掩盖真实收款人

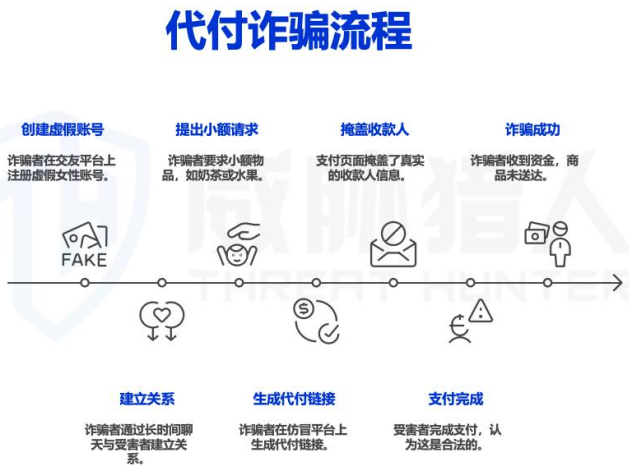
用户扫码后看到的是一个几乎完全正常的“商品付款页”，由于使用微信代付功能，付款人无法看到收货地址或收款人，仅看到商品名称和金额，极易误判为真实平台请求。

### 4. 风控绕过与多次转发技巧

黑产操作人员通常先将链接发至自己的微信小号测试有无风险提示，若无异常再转发给受害人，确保诈骗操作不被微信风控拦截。

### 5. 支付完成即为诈骗成功

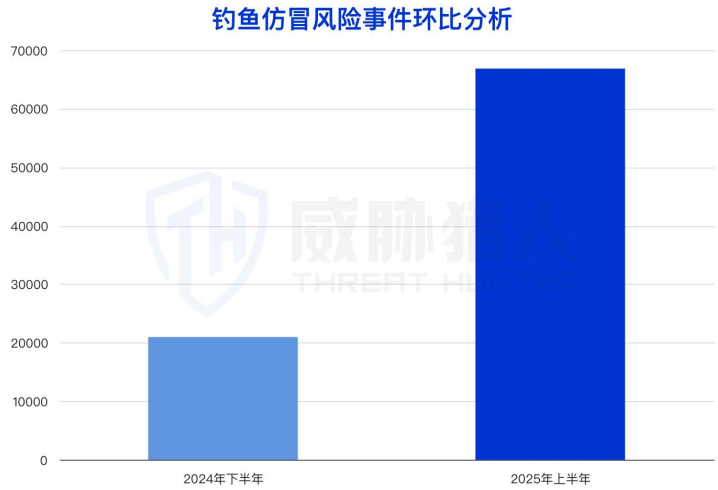
一旦代付成功，平台显示“已付款”，但商品从未真正配送，收款方为黑产账户。用户常因金额较小、对方态度亲密而不疑有他，甚至多次帮对方代付。




## 3.4 钓鱼仿冒场景分析

### 3.4.1 风险事件总量超 3 倍，社媒驱动及侵权成新攻击趋势

2025 年上半年，威胁猎人共捕获 66855 起钓鱼仿冒风险情报，相较于 2024 年下半年的 20968 起，呈暴增趋势，总量超 3 倍。这一爆炸式增长的背后，是攻击模式的系统性升级：传统的钓鱼攻击依然是“基本盘”，但以社交媒体为流量入口、以商品侵权为变现手段的新型攻击链条，正表现出强劲的增长势头，成为威胁情报增量的核心因素。



**商品侵权：** 指攻击者在各大电商平台中，公开售卖侵犯企业知识产权的商品。在本报告的语境下，它主要涵盖游戏私服的初始号、盗版软件激活码、破解账号等虚拟商品，是黑灰产将流量转化为收入的关键环节。

**仿冒网站：** 指攻击者创建的、在外观和域名上与官方网站高度相似的虚假网站。其主要目的是诱骗用户输入账号密码、个人身份信息、银行卡或支付信息等敏感数据，是网络钓鱼攻击中最直接、最常见的手段。

**仿冒社交媒体：** 指攻击者在社交平台、短视频平台等渠道上，注册并运营与官方品牌或个人形象高度一致的虚假账号。这些账号通常通过发布虚假活动、抽奖信息等内容进行引流，或直接与用户私信互动实施精准诈骗，是当前黑灰产最主要的流量入口和用户触达渠道。

**仿冒 APP：** 指攻击者制作的、在图标、名称和界面设计上模仿官方正版应用的恶意移动应用程序。这些应用通常通过第三方下载站、社交群组、短信链接等非官方渠道传播，安装后可窃取用户设备中的敏感信息或植入木马，是一种危害性极高的攻击形式。

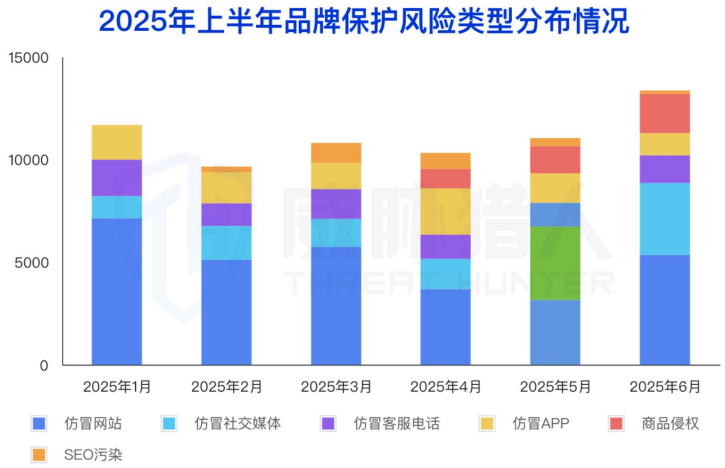
**仿冒客服电话：** 指攻击者利用虚假号码或通过改号软件伪装成官方客服热线，主动联系用户。攻击者通常以“订单异常”、“账户安全问题”等为由，利用社会工程学进行言语欺诈，诱导用户提供验证码、密码或直接进行转账操作，常用于诈骗的“收割”环节。

**SEO 污染：** 指攻击者利用搜索引擎优化（SEO）技术，将包含恶意代码或指向钓鱼网站的虚假页面，优化至搜索结果的前列。当用户搜索特定关键词（如“XX 官方客服”、“XX 软件下载”）时，会误入这些陷阱页面，这是一种通过劫持用户正常搜索意图来实现精准攻击的手段。

### （1）仿冒网站是攻击的基石、仿冒社媒、商品侵权增长强劲

在整个上半年，仿冒网站攻击事件累计捕获 30155 起，占风险情报总量的 45.11%，几乎为每月保持最高占比的单一风险类型 ，构成了网络钓鱼攻击的“底盘”。这表明通过搭建虚假站点来直接窃取用户账号、密码、支付信息等敏感数据，依然是攻击者最常用、最核心的手段。其体量之大，决定了它仍是品牌保护工作的首要防御阵地。

另值得注意的是，与商品侵权和仿冒社媒相关的攻击事件占比分别从 3 月和 4 月起有了明显的占比体现，表现出强劲的增长势头。



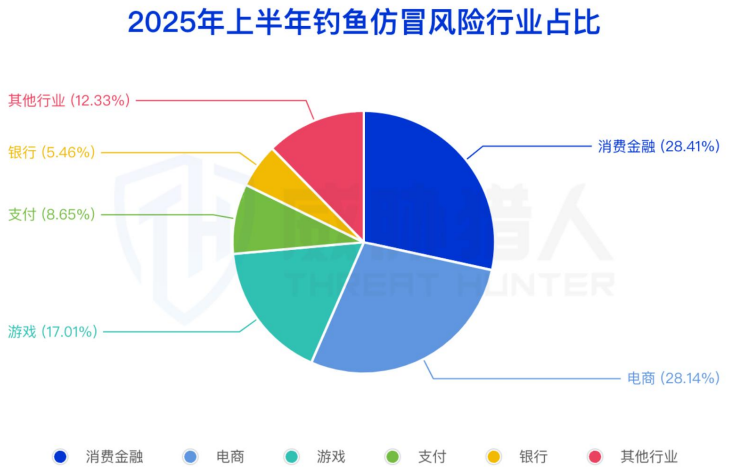

### （2）仿冒社媒与商品侵权呈现“协同增长”，驱动攻击模式变革

威胁猎人对游戏行业的持续监控发现，大量仿冒官方的社媒账号，其最终目的并非直接钓鱼，而是系统性地将用户引流至电商平台，购买私服、外挂等侵权商品。为完整揭示这条“前端引流、后端变现”的攻击链路，威胁猎人从 4 月起将“商品侵权”正式纳入监控。随后的数据清晰地验证了我们的判断：作为流量入口的仿冒社媒风险在 5 月激增至 3581 起，而作为变现渠道的商品侵权风险也从 4 月新纳入监控的 948 起，一路上升至 6 月的 1911 起。

这两条风险曲线的高度同步，标志着一个以游戏行业为起点，通过仿冒社媒引流、再以侵权商品变现的完整产业链攻击模式，已完全浮出水面。


## 3.4.2 泛金融领域与游戏 IP 成两大独立战场

2025 年上半年的数据显示，钓鱼仿冒风险呈现高度集中的态势。其中，泛金融领域是攻击最集中的重灾区，该领域以直接窃取资金为目标，包含消费金融（28.41%）、电商（28.14%）、支付（8.65%）、银行（5.46%），合计占比高达 70.66%，而以系统性瓦解商业模式为核心的游戏行业，占比为 17.01%。综合来看，泛金融和游戏这两大领域合计占比已近九成，构成了当前钓鱼仿冒攻击的主要战场。



**（1）泛金融领域：以资金为核心的直接掠夺生态**

泛金融领域（消费金融、电商、银行、支付行业合计占比高达 80.6%）因其直接处理海量资金流、支付信息和用户个人数据，成为网络钓鱼和诈骗的“天然狩猎场”。攻击者通过仿冒网站、支付页面、客服电话等手段，旨在窃取用户的银行卡号、密码、验证码等关键信息，实现资金的直接盗取。

**（2）游戏行业：以釜底抽薪的方式，系统性瓦解商业根基**

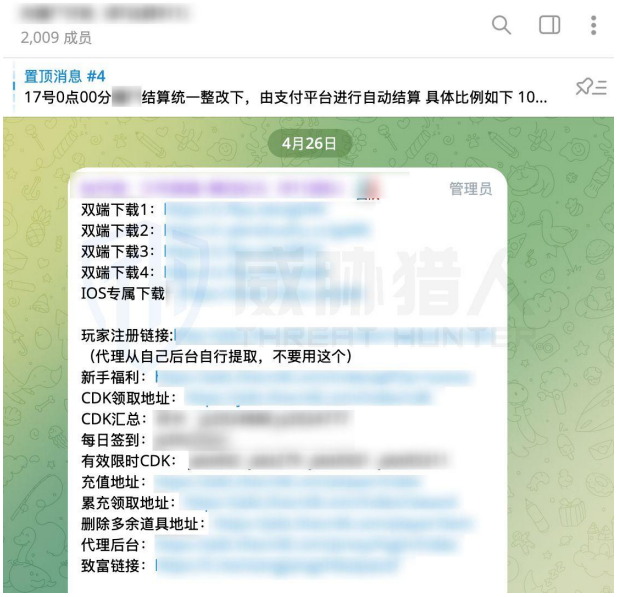
游戏行业的风险则源于完全不同的逻辑，其核心是如私服、外挂等知识产权侵权攻击。攻击者通过搭建私服直接复刻官方游戏，不仅侵蚀品牌价值，更重要的是分流核心付费用户、直接蚕食官方商业收入。这种攻击的本质，是对目标企业商业模式的系统性破坏，通过构建一个寄生的灰色产业链，掏空正版游戏的收入基础，缩短其生命周期。

## 3.4.3 揭秘游戏私服“引流矩阵”：一种系统性窃取品牌核心资产的黑产新范式

**（1）产业链结构：从技术源头到矩阵式分发**

游戏私服的猖獗，已从过去的“小作坊”演变为一个分工明确、多平台联动、自动化运作的黑灰产帝国。其核心不再是单一的推广链接，而是一个精心设计的、层层递进的“引流矩阵”：


**上游-技术源头**：由匿名的技术团队负责破解官方源码、搭建私服，并通过 Telegram 等加密渠道发布。这是整个黑产的“军火库”，是传统打击方式的难点。




**中游-渠道分发**：由专业的运营团队建立大量私服下载网站，并发展金字塔式的下线代理网络，构建起一个覆盖全网的、极具韧性的矩阵化分发渠道，封堵单一节点无法动摇其根本。

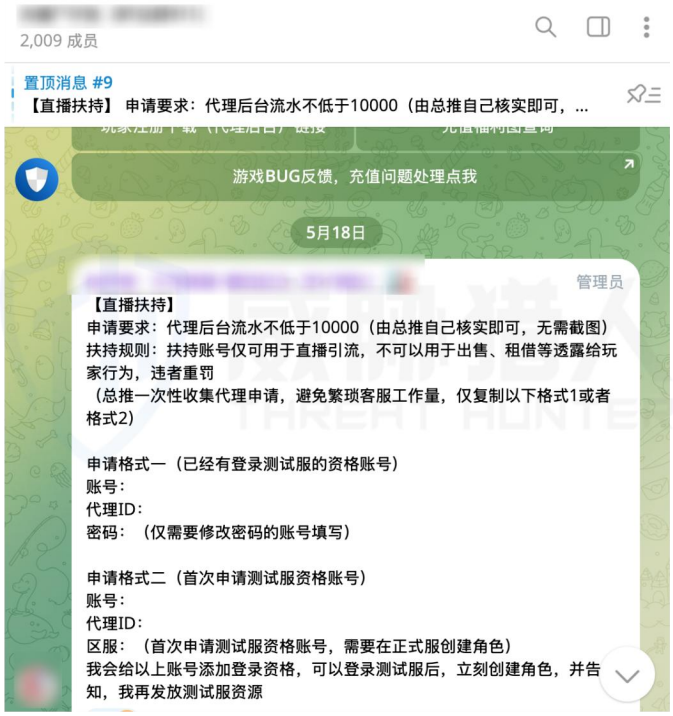
**下游-引流转化**：由数量庞大的代理商执行，负责将公域流量精准地转化为私域用户，是整个体系中最为活跃和庞大的一环。

### （2）核心运作：“引流-筛选-转化”的精准漏斗

下游的引流转化遵循一套标准化的三步曲，每一步都经过精心设计：

**初步引流（社媒曝光）：**

代理商注册大量账号，发布私服相关的“内部福利”、“高爆率”等诱惑性内容，进行广泛曝光，吸引潜在玩家的注意。一般有两种引流方法，一是在图文社媒平台发帖引流，二是在视频平台直播引流。

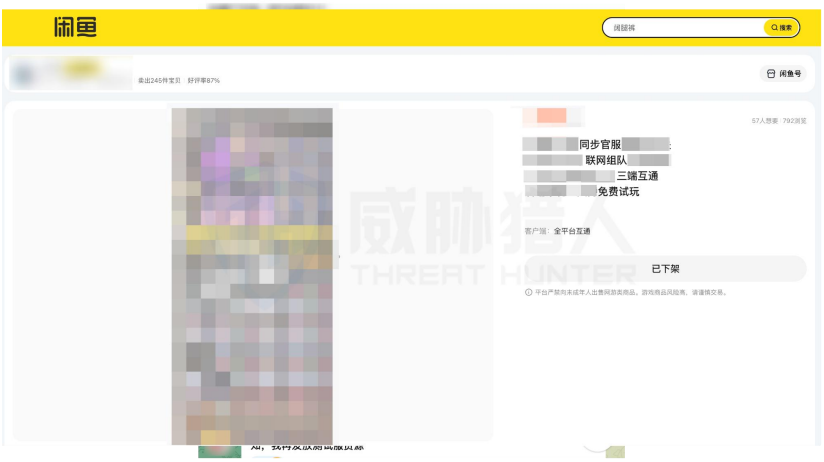



**深度引流（电商筛选）：**

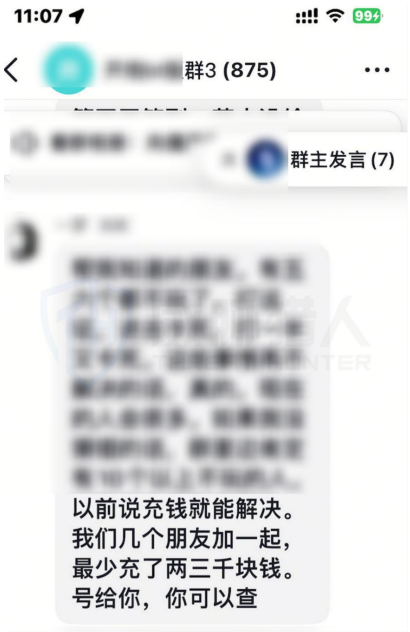
这是整个攻击链条中最关键的枢纽。 攻击者不会在社媒直接提供下载链接，而是引导用户去电商平台，购买价格仅为几元的“初始号”或“资源包”。此举一箭双雕：

- **筛选高价值目标：**付费行为本身就是一次高效的“意向筛选”，能从海量用户中精准识别出未来可能进行大额充值的“潜在金主”。

- **规避平台封禁：**相较于直接在社媒发布私服网站或私服 APP，这种“电商引流”模式更加隐蔽。因为攻击者发布的引流内容（如游戏攻略、福利领取等）本身不包含直接的违规信息，而是“既模糊又清晰”地引导用户至电商平台完成一个看似正常的交易。这使得游戏官方难以仅凭社媒内容进行有效投诉和封禁，从而极大地延长了整个攻击链路的存活时间。




- **最终转化（私域沉淀）：**用户购买后，通过客服引导或自动发货被拉入 QQ 群、微信群等私域社群。至此，黑产完成了从公域流量到私域资产的沉淀。在这个封闭的环境中，后续的大额充值、策反核心付费玩家等行为将完全脱离监管，品牌方不仅损失了收入，更永久性地失去了核心用户。



**（3）商业闭环：高额分成与匿名结算驱动的病毒式扩张**

这套体系能病毒式扩张，其核心驱动力在于其商业模式。威胁猎人独家情报显示，某私服代理商能获得高达 46% 的玩家充值返佣，并通过 USDT（泰达币） 等加密货币进行结算。这套“高佣金+匿名结算”的模式，极大地激励了下游代理商的扩张，同时也给追溯和打击带来了巨大挑战。


## 3.5 数据泄露场景分析

### 3.5.1 2025 年上半年数据泄露事件共 57092 起，较 2024 年下半年上升 1.54%

据威胁猎人数据泄露风险监测平台数据显示，2025 年 1 月至 6 月期间，全网共监测到 1.8 亿条情报线索。经真实性验证引擎与 DRRC 人工分析，其中确认为有效的数据泄露事件共计 57,092 起，较 2024 年下半年上升 1.54%。

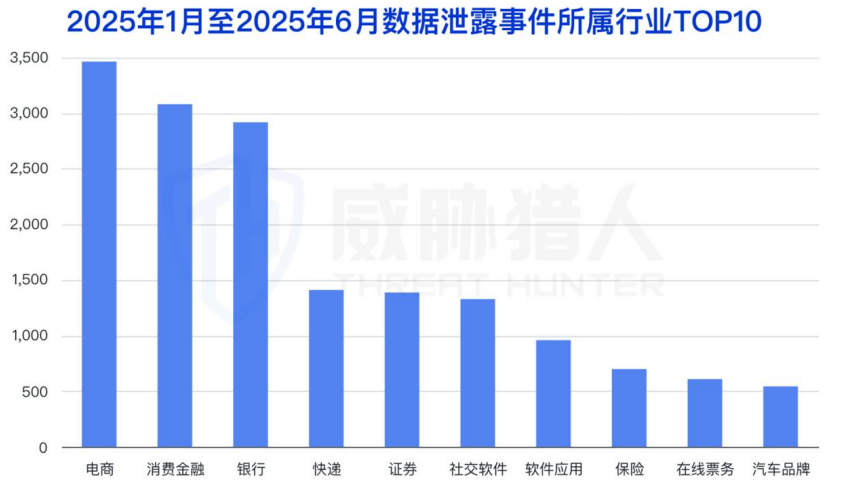
从上半年的数据泄露事件量的变化趋势来看，显示出了明显的异常波动，1-3 月呈上升趋势，4、5 月起攻击事件量连续下滑，6 月出现明显回升。


威胁猎人发现，这一波动与 Telegram 平台于 2025 年 4 月启动针对非法团伙的“封群行动”或存在强关联。该行动导致大量非法数据交易群被封禁，黑产交易渠道受阻，或直接导致数据泄露事件量下降。

从威胁猎人捕获数据分析发现：活跃的非法数据交易团伙数量从 3 月的 1,943 个减少至 4 月的 1,477 个，降幅达 23.98%；进一步分析发现，3 月活跃的团伙中有 33.71%在 4 月疑似遭遇封禁。与此对应的是，我方 2025 年 4 月监测到的数据泄露事件为 9,085 起，环比下降 29.93%。

然而，由于 Telegram 平台的封禁难以彻底，且非法团伙具备极强的“再生能力”，大量新群或替代群在短时间内重新活跃，推动了 2025 年 6 月数据泄露事件数量重新回升。

从行业分布来看，2025 年上半年全网数据泄露事件共涉及 76 个行业，TOP3 行业是电商、消费金融、银行。其中，以电商、金融为代表的高敏感度、高变现率行业，仍然是数据泄露的重灾区。

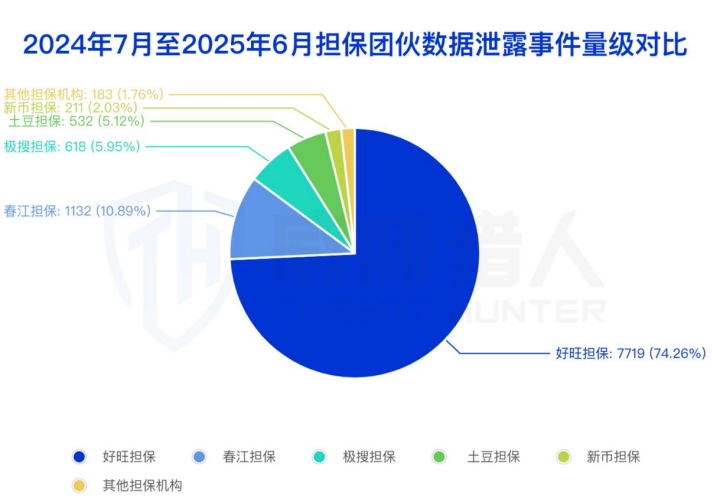



## 3.5.2 头部担保团伙遭打击，新担保迅速补位

**（1）好旺担保遭遇重创停运、短暂影响黑产数据泄露交易**

在非法数据交易市场中，数据供给端和需求端都高度活跃，形成了强烈的供需关系，也催生了完整的黑产交易链条。然而，由于交易本身存在高风险与高不确定性，买卖双方难以建立直接信任关系，担保群组作为中立“第三方担保人”机制应运而生。

其中，“好旺担保”（前身为“汇旺担保”）曾长期活跃于 Telegram 等匿名社交平台，凭借第三方信用中介服务，成为数据交易、诈骗、洗钱等黑产活动的核心担保平台，在 2025 年上半年及以前处于市场主导地位，以近一年事件数据来看，由其进行担保的数据泄露交易事件量占比高达 74.26%。

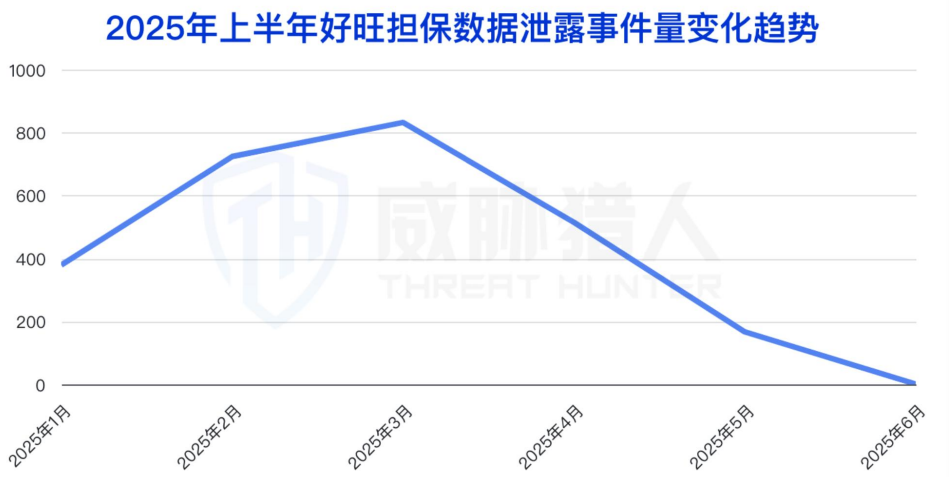



然而，在 2025 年 5 月，好旺担保遭遇重创。

- 5 月 1 日，美国金融犯罪执法网络（FinCEN）将其母公司 Huione 集团（汇旺）列为“首要洗钱关注”机构，切断其国际金融通道。随后 Telegram 官方于 5 月初集中封禁其交易群组及账号。

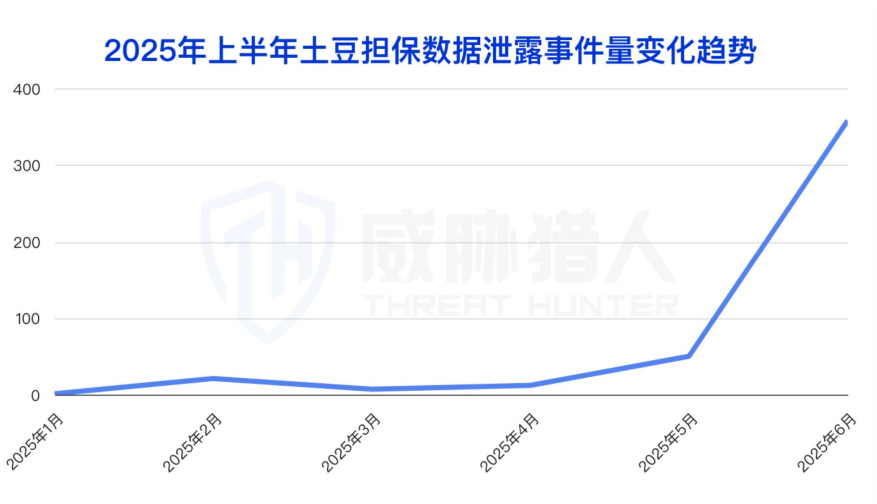
- 5 月 9 日，好旺官方发布公告称“交易员账号被大量注销”，至此，其运营体系全面崩溃，公群业务中断率达到 100%。


威胁猎人监测发现，自“好旺担保”停运后，其相关数据泄露事件量从 3 月的 832 件直线下降，至 6 月基本归零。



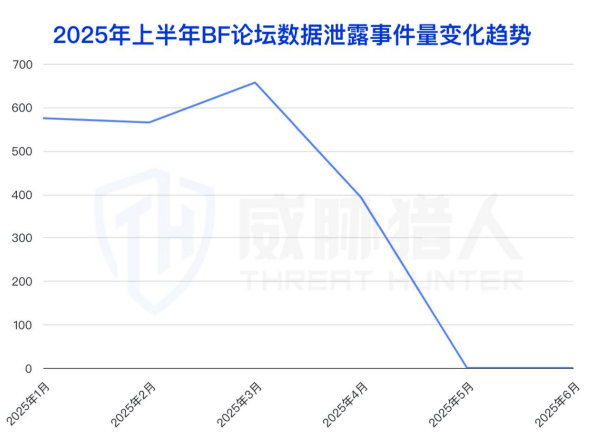

**（2）新担保迅速补位，交易快速恢复运转**

但黑产市场的需求并未消失。“好旺担保”倒下后，以“土豆担保”为代表的等新平台迅速崛起。数据显示，土豆担保涉及的相关的数据泄露事件从 4 月的 12 起暴增至 6 月的 358 起，增幅接近 30 倍。




黑产生态中逐渐出现了“担保平台”这一中介角色，中间商的存在不仅撮合交易，还承担着托管资金、仲裁纠纷的职能，是整个黑产交易能够持续运转的重要支点。正因如此，哪怕某个平台被打击清除，新的中间商也会迅速补位、变换马甲再次出现，只要交易存在，市场对这类“黑产服务商”的需求就不会消失，使得他们很难被彻底根除。

这一产业链定律在黑产交流传播的重要渠道源上也同样奏效。以头部暗网论坛 BF 为例，在 2025 年 4 月同样遭打击，关停前贡献暗网渠道近 15%数据事件。尽管黑产平台面临持续高压打击，但数据交易的市场需求始终未见减弱。以头部暗网论坛 BF 为例，2025 年上半年，该平台依然是全球范围内最主要的数据泄露供给节点之一。



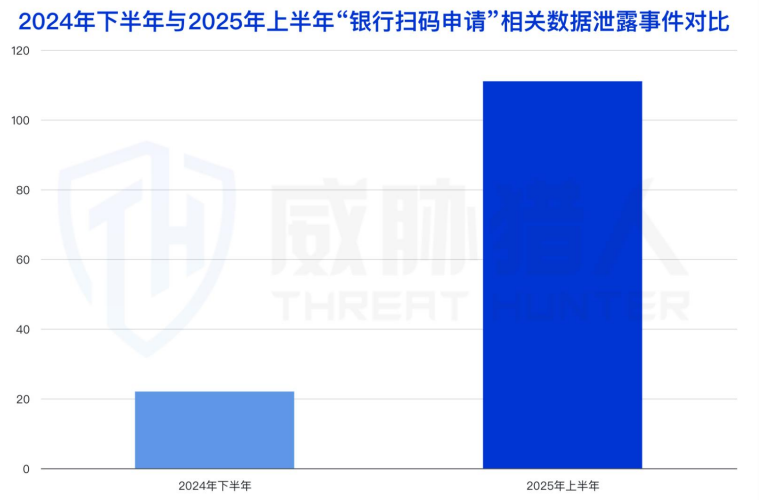
BF 的案例印证了黑灰产市场的核心规律：当主要交易平台被打击时，用户和需求会迅速迁移至现有或新兴替代品。数据交易市场具备极强的适应能力，即使头部平台被摧毁，黑产从业者仍能依托其他渠道维持业务运转。

## 3.5.3 银行“扫码申请”贷款信息泄露事件较比 2024 年下半年大幅上升，涨幅超过 4 倍

### （1）银行“扫码申请”贷款信息泄露事件上半年暴增

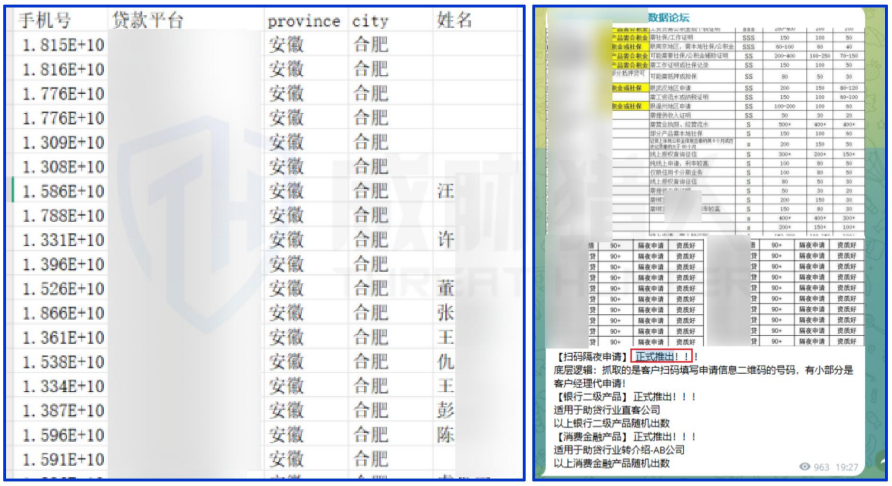
威胁猎人持续监测发现，在 2025 年上半年所捕获的泄露数据中，还有另一类名为“银行扫码申请料”的贷款信息泄露事件，共计 111 起，相较于 2024 年下半年新增 89 起，涨幅高达 404.55%。

**银行扫码申请：**是指用户通过扫描银行客户经理提供的贷款活动二维码，申请办理贷款业务的信息数据。




通过深入分析，威胁猎人了解到黑产中所称的“扫码申请隔夜”数据，其主要集中在银行“贷款”业务上。主要包含贷款用户的手机号、城市地区以及申请贷款审批结果等信息；同时，根据黑产

提供的银行贷款平台筛选上来看，共超过 80 家银行贷款业务，基本上以地方性银行或商业银行为主。

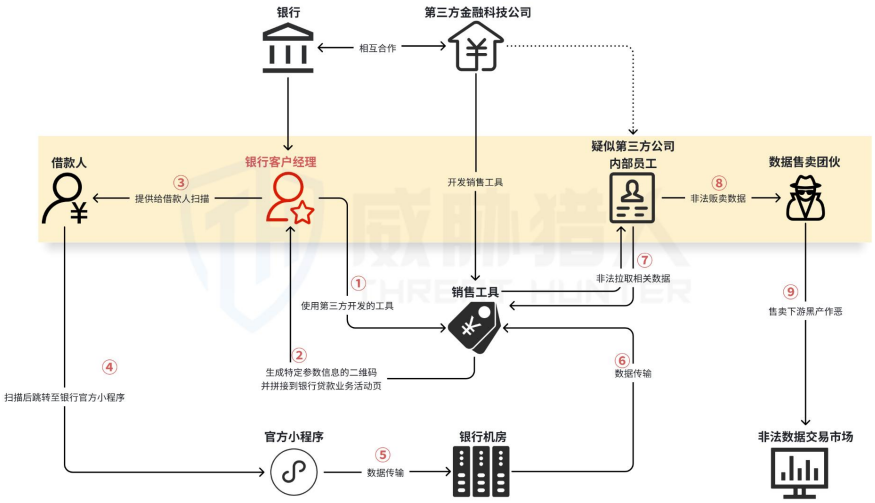


| 手机号 | 贷款平台 | province | city | 姓名 |
|---|---|---|---|---|
| 1.815E+10 | | 安徽 | 合肥 | |
| 1.816E+10 | | 安徽 | 合肥 | |
| 1.776E+10 | | 安徽 | 合肥 | |
| 1.776E+10 | | 安徽 | 合肥 | |
| 1.309E+10 | | 安徽 | 合肥 | |
| 1.308E+10 | | 安徽 | 合肥 | |
| 1.586E+10 | | 安徽 | 合肥 | 汪 |
| 1.788E+10 | | 安徽 | 合肥 | |
| 1.331E+10 | | 安徽 | 合肥 | 许 |
| 1.396E+10 | | 安徽 | 合肥 | |
| 1.526E+10 | | 安徽 | 合肥 | 董 |
| 1.866E+10 | | 安徽 | 合肥 | 张 |
| 1.361E+10 | | 安徽 | 合肥 | 王 |
| 1.538E+10 | | 安徽 | 合肥 | 仇 |
| 1.334E+10 | | 安徽 | 合肥 | 王 |
| 1.387E+10 | | 安徽 | 合肥 | 彭 |
| 1.596E+10 | | 安徽 | 合肥 | 陈 |
| 1.591E+10 | | 安徽 | 合肥 | |




**（2）银行“扫码申请”贷款信息泄露：第三方金融科技公司营销工具成核心风险点**

威胁猎人通过对泄露数据涉及到的银行二维码进行分析溯源，发现其均指向同一家知名金融科技服务商开发的“xx 营销助手”平台。结合黑产发布的银行贷款平台名单来看，可以确认影响范围超过 80 家银行机构。



基于该类相关事件涉及多家银行，根据威胁猎人针对具体细节进行深入还原发现：

1. 用户在申请贷款的过程中，是通过扫描银行客户经理所提供的贷款业务活动二维码进行办理；

2. 这一类银行贷款业务的二维码信息携带着客户经理信息，去跳转到银行官方的小程序上；

3. 然后用户在银行官方小程序具体的贷款业务上操作提交贷款申请。

威胁猎人了解到客户经理所提供的贷款二维码信息，实际上是通过第三方金融科技公司开发的销售工具进行制作的（由于该工具页面较为敏感，此处不做具体展示）。

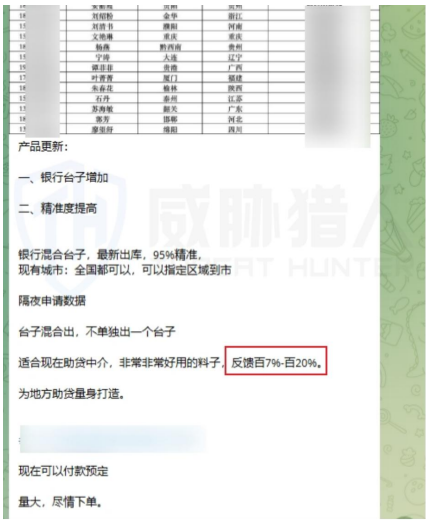
威胁猎人针对该第三方金融科技公司进行分析后发现，该公司不仅为银行提供应用系统软件开发，还提供智能风控策略。针对不同资质的贷款用户提供不同的风控策略，用于配合银行客户经理进行跟进，主要为银行提供业务数字化，推动银行贷款业务发展。用户在银行官方小程序提交地贷款申请后，银行会将用户相关信息同步至销售工具上，便于银行客户经理业绩统计以及跟进，与此同时也带来了数据泄露的风险。

| 隔夜申请平台推荐 | | | | 每日出量（三网）不固定 预计出量 | | |
|---|---|---|---|---|---|---|
| 平台名称 | 是否需要公积金 | 其他材料/备注 | 推荐级别 | 一线及高配二线 | 二线 | 三线及以下 |
| | 部分产品需公积金 | 本地户籍优先 | SSS | 200左右-300 | 100-200 | 40-100 |
| | 否 | 需银行流水或工资证明 | SSS | 200左右-300 | 100-200 | 40-100 |
| | 部分产品需公积金 | 需公积金或个税证明 | sss | 250-400 | 200 | 100 |
| | 部分产品需公积金 | 需社保/工作证明 | SSS | 150 | 100 | 50 |
| | 需公积金或社保 | 限南京地区，需本地社保/公积金 | SSS | 60-100 | 60 | 40 |
| | 部分产品需公积金 | 可能需要社保/公积金辅助证明 | SS | 200-400 | 100-250 | 70-150 |
| | 部分产品需公积金 | 需工作证明或社保记录 | SS | 150 | 100 | 50 |
| | 否（部分抵押贷可能需） | 可能需抵押或担保 | SS | 80 | 50 | 30 |
| | 需公积金或社保 | 限武汉地区申请 | SS | 200 | 150 | 80-120 |
| | 否 | 需工资流水或纳税证明 | SS | 150 | 100 | 60-100 |
| | 需公积金或社保 | 限温州地区申请 | SS | 100-200 | 100 | 60 |
| | 否 | 需提供收入证明 | SS | 50 | 30 | 20 |
| | 否 | 需营业执照、经营流水 | S | 500+ | 400+ | 400+ |
| | 否 | 部分产品需本地社保 | S | 150 | 100 | 60 |
| | 需要 | 征信上体现公积金信息且缴纳满6个月或历史记录缴纳大于60个月 | s | 200 | 150 | 50 |
| | 否 | 线上授权查询征信 | S | 300+ | 200+ | 150+ |
| | 否 | 纯线上申请，利率较高 | S | 100 | 80 | 50 |
| | 否 | 仅限信用卡分期业务 | S | 100 | 80 | 50 |
| | 否 | 线上授权查询征信 | S | 80 | 50 | 30 |
| | 否 | 需提供工作证明 | S | 50 | 30 | 20 |
| | 否 | 需绑定 银行卡 | S | 200 | 150 | 30 |
| | 否 | 需绑定 账户，利率较高 | S | 150 | 80 | 30 |
| | 否 | | s | 400+ | 400+ | 300+ |
| | 否 | | s | 200+ | 150+ | 100+ |
| | 否 | 线上申请，需人脸识别 | A | 150-200 | 100-150 | 100+ |
| | 否 | 需提供银行流水 | A | 150-200 | 100 | 80 |
| | 否 | 需授权查询征信 | A | 100 | 80 | 30 |
| | 否（抵押贷可能需） | 可能需房产/车辆抵押 | A | 80 | 50 | 20 |
| | 否 | 线上申请，需人脸识别 | A | 100 | 70 | 30 |

据威胁猎人针对黑产发布的信息进行跟进以及分析后发现，在此类型事件开始宣传时，黑产声称，数据是来源于“内鬼”，即内部员工泄露的。结合上文中涉及到超过 80 家银行机构，80 家银行机构内部员工泄露的概率极低，初步推断为第三方金融科技公司内部员工。



根据威胁猎人调研发现，此类信息数据泄露到非法数据交易市场后，主要用于助贷公司进行精准营销。同时，根据黑产在营销后的效果反馈上来看，效果是非常好，成功率最高可达 20%，也在侧面证明了此类数据的真实性。



**风险与危害：**

**客户流失与营收损失：** 高意向客户在申请次日即被竞争对手（助贷公司）联系，提供利率更低或审批更快的替代产品，直接导致银行潜在客户流失，损失可预期的利息收入和中间业务收入。

**品牌声誉损害：** 数据泄露严重打击了用户对银行数据安全能力的信任，尤其是在贷款这一核心业务上，将对银行品牌造成长期负面影响。”

**监管合规风险：** 此类事件已构成严重的个人金融信息泄露，违反了《个人信息保护法》等相关法规，银行作为数据处理者将面临高额罚款和监管问责的风险。

## 3.6 API 安全场景分析

数字化与线上化趋势下，API 接口作为应用连接、数据传输的重要通道，近年来大规模增长。API 应用的增速与其安全发展的不平衡，使其成为恶意攻击的首选目标，围绕 API 安全的攻防较量愈演愈烈。

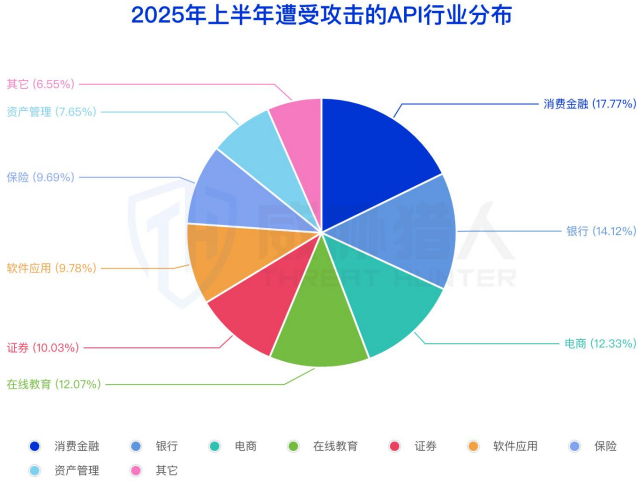
威胁猎人情报数据显示，2025 年上半年遭受攻击的 API 数量超过了 149 万，涉及消费金融、银行、电商、在线教育、证券等多个行业。

### 3.6.1 2025 年上半年月均遭受攻击的 API 数量超 24.9 万

威胁猎人监测显示，2025 年上半年每月捕获 API 攻击量呈上升趋势，月均遭受攻击的 API 数量达 24.9 万个，较 2024 年下半年 19.4 万个显著增加，月均增长量达 5.5 万个，增幅达 28.35%，增长趋势明显主要是因为金融行业受黑灰产攻击增多导致总体趋势上升。


## 3.6.2 金融业成首要靶标，消费金融风险登顶

2025 年上半年，威胁猎人蜜罐平台共监控到近 150 万起 API 攻击事件，波及 1,176 家企业。从行业维度来看,攻击高度集中于消费金融、银行、电商、在线教育及证券五大行业；其中，消费金融、银行与证券构成的金融业遭受攻击为重灾区，攻击占比高达 41.92%，消费金融行业更是攻击者的首要目标。



从攻击主体量级来看，2025 年有 209 个消费金融公司被攻击，在 API 遭受攻击行业中占比高达 17.77%，攻击主要集中在持牌消费金融公司，互联网平台金融业务、转型助贷平台和小额贷款公司。经分析，消费金融公司被黑产高度关注的原因主要有以下三方面：

1. **数据收集与流转的复杂性剧增：** 消费金融平台业务深度嵌入电商、社交等复杂场景，导致用户数据来源广、类型杂，平台与合作方之间的数据流转链条冗长且脆弱。攻击者往往利用链条中任一环节的接口薄弱点，发起信息窃取、撞库等攻击。

2. **开放生态下的 API 接口爆炸式增长：** 为支撑复杂的嵌入式金融场景（如场景分期、信用支付、联合风控），平台需向大量内外部合作伙伴（商户、技术服务商、数据源）开放海量且功能各异的 API 接口。接口数量的激增和调用关系的复杂化，显著扩大了攻击暴露面。安全管理若未能同步精细化，极易被攻击者利用进行接口探测、未授权访问乃至大规模撞库攻击。

3. **高敏数据价值高带来的利益驱动：**消费金融平台集中存储海量用户敏感信息（身份、征信、财务等），这些敏感信息在黑市中单条价格可达 100 元，远超其他行业数据，对攻击者形成巨大诱惑。

## 3.6.3 2025 年上半年值得关注典型 API 攻击典型事件

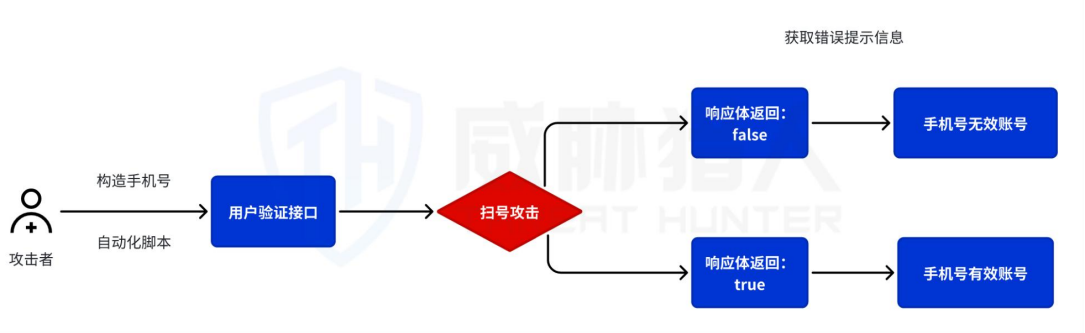
威胁猎人监控到黑产通过 API 攻击涉及下游多个作恶场景，涵盖薅羊毛、恶意刷单、数据爬取、营销业务欺诈及库存预留等。2025 年上半年监测数据显示，支撑这些恶意活动的核心 API 攻击手段集中于扫号攻击、撞库攻击与占库攻击。

**（1）扫号攻击：某互联网平台线上业务遭受黑灰产扫号攻击，大量用户信息被泄露**

2025 年 3 月，威胁猎人监测到攻击者对国内某互联网平台发起扫号攻击，2 月至 3 月期间，攻击者使用代理 IP 对该平台接口发起超 10 万次攻击，导致 5 万有效账号暴露。

经过流量分析与复现，发现该平台用户验证接口，已注册用户和未注册用户验证返回响应体数据存在明显差异，因此黑产通过该接口大批量验证手机号是否为平台注册用户，导致有效账号暴露，用户隐私泄露。

具体攻击流程如下图所示，黑产对请求体进行构造，使用不同的手机号，而其他鉴权参数信息特征保持不变，黑产可以通过回显来判断手机号是否为有效账号，如果手机号码为无效账号，回显“false”，如果手机号码为有效账号，平台回显“true”。

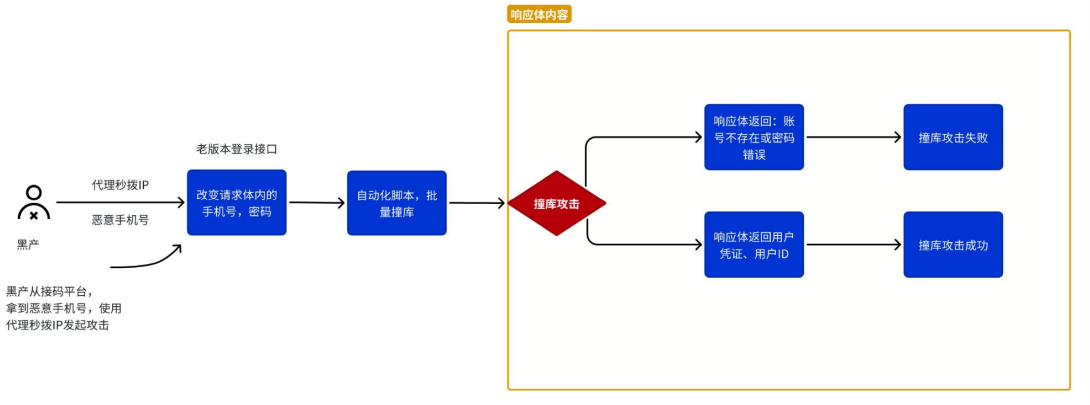



**（2）撞库攻击：老旧登录接口未下线成撞库突破口，某平台遭批量撞库攻击**

从威胁猎人蜜罐捕获的流量发现，在 2025 年 5 月，攻击者使用代理 IP 对该平台老版本登录接口发起攻击超 30 万次，撞库成功近 3000 个账号。

深入分析，攻击者攻击接口为该平台老版登录接口，该接口存在明文密码传输缺陷，缺少动态签名、人机验证，从而使黑产可以通过极低的成本绕过安全防护，对账号体系造成威胁。撞库攻击得逞后，攻击者通过盗用的账户凭证，恶意发起高频付费操作，造成原账户持有人实质经济损失。

攻击流程如下图所示，黑产利用老版本登录接口发起撞库攻击，由于老版本接口缺少频次限制和明文密码传输缺陷，攻击者针对请求体中的 Mobile 字段和密码字段，使用自动化脚本攻击，基于响应体返回的数据内容不同，判断是否撞库成功，撞库失败，响应体信息返回“账号不存在或密码错误”，撞库成功，响应体返回用户凭证、用户 ID 等敏感信息。

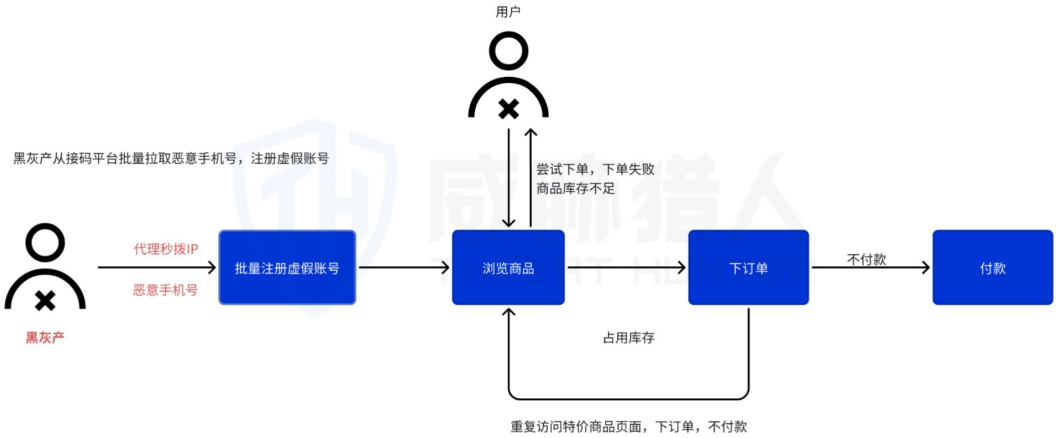



**（3）占库攻击：某平台接口漏洞被利用实施占库攻击获利**

2025 年 6 月，威胁猎人蜜罐捕获攻击者利用代理秒拨 IP 及接码平台手机号发起的批量攻击流量，具体针对某电商店铺接口发起攻击 10 万次，批量占库 1 万件特价商品，自购套利。

深入分析，目标接口存在高危漏洞：异常账号可对特价商品无限次加购并生成待支付订单，直至库存耗尽。后续该账号再批量下单商品，第三方平台兜售，实现套利。

攻击流程如下图所示，黑产通过接码平台获取海量虚假号码，叠加代理秒拨 IP 池技术，批量注册该平台傀儡账号，恶意挤占特价商品库存。其通过虚假账号自购订单完成套利洗货，同时也致使正常用户无法成交，破坏平台公平交易生态。




## 写在最后：

对企业而言，必须充分认识到与黑产的攻防博弈是长期、动态且持续演进的过程。唯有依托覆盖全网、跨平台的黑灰产情报数据，才能从攻击“尚未发生”阶段就提前识别潜在威胁，在攻击资源筹备、工具调度、路径构建等阶段实现精准溯源与前置拦截——清楚黑产将用什么资源、走哪条路径、以何种方式实施攻击，才能真正做到“敌未至，我先控”。

这正是情报的价值所在，也是威胁猎人持续投入的方向：通过系统化的黑灰产攻防研究与情报监测能力，帮助企业在对抗中掌握主动权，构建更具韧性的业务安全防线。

**说明：**本报告所提供的数据信息系威胁猎人依据大样本数据抽样采集、小样本调研、外部情报数据采集、数据模型预测及其他研究方法估算、分析得出，由于统计分析领域中的任何数据来源和技术方法均存在局限性，依据上述方法所估算、分析得出的数据信息仅供参考。

威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

关注“威胁猎人”

公司官网：www.threathunter.cn

合作邮箱：Marketing@threathunter.cn