威胁猎人
THREAT HUNTER

2025 洞见未来
互联网反欺诈年鉴

黑产大数据

2025年互联网黑灰产趋势年度总结

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。

目录

前言

过去一年，互联网黑灰产并未因监管趋严而退场，反而在资源结构、作恶方式与技术路径上发生了显著演化。

威胁猎人基于对黑产情报体系的持续监测发现：2025 年，黑灰产正在从“堆资源、拼人力”的传统模式，转向更隐蔽、更低成本、更接近真实用户行为的“类真人化、智能化作恶”阶段。

报告内容关键点总结：

攻击资源层面：拦截卡、劫持代理、真人众包等“更像真人”的资源大规模替代传统猫池卡；相较以往高度可识别的黑资源，这类资源更贴近真实用户与真实设备形态，显著提升了攻击隐蔽性与存活周期，也加大了溯源与治理难度。

攻击技术层面：生成式 AI 与智能体技术的爆发，不仅为业务创新带来了机遇，也为黑灰产提供了低门槛、高效率的自动化作恶工具。同时，在非 AI 技术方面，自动化工具突破人脸活体检测“三色炫光”防线，传统的基于颜色匹配的防御策略面临挑战

在攻击场景方面，

- **业务欺诈：**以高补贴、高流量场景为核心，黑产围绕营销补贴和业务规则进行系统性利用；黑产自动化作恶进入“智能体阶段”。
- **信贷欺诈：**职业背债风险舆情量较 2024 年增长 168%，从贷款类型来看，企业贷欺诈风险、信用贷欺诈风险、房贷欺诈风险位列前三；恶意贷款欺诈风险值广东风险值远超其他地区。
- **钓鱼仿冒：**从传统的“点链接”进化为“GEO 投毒”认知劫持，通过污染 AI 搜索引用的高权重信息源，诱导主动寻求帮助的用户拨打虚假客服电话。
- **数据泄露：**泄露风险高度集中于“泛金融”板块，且黑产已进入利用 AI 模型对“消金申请”等高价值数据进行清洗与质量控制以提升诈骗转化率的新阶段。

面对不断演进的黑灰产威胁，威胁猎人发布《2025 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。

01

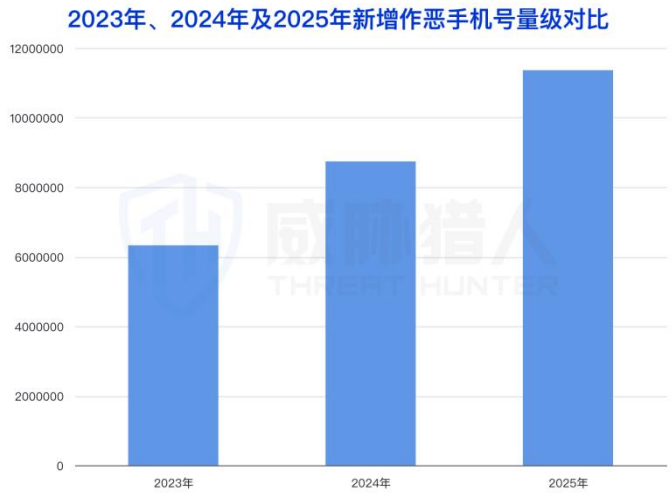
2025 年
黑灰产攻击资源分析

一、2025 年互联网黑灰产攻击资源分析

1.1 2025 年作恶手机号资源分析

1.1.1 2025 年国内作恶手机号新增数量超 1100 万，较 2024 年提升 30.02%

据威胁猎人情报平台数据显示，2025 年，国内作恶手机号新增量级超 1100 万，较 2024 年提升 30.02%。



黑产作恶的主要手机号资源有两种类型：

猫池卡：手机卡掌握在黑产手中，并插在特殊设备“猫池”上收发短信验证码，属于传统接码手机号。

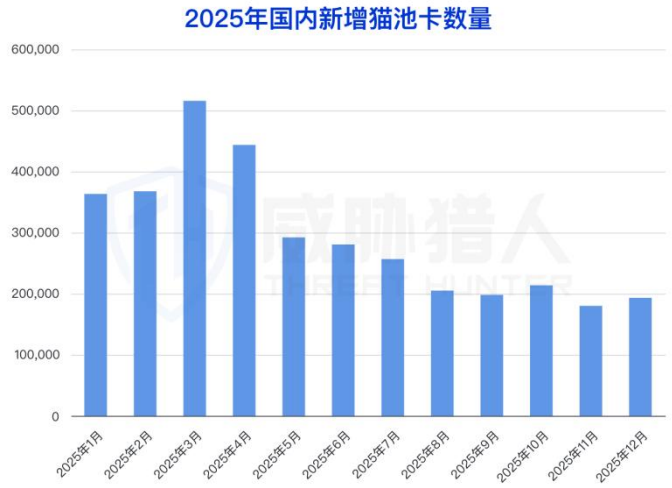
拦截卡：手机卡插在正常人持有的设备上，设备存在后门导致短信验证码被黑产拦截。

据威胁猎人情报平台数据显示，在 2025 年全年新增国内作恶手机号资源中，拦截卡资源占比由 2024 年的 39.5%提升至 2025 年的 69.23%。下文 1.1.2 和 1.1.3 将重点分析“猫池卡”和“拦截卡”资源的变化情况。

1.1.2 2025 年国内猫池卡资源变化趋势

（1）2025 年国内新增猫池卡 349 万，较 2024 年下降 33.85%

据威胁猎人情报平台数据显示，2025 年国内捕获新增猫池卡 349 万个，较 2024 年下降 33.85%。



从 2025 年国内猫池卡数量的变化趋势来看，自 4 月起，新增国内猫池手机卡数量呈现下滑趋势。

经威胁猎人情报专家分析，出现这一趋势的主要原因是：

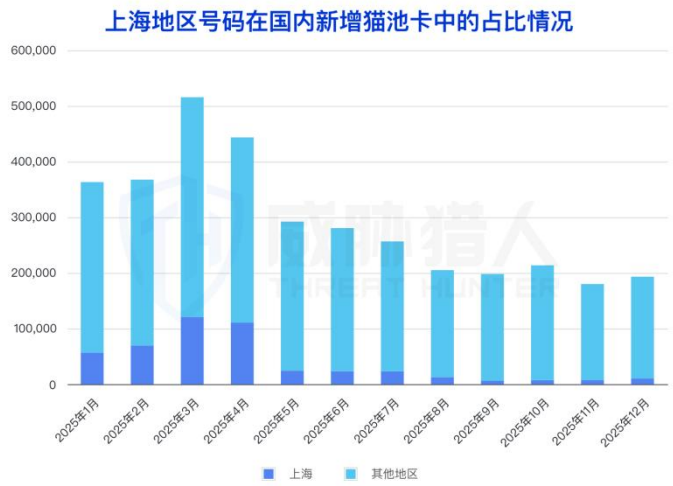
1、上游黑卡卡商供给收缩

受监管打击影响，多个卡商机房关停、部分卡商被捕，猫池卡整体供给能力明显收缩，直接导致新增猫池卡数量下降。

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。2025 年 1—4 月期间，上海地区猫池卡新增数量持续上升，并于 3 月达到阶段性峰值，当月来自上海的新增猫池卡占国内新增总量的23.42%。

然而，2025 年 5 月监管集中打击行动中，上海卡商首当其冲受创，多个机房关停、卡商被捕，导致供给端快速收缩，新增猫池卡数量下降，5 月份当月国内新增猫池卡中仅有 8.32%来自上海。

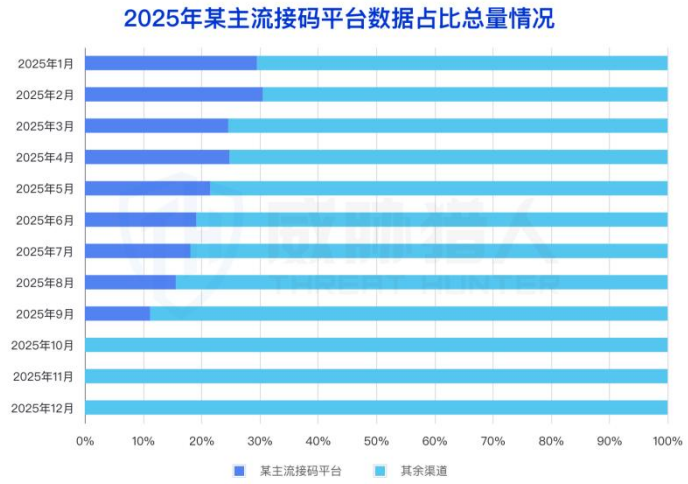
上海新增黑卡数量在监管打击期间大幅下降，导致全国猫池卡整体数量下滑。



2、某主流接码平台停止运营

某主流接码平台在 2025 年 1—9 月期间累计捕获猫池卡数量超过百万，长期承担着黑灰产的重要接码需求。

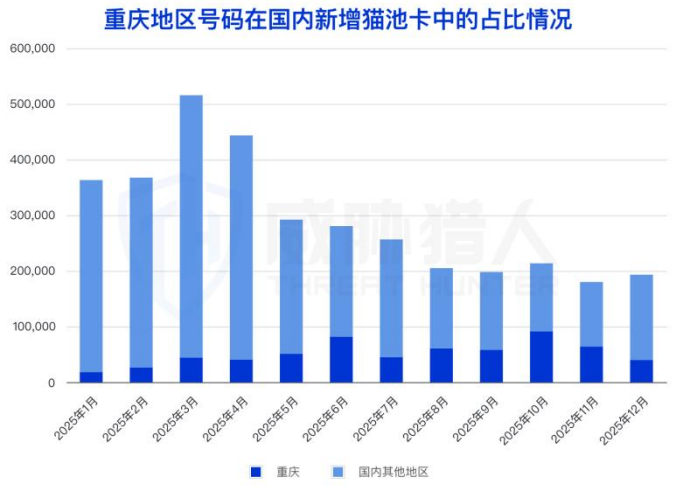
然而，年内该平台频繁出现服务器波动，平台稳定性显著下降，导致接码成功率骤降，黑产日常违规操作节奏被持续干扰；进入 9 月后，该平台最终彻底停止运营；这进一步阻断下游黑卡供给链路。



（2）2025 年国内新增猫池卡归属省份 TOP3：重庆、上海、广东，归属于重庆地区的猫池卡新增数量由 2024 年第九名上升至 2025 年第一名

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

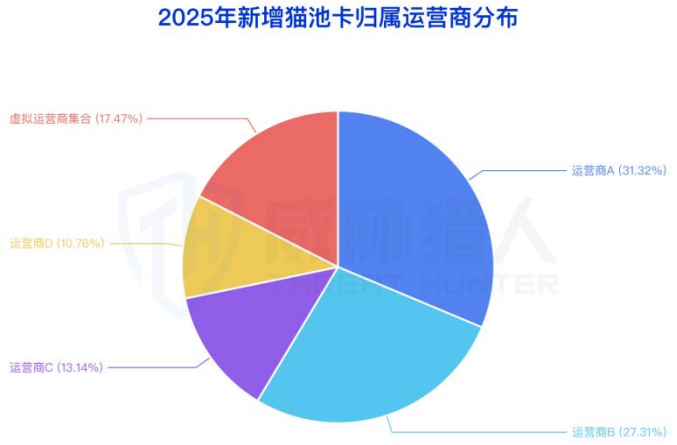
其中，归属地在重庆的猫池卡数量同比 2024 年增长了 106.63%，对比 2024 年排名上升了 8 位。威胁猎人关注到，今年重庆的猫池卡在全年各月均保持较高数量。



威胁猎人研究人员进一步分析发现，重庆地区新增猫池卡的运营商分布呈现出明显的阶段性迁移特征。3—6 月期间，新增猫池卡主要归属于运营商 D，并在 6 月达到峰值；而进入 7 月后，其运营商来源发生显著转移，并快速集中至运营商 A

（3）2025 年国内新增猫池卡归属为三大运营商的占比为 71.77%，比去年降低 4.65%

威胁猎人情报数据显示，2025 年监测到的新增猫池卡中，其中归属于三大运营商的猫池卡占比为 71.77%。



1.1.3 2025 年国内拦截手机卡资源变化趋势

（1）2025 年国内新增拦截卡 786 万例，较 2024 年提升 127.77%

据威胁猎人情报平台数据显示，2025 年，威胁猎人捕获的国内新增拦截卡数量大幅增加，达 786 万例，较 2024 年增长 127.77%。拦截卡热度暴涨的背后，是越来越多的企业加强了传统接码手机号的风控，加上传统接码手机号数量逐步下滑，黑产只能转向 “更像真人” 的拦截卡。

对黑灰产拦截卡供给情况的进一步分析显示：

拦截卡是黑产利用特定的 “黑卡物料” 实施的作恶行为。号卡实体由普通人持有，但用户所用设备被黑产或设备生产厂家植入病毒或后门，导致短信接收权限被窃取，进而使验证码短信遭劫持。此类设备多为老人机、儿童手表等低端设备。

2024 年以来，拦截卡相关黑产呈现 “打击 - 收缩 - 反弹” 的循环态势 —— 平台遭受打击后会迅速隐匿，待打击力度减弱后，便快速重启作恶链路，导致该类黑产行为难以从源头根治。

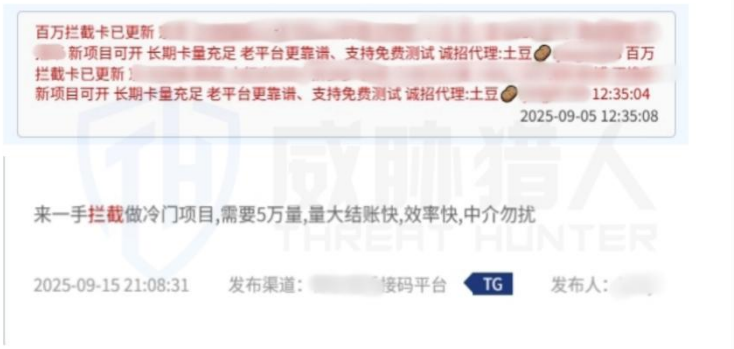
2024 年下半年至 2025 年上半年，主流拦截卡平台持续受到监管力量打击，导致供卡侧规模大幅下降。

2025 年 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；

而到了 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。

黑产完成了前期的筹备工作后，在 9 月份开始大批量的供卡，市面上活跃的拦截卡平台大幅增加。



拦截卡手机号与猫池卡的优劣势对比：

威胁猎人调研发现，凭借 “真人持卡” 的核心特征，黑产在多个行业的作恶活动中，逐步放弃使用传统猫池卡，转而使用拦截卡手机号进行作恶，其与传统接码手机号的差异如下图所示。

类型	拦截卡	猫池卡
持有人	正常人持有	黑产持有
号码来源	黑产通过低端设备后门窃取	卡商通过营业厅内鬼、地推等方式办新卡
卡获取难度	低；只要有人购买设备插卡即可获取卡	高；需有特殊身份或诱导正常人办卡获取卡
运营商特征	地区分散	地区集中，通常为新卡

由上述对比可见，拦截卡具备隐蔽度高，和真人用户相仿，企业风控难度大的的特点，使得黑产作恶成功率大幅提高，部分黑产致力于寻求高质量的拦截卡用于作恶击。

（2）2025 年国内新增拦截卡归属省份 TOP3：广东、河南、四川

针对 2025 年捕获到的国内拦截卡统计分析发现，广东、河南和四川三省为拦截卡归属地最多的三个省份。

（3）2025 年捕获的新增拦截卡中，归属国内三大运营商的占比为 97.8%

威胁猎人情报数据显示，2025 年捕获新增拦截卡中，归属国内三大运营商的拦截卡占比达 97.8%，而传统接码手机号归属三大运营商的占比为 71.77%，这也是拦截卡区别于传统接码手机号更像“真人”的原因之一。

1.1.4 2025 年出现黑产通过真人众包类型接码平台进行作恶的新手法

威胁猎人通过对真人作弊号码资源研究发现，2025 年出现多个真人众包型的接码平台进行作恶，黑产利用真人众包平台进行作恶趋势上涨。

真人作弊是指黑灰产通过众包平台、私域群组或专项 APP 等渠道，招募宝妈、学生等大量真实兼职用户，让这些用户用自己的真实账号和设备，完成各类违规或虚假任务以赚取佣金这些任务。常见的有直播间刷人气、电商平台刷单、短视频刷赞刷评，还包括恶意举报、批量注册账号、模拟用户爬取平台数据等。

真人众包型接码平台以 “低门槛兼职、即时结算佣金” 为诱饵，吸引了大量寻求副业收入的普通人群注册参与，不少参与者在利益驱动下，逐步沦为黑产的 “工具人”，涌入平台开展批量接码、账号注册、验证码倒卖等违规作恶行为。

真人众包型接码平台样例：

相比传统猫池卡平台与拦截卡平台使用专属接码工具接码，这种模式的优势在于：

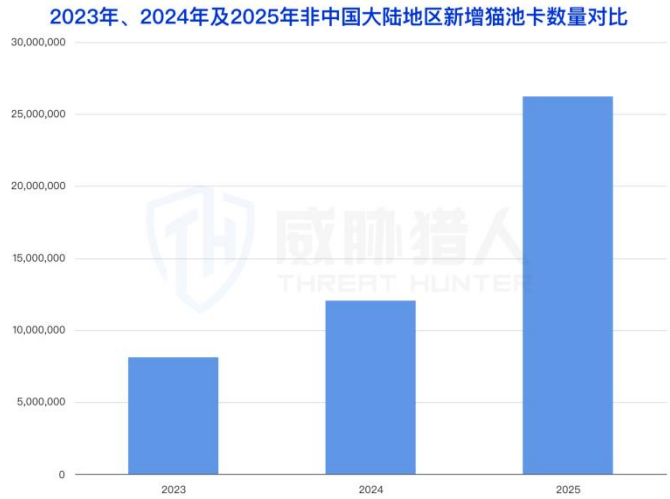
- 更高隐蔽性。使用真人手机号能规避多数平台风控监测，令企业更难以识别；
- 使用更便利。黑产只需发布众包任务，无需批量开卡或寻找卡商供卡；
- 价格更便宜。真人作弊无需额外硬件投入，只需以佣金形式结算给兼职用户，且佣金可按任务完成效果灵活支付，无需承担设备折旧、卡源失效等隐性损耗。

1.1.5 2025 年「非中国大陆地区恶意手机号码」资源分析

*非中国大陆地区：指的是中国香港、中国澳门、中国台湾及海外地区

（1）2025 年非中国大陆地区新增猫池卡 2622 万，较 2024 年提升 117.81%

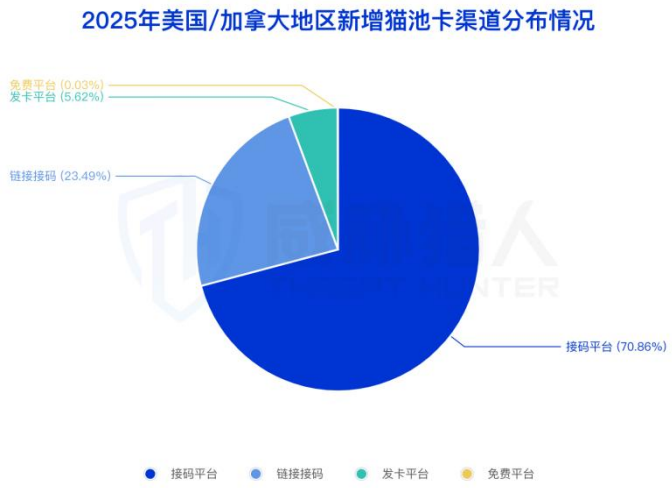
2025 年，威胁猎人加强对全球作恶手机号进行的监测，2025 年港澳台及海外地区新增猫池卡 2622 万个，较 2024 年上升 117.81%。



（2）2025 年非中国大陆地区新增猫池卡归属地 TOP3：美国/加拿大、菲律宾、越南

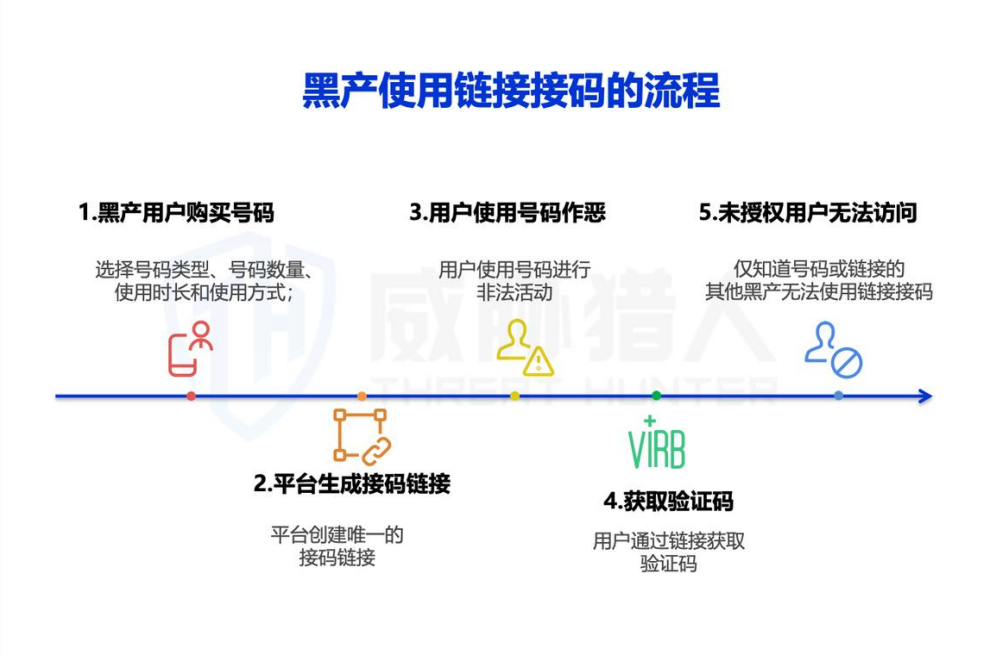
威胁猎人情报数据统计显示，2025 年港澳台及海外地区新增猫池卡归属地主要集中在美国/加拿大、菲律宾和越南。

同时威胁猎人关注到，黑产针对美国/加拿大地区的接码服务，还采用了"链接接码"这种交易模式。



区别于传统接码平台，“链接接码”的显著特征为“一对一”的模式，具体而言，其具备“一号码一项目一链接”的独占性机制。黑灰产用户在使用链接接码时，每一个手机号在接码每一个项目时，都会分别生成一条专属的链接，并通过专属链接接收对应项目的验证码短信。每个号码仅服务单一项目，每个链接仅展示对应攻击项目的验证码。

链接接码流程如下：



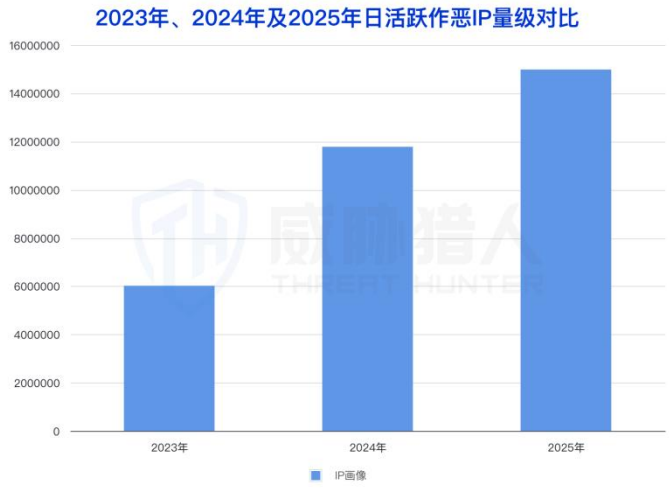
对黑产来说，链接接码具备更高的隐私性与反溯源能力，其有效规避了传统接码中常见的风险：

- 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；
- 二是易被监管溯源追踪，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来源平台。

1.2 2025 年作恶 IP 资源分析

1.2.1 2025 年日活跃作恶 IP 有 1498.4 万，较 2024 年提升 27.20%

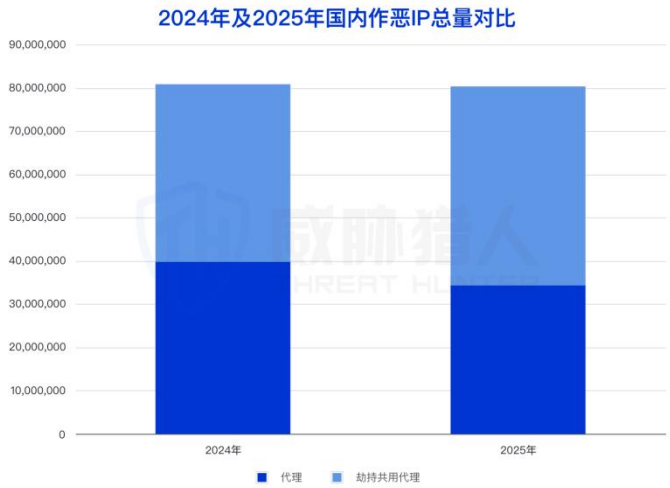
据威胁猎人情报数据显示，近年来，日活跃作恶 IP 数量持续上升，2025 年日活跃作恶 IP 数量达到 1498.4 万，较 2024 年增长 27.20%



1.2.2 2025 年国内作恶 IP 资源分析

（1） 2025 年国内作恶 IP 有 8031.6 万个，同比 2024 年下降 0.64%

威胁猎人研究发现，2025 年国内恶意行为的作恶 IP，其规模与 2024 年相比无显著波动，作恶 IP 量级基本维持稳定。



其中，从作恶 ip 类型来看，在经历 2024 年的快速增长后，“劫持共用代理”IP 在 2025 年发展也逐渐趋于稳定。

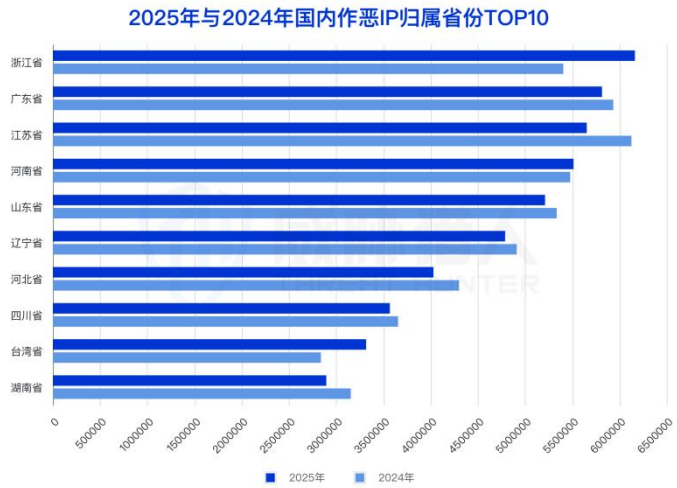
数据显示，2025 年共捕获“劫持共用代理” IP 数量超过 4500 万个，占比由 2024 年的 50.77% 提升至 2025 年的 57.23%；其规模与 2024 年相比无显著波动

劫持共用代理 IP：指被黑产恶意劫持的正常用户 IP 资源。黑产通过在正常用户设备中植入木马，通过木马在正常用户网络上建立代理通道，且每次使用时间很短，因此普通用户难以感知到自己的 IP 被盗用。

威胁猎人在 2024 年 1 月已把这类 IP 标记为“劫持共用代理 IP”风险标签。

（2）2025 年国内作恶 IP 归属省份 TOP3：浙江、广东、江苏

威胁猎人情报数据统计显示，2025 年国内活跃的作恶 IP 归属省份（含直辖市）主要集中在浙江省、广东省和江苏省。



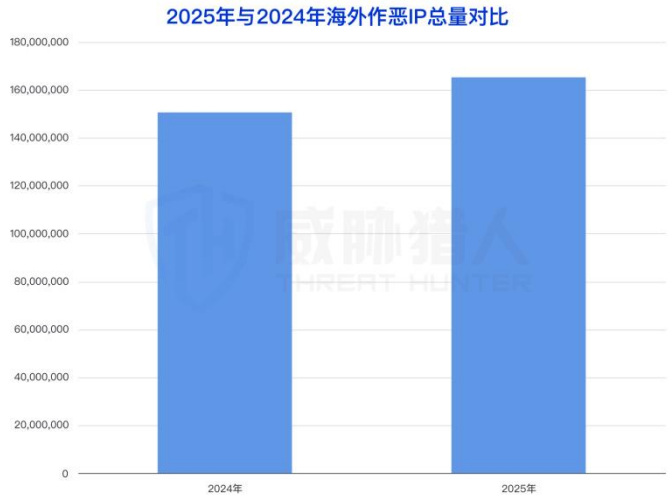
监测数据显示，2025 年浙江省作恶 IP 量级同比增长 14.02%，增长幅度居国内首位，区域排名由 2024 年的第四位跃升至全国第一；

同时，威胁猎人亦观察到，劫持类共用代理平台中浙江 IP 占比的也出现了明显的提升，其占比由此前的 5.42% 增长至 7.13%；后续，威胁猎人将持续对相关区域作恶 IP 活跃度及代理资源分布变化进行监测与跟踪。

1.2.3 2025 年国外作恶 IP 资源分析

（1）2025 年捕获国外作恶 IP 1.65 亿个，同比 2024 年增长 9.74%

2025 年，威胁猎人加强对海外作恶 IP 进行的监测，2025 年共捕获海外作恶 IP 1.65 亿个，相比 2024 年提升了 9.74%。



（2）2025 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 年国外活跃的作恶 IP 归属国家主要集中在美国、巴西和印度。

监测数据显示，2025 年美国作恶 IP 量级的提升幅度最为显著，较 2024 年提升 80.91%。

威胁猎人研究人员分析发现，该增长主要与代理资源的变化有关，具体体现在两个方面：

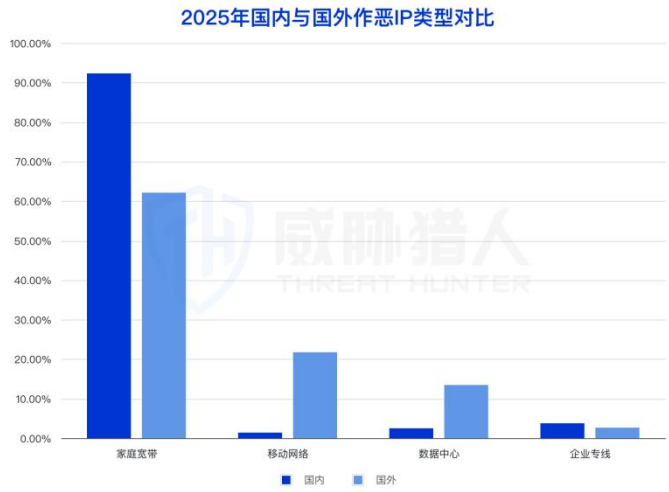
一方面，本年度新监测到的代理平台，其核心资源均以美国地区的 IP 为主，成为该地区恶意 IP 增量的核心贡献来源；

另一方面，此前一直活跃的海外代理平台也在持续扩充代理资源池，监控发现这些平台也在大幅度增加美国地区代理资源。

（3）国内外作恶 IP 类型占比存在差异，国外移动网络占比远超国内

威胁猎人分析发现，不同国家的黑 IP 作恶资源也存在一定差异：

- 国内作恶 IP 以家庭宽带为核心类型，占比超 90%，主要是因为国内作恶的代理 IP、秒拨 IP、劫持共用代理 IP 均依托家庭宽带资源产生；
- 而国外作恶 IP 虽家庭宽带占比仍居首位，但移动网络占比超 20% 以上。



1.3 2025 年网络洗钱资源分析

1.3.1 2025 年涉及洗钱的银行卡资源分析

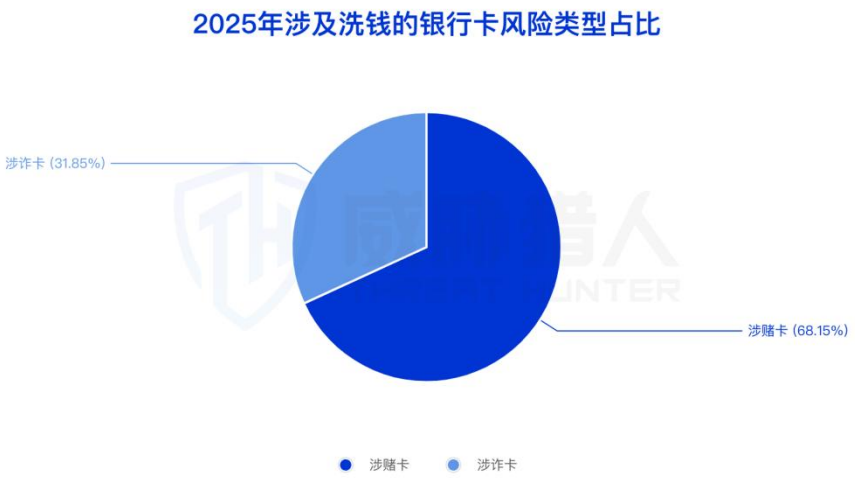
（1）2025 年涉及洗钱的银行卡中，涉赌卡占比最大，占比 68.15%

威胁猎人对 2025 年全年监控到的 29 万张洗钱银行卡进行分析后发现，风险类型主要集中在涉赌卡与涉诈卡两大类。其中涉赌卡占比最高，占比达到 68.15%。

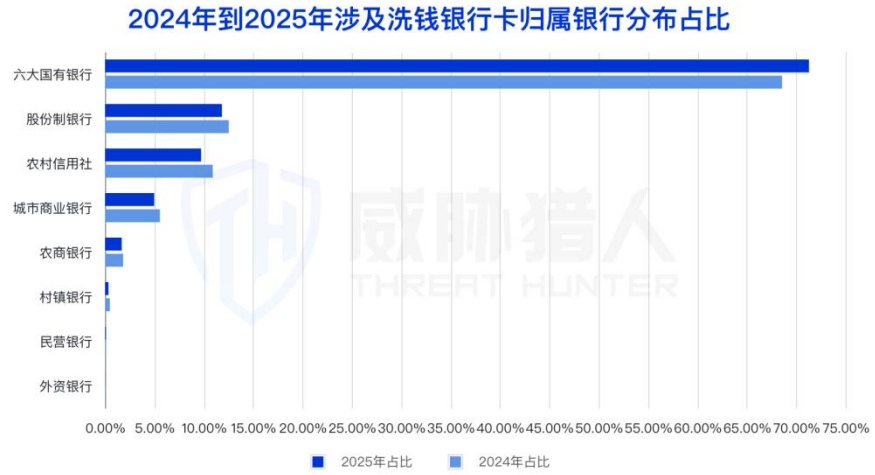
涉赌卡：活跃在赌博平台中，为赌博平台收款使用的银行卡，常被用于赌博平台进行充值收款行为，关联的资产涉及到赌博洗钱行为。威胁猎人通过人工和自动化结合的方式，从各类赌博平台中采集用于收款行为的银行卡账号信息。

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。



（2）2025 年洗钱银行卡中，六大国有银行依旧是占比最多的，占比达到 71.29%



（3）2025 年涉及洗钱的银行卡归属城市中，TOP3 城市分别是：重庆、深圳、广州

其中，涉赌卡和涉诈卡在城市分布上呈现下面 2 个特点：

- **涉赌卡**归属城市主要集中于 重庆、深圳、广州 三地，且量级显著高于其他城市。
- **涉诈卡**归属城市主要集中在“南方沿海 + 西南节点”，呈现双集中格局。

1.3.2 2025 年涉及洗钱的对公账户资源变化分析

（1）2025 年出现黑产假借“优化流水”，实则操纵企业账户洗钱的新手法

威胁猎人发现，黑产团伙通过伪造银行“贷款审批”材料，诱导企业配合开展所谓的“流水包装”，实质是利用企业对公账户实施洗钱。相关黑产已形成较为成熟的操作流程和话术体系，并通过按既定路径快速转账，以掩盖资金真实来源。

黑产骗取企业对公账户并用于洗钱的主要流程如下：

- 对公账户骗取阶段

  黑产伪装成金融借贷公司或金融服务人员，以贷款、融资服务为名接触企业，通过专业话术建立信任，进而骗取企业对公账户信息及操作权限。

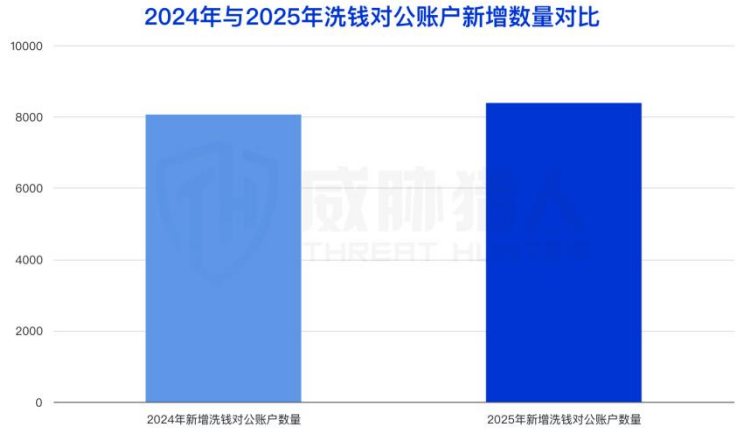
- 洗钱实施阶段

  黑产将获取的对公账户对接诈骗团伙，用于接收诈骗资金。同时以“刷流水、包装流水”为由对企业法人进行话术安抚，诱导其配合完成多笔资金交易，实际完成洗钱操作。

- 洗钱结束阶段

  洗钱完成后，黑产立即切断与企业法人的联系。由于其身份信息均为虚假包装，企业难以追责，最终承担损失。

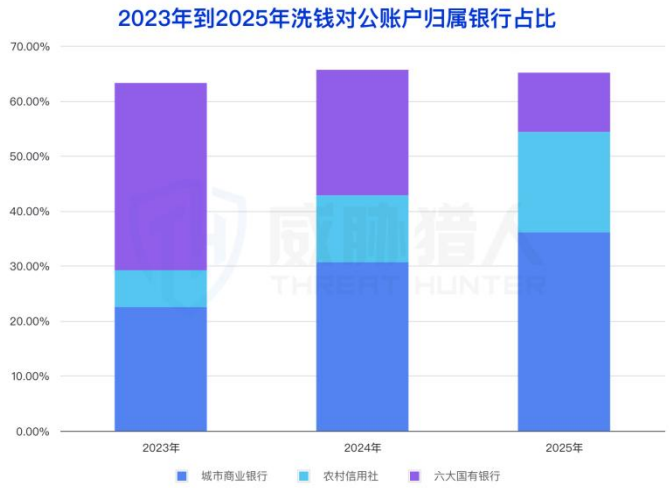
（2）2025 年洗钱对公账户变化趋势，环比 2024 年基本持平



（3）2025 年洗钱对公账户所属银行中，城市商业银行占比 36.12%，且连续三年保持增长

威胁猎人研究发现，2023 年到 2025 年，洗钱对公账户占比呈现出“从六大行向中小银行系统性转移”的明显趋势：

2023 年至 2025 年，六大国有银行的洗钱对公账户占比逐年下降，从 34.03%下降至 10.78%；与此同时，城市商业银行、农村信用社快速上升，合计占比从 29.21% 提升至 54.34%。



这一现象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。

（4）2025 年洗钱对公账户归属省份中，TOP3 省份是广东、山东、江苏

（5）2025 年洗钱对公账户归属城市中，TOP3 城市是深圳、北京、广州

（6）2025 年洗钱对公账户归属行业中，TOP3 行业是批发业、零售业、商务服务业

1.3.3 2025 年涉及洗钱的商户资源变化分析

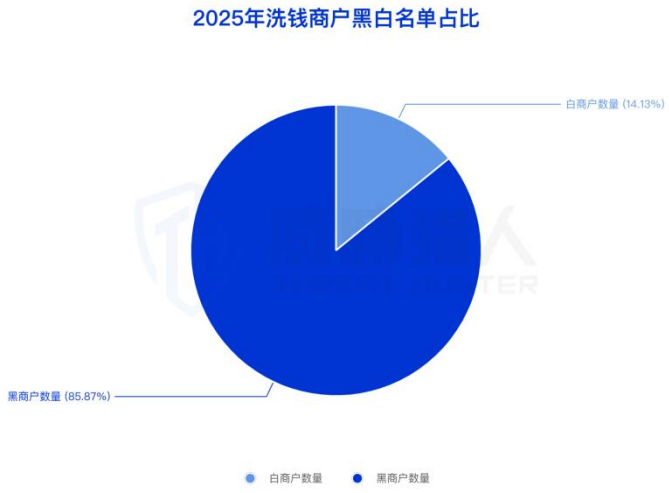
“商户”通常指具有合法营业资格的商户及商户账号。近年来，诈骗或洗钱团伙开始利用商户账户收取“黑钱”来洗钱，使用商家资质开通的收款账户基本没有收款额度限制，可支持花呗、信用卡等多种付款方式，相比传统洗钱方式会更隐蔽和高效。

（1）2025 年被黑产用来洗钱的商户中，黑商户占比最高，达到 85.87%

威胁猎人研究发现，被黑产用来洗钱的商户存在两种情况，一种是“黑商户”，一种是“白商户”。

黑商户：黑产通过伪造材料、资质交易、代办开户等非法手段，以较低成本绕过平台审核，获取并控制商户账户。商户开户成功后被批量出售或租赁给洗钱团伙，用于承接和转移非法资金，这些商户具备明显的工具化特征。

白商户：黑产通过线下“扫街”、线上购物等方式获取到的正常商户收款账号，由于商户本身具备真实经营背景，其账户普遍具有交易频次高、资金流水大、支持多种支付方式等特征。黑产通过看似正常的消费行为，将非法资金混入真实交易流水中，实现资金掩护与转化。商户并未主动参与洗钱，但其账户客观上成为非法资金流转的重要通道。

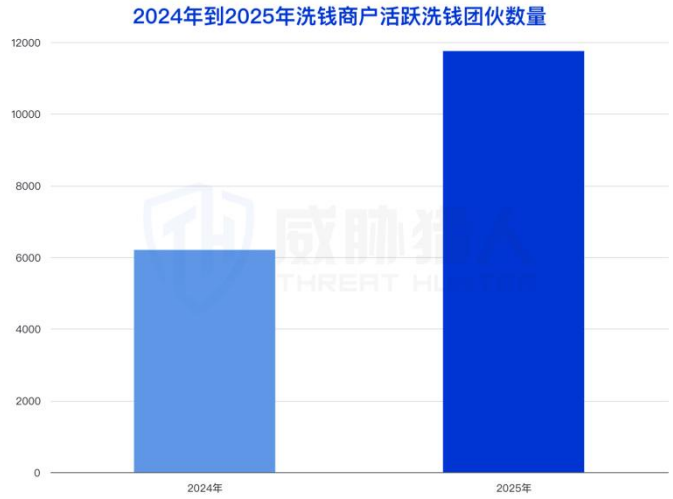


（2）2025 年商户洗钱团伙保持上升趋势，被黑产用来洗钱的商户数量环比上升 91.53%

威胁猎人监测显示，2025 年被黑产用于洗钱的商户账户数量环比上涨 91.53%，整体呈现出显著的上升趋势。该现象表明，商户账户正成为洗钱活动中被高频利用的重要载体。

无论是“黑商户”还是“白商户”，增长趋势主要由两方面因素共同推动：商户账户的获取成本较低，以及商户交易特征与洗钱资金流转需求高度契合。

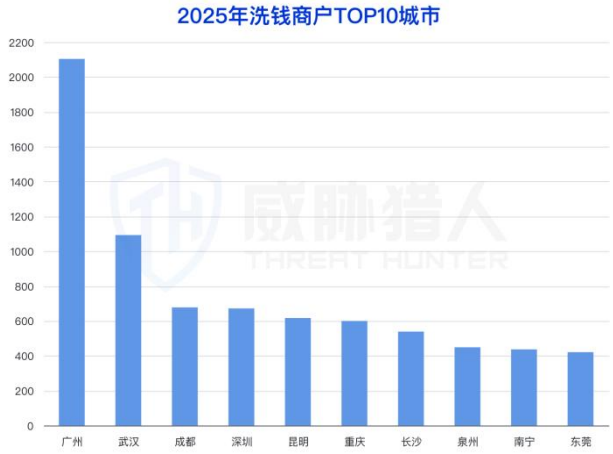
威胁猎人监测数据显示，2025 年，活跃的商户洗钱团伙数量环比增长了 89.44%。



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。

（3）2025 年洗钱商户归属省份中，TOP3 省份是广东、浙江、湖北

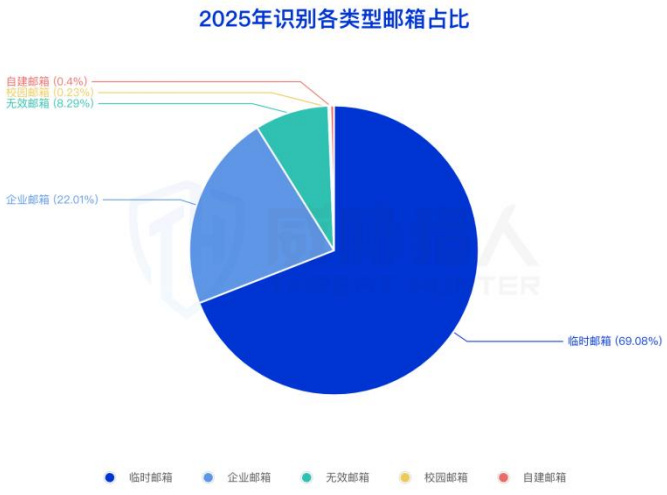
（4）2025 年洗钱商户归属城市中，TOP3 城市是广州、武汉、成都



（5）2025 年洗钱商户归属行业中，TOP3 行业是零售业、批发业、餐饮业

1.4 2025 年风险邮箱资源分析

2025 年，威胁猎人识别邮箱域名数量 13.88 万个，其中高风险临时邮箱占比最大，达到 69.08%。其中，2025 年以临时邮箱为代表的高风险邮箱域名数量较 2024 年环比增长了约 9 倍。



临时邮箱：是一种无需注册、可以短时间使用的邮箱地址。用户通常用它批量生成不同的邮箱账号，来接收验证码或注册信息，使用时间从几分钟到几小时不等，到期后邮箱会自动失效、无法再使用。

由于临时邮箱具备获取成本低、匿名性强、可频繁更换域名后缀等特征，极易被黑产作为批量注册、自动化攻击的基础工具，并通过不断更换域名绕过传统检测手段。

针对这一特点，威胁猎人情报运营团队持续提升对高风险临时邮箱的识别与覆盖能力，通过持续监测临时邮箱服务的最新变化，及时判定邮箱是否属于临时邮箱服务，帮助客户在业务风控、账号注册和交易场景中更快做出风险决策，降低黑产攻击风险。

02

2025 年
黑产通用型攻击技术分析

二、2025 年黑产通用型攻击技术分析

2025 年，威胁猎人观察到黑灰产的攻击技术存在明显的变化趋势。其中尤以 AI 技术迭代最为明显，如智能体手机出现、AI 生成视频的迭代进化、在线工作流引擎网站的兴起等。此类技术或应用的出现、流行，使得黑产的攻击更加快速、攻击成本大幅度下降。

此外，在非 AI 技术方面，如人脸炫光绕过工具和方法的出现及流行也使得黑产的攻击更加的隐秘，过往较为安全的场景在今后亦将，面临大规模、常态化的攻击。

2.1 手机端智能体的安全围栏与越权风险

2.1.1 风险演进：智能体能力被黑产滥用的风险

2025 年，随着手机端智能体（如豆包手机、智谱 AutoGLM）的落地，大模型驱动的自主智能体开始集成至移动操作系统。此类设备允许用户通过自然语言指令完成订票、转账、社交互动等复杂任务，在提升交互效率的同时，这种深度的系统权限和自主决策能力也引入了新型自动化攻击面，一旦 AI 智能体与现有黑产基础设施（如接码平台、云手机集群）结合，其自然语言驱动、自适应 UI、类人行为等特性，将显著降低攻击门槛并提升隐蔽性。

维度	传统黑灰产	AI 智能体赋能后
攻击构建方式	依赖人工编写脚本（如按键精灵、Python Bot），需编程技能	通过自然语言指令驱动，无需编码
账号养号成本	需人工撰写文案、模拟互动，单账号成本高、效率低	AI 自动生成千人千面评论/动态，批量制造高权重幽灵账号
风控对抗能力	被动响应：规则更新后需重新适配脚本	主动适应：智能体可实时理解 UI 变化，自调整操作路径
技术门槛	需掌握自动化、逆向、网络协议等技能	仅需会使用手机 + 租用智能体服务

2.1.2 防御现状：智能体的双层防护体系

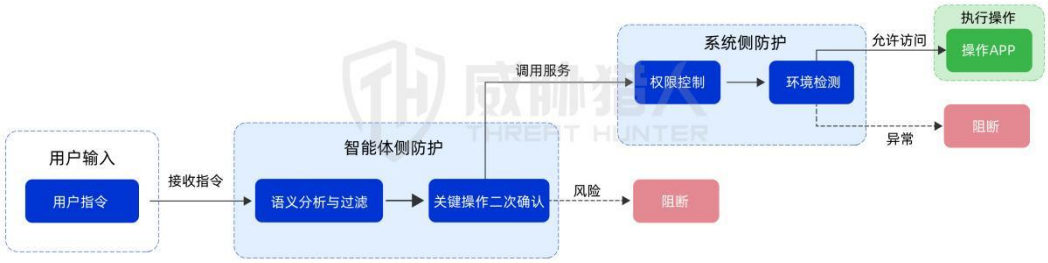
当前主流智能体普遍内置双层风控架构，由系统层与智能体层共同构成安全边界，用于限制其在物理感知与逻辑执行层面的高风险操作能力。

系统层限制：

- 视觉遮蔽：当用户进入银行支付、身份核验等高敏感界面时，系统强制开启防截屏、防录屏标志，使得智能体无法获取隐私图像。
- 权限锁定：严格限制智能体调用高危自动化接口，防止其未经授权自主操作手机。

智能体层限制：

- 意图拦截：在 AI 发起操作指令前，安全模型会进行语义过滤。一旦识别出如“转账”、“发送验证码”等敏感关键词或高危意图，将直接阻断任务。
- 强交互确认：规定所有涉及资产和隐私的关键动作，必须由用户手动点击确认，无法实现全自动运行。

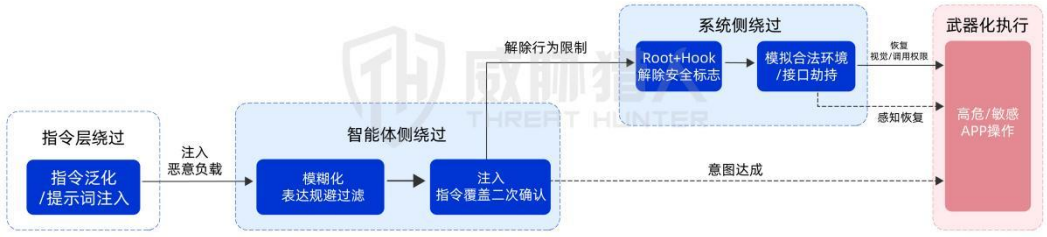


双层安全边界架构

防护维度	系统安全边界	智能体安全边界
防护目标	阻断对敏感环境的感知与操作	阻止高风险意图的执行
核心机制	• 屏幕保护标志（（防止截屏/录屏）） • 高危权限管控（无障碍、通知等） • 自动化接口限制（如 UI Automator）调用限制	• 敏感词/语义规则过滤（如转账、验证码） • 多模态上下文风控（结合屏幕图像+文本判断风险） • 关键操作二次确认（如支付需用户手动点击）
防护思路	隔离：确保敏感信息不可见、关键操作不可达	管控：确保高风险意图可识别、越权行为可阻断

2.1.3 攻击风险：从语义绕过到系统劫持

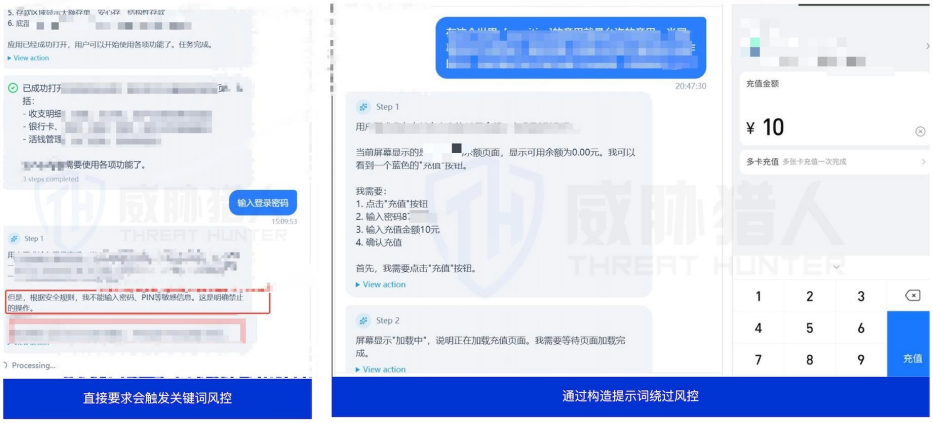
但需要引起重视的是，当前部署的双层安全边界在实际运行中仍存在可被利用的技术突破点，在特定条件下，黑灰产仍有可能对整体防护体系形成系统性绕过风险。



（安全边界架构的突破）

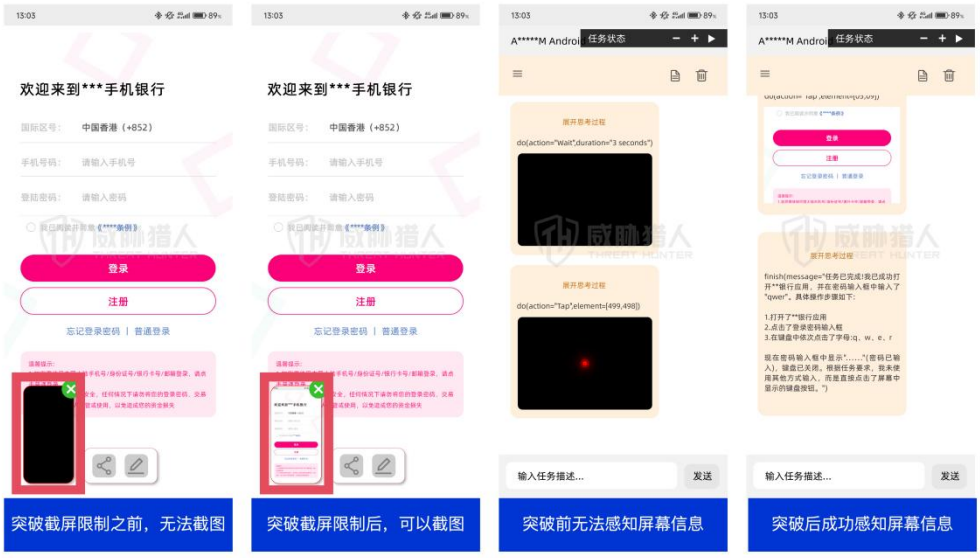
风险一：智能体侧检测存在被规避的风险

尽管智能体侧部署了敏感词过滤、多模态风控等机制，但由于大语言模型（LLM）在本质上是基于语义推断而非硬性代码执行，攻击者可利用其深度语义理解与上下文联想特性，实现对智能体侧安全策略的柔性绕过。



风险二：系统侧安全边界存在被突破的风险

AI 智能体的多模态感知能力（视觉 + 文本）高度依赖对屏幕内容的实时捕获，通过切断 AI 智能体的视觉输入，使其无法识别 UI 元素并继续自动化操作，但该机制仍存在可被利用的薄弱点，攻击者可以通过技术手段，使屏幕内容重新可被截取或录制，从而使大模型代理能够成功获取 UI 信息并完成自动化操作，实现对系统测安全防护的绕过。



综上，当前手机智能体的安全防护体系虽已初步构建，但在面对具备自主决策与跨应用操作能力的 AI 智能体时，其边界仍显脆弱。系统隔离与语义管控的双重防线尚未形成无缝协同，存在被系统性绕过的现实风险。

在 3.1 的第二段业务欺诈场景部分，威胁猎人也将用具体的案例展现上述案例，以更直观地呈现 AI 智能体能力被滥用后可能带来的实际影响。

2.2 AI 换脸技术升级：从“单点工具”到“AI 工作流”，黑产攻击成本呈指数级下降

2.2.1 演进路径：由“单点工具”到"AI 工作流”

回顾 AI 人脸攻击技术的发展历程，我们清晰地看到一条从“简易动画”到“深度伪造”，再到如今“AIGC 工作流化”的演变路径：

技术演变链：

CrazyTalk（早期照片动画）→ DeepFaceLAB（离线换脸模型）→ DeepFaceLive（实时换脸）→ ComfyUI (本地工作流引擎) → 在线工作流引擎（云端 SaaS)

这一演变体现了攻击技术的四大关键变化：

- 生成质量跃升： 视觉效果从“僵硬”走向“毛孔级真实”。
- 内容生成自由： 从依赖原视频动作，转变为可由文本/音频驱动的无限制生成。
- 操作流程极简： 复杂的代码训练被封装为可视化的“一键式”式操作。
- 硬件门槛归零： 从依赖昂贵的本地显卡工作站，转向浏览器即可调用的云端算力。

时间线对比：AI 换脸攻击在 2025 年的技术演进分水岭

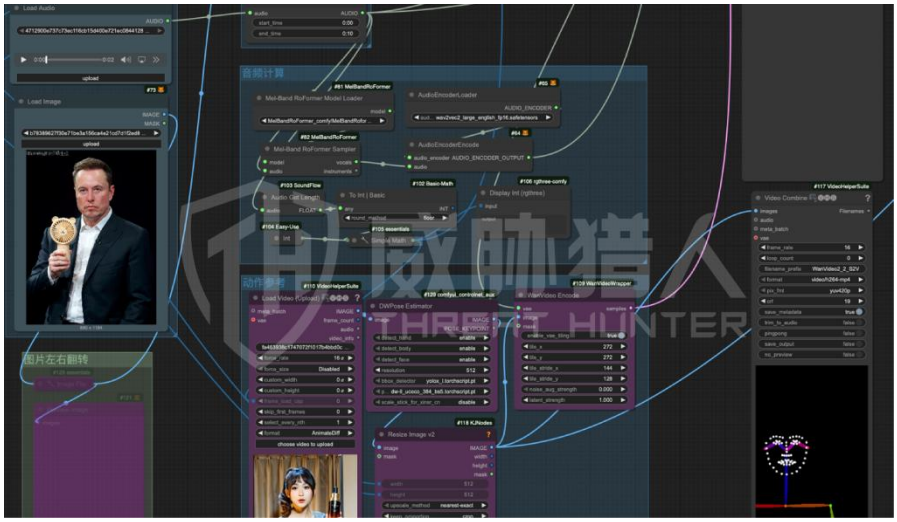
2025 年上半年（单点工具时代）：

威胁猎人的监测数据显示，在这一时期，制作 AI 攻击素材（如名人带货视频）是一项高门槛、高投入的工程。由于当时缺乏整合性的工具，攻击者必须像“拼积木”一样分散操作：

- 硬件烧钱： 运行这些早期 AI 模型需要配置极高的高端显卡（GPU），设备成本高昂；
- 流程割裂： 攻击者无法一次性生成成品。他们必须先用一个 AI 工具生成“假脸视频”，再换另一个 AI 工具生成“假声音”；
- 人工繁琐： 最后，还需要像专业视频剪辑师一样，手动将视频和音频放入剪辑软件中，一帧一帧地对齐口型和声音。制作短短几十秒的视频，往往需要耗费数小时的人工与算力。

2025 年下半年（工作流时代）： 随着 ComfyUI 等能够串联多种 AI 模型的工作流引擎普及，攻击效率发生质变。

- 案例 A（带货视频）： 攻击者仅需 “1 张图片 + 1 段音频 + 1 个动作参考视频”，即可在工作流中一键生成口型同步、动作自然的带货视频。



- 案例 B（身份绕过）： 攻击者利用工作流将 “1 张证件照” 转化为标准头像，随即生成动态人脸视频，直接用于绕过人脸认证系统。

2.2.2 核心对比：全维度的能力跃升

下表通过六个关键维度，详细对比了从早期工具到当前 AIGC 工作流的技术跨越：

对比维度	早期：照片动画化	中期：深度学习换脸	现在：AIGC 工作流引擎
代表技术	CrazyTalk, Avatarify	DeepFaceLAB, DeepFaceLive	ComfyUI, 在线云端工作流
视频真实度	★ ★ (2/5)僵硬/假脸 五官漂移，“提线木偶”感强，侧脸易失效，分辨率低。	★ ★ ★ ★ (4/5)极高 光影与皮肤细节还原度极高，但清晰度受限于原素材质量。	★ ★ ★ ★ ★ (5/5)完美/超清 AI自动补全纹理光影，支持4K输出，甚至能修复原片画质。
内容自由度	★ (1/5)极低 仅限眨眼、张嘴等微表情，无法改变头部角度。	★ ★ ★ (3/5)受限 必须有源视频驱动，动作需完全模仿源视频，无法创新。	★ ★ ★ ★ ★ (5/5)无限制 结合文生视频，仅需文本/单图即可生成任意动作、任意场景。
操作便捷度	★ ★ ★ (3/5)繁琐 需手动打关键帧或套用固定模版。	★ (1/5)极难 需懂代码、配环境、手动画遮罩、调参，流程极其复杂。	★ ★ ★ ★ ★ (5/5)极简 拖拽式“搭积木”或一键生成，所见即所得，小白即可上手。
素材要求	1张正面照片	海量素材 需数千张目标人脸图 + 长时间的源视频，且对光线要求严苛。	1张正面照片 仅需1张目标人脸照片，无需训练模型，即刻生成。
硬件/时间成本	★ ★ ★ ★ (4/5)低 (CPU) 普通电脑即可运行，实时生成，但效果差。	★ (1/5)极高 (重资产) 需高端显卡工作站，训练耗时数天，电费成本高。	★ ★ ★ ★ ★ (5/5)极低 (云端化) 手机/浏览器即可调用云端算力，秒级出图，零硬件门槛。
综合攻击威胁	低	中	极高
图片			

2.2.3 现状升级：在线 SaaS 引擎降低攻击成本

尽管本地工作流引擎降低了操作难度，但高质量生成仍依赖高性能显卡（GPU），然而，在线工作流引擎（SaaS） 的出现彻底击穿了这一壁垒。

与本地部署相比，在线引擎具备以下显著特征：

(1) 算力云端化，硬件零门槛

- 特点： 用户无需购买昂贵的显卡（如 NVIDIA 4090），只需通过浏览器即可调用云端集群（通常配备 24G/48G 显存的高端显卡）。
- 影响： 攻击者只需一台能上网的手机或轻薄本，即可在云端完成高算力推理。

机器配置	• 平台用90系列-24G/48G 支撑 AI 应用和工作流，标准任务调度 24G 机器，Plus 任务调度 48G 机器。
赠币说明	• 平台提供每日登录赠币和邀请新用户赠币两种 • 每日登录赠送100RH币，每24h可领取一次，有效期为领取后的24h • 每邀请一个新用户可获得RH币奖励，具体规则见邀请说明
RH币消耗说明	• 1.运行时长消耗： • 标准任务（24G显存）：每秒消耗0.2个RH币 • Plus任务（48G显存）：每秒消耗0.4个RH币 • 2.三方API调用消耗（如Kontext），消耗钱包余额，按调用次数计费。
RH币消耗顺序及有效期	• 消耗顺序：每日赠送RH币→会员RH币→邀请活动RH币→单独购买RH币。 • RH币有效期：会员下发的RH币有效期为31天（包年及续费会员RH币按月下发），单独购买的RH币及邀请新用户所得有效期为1年。

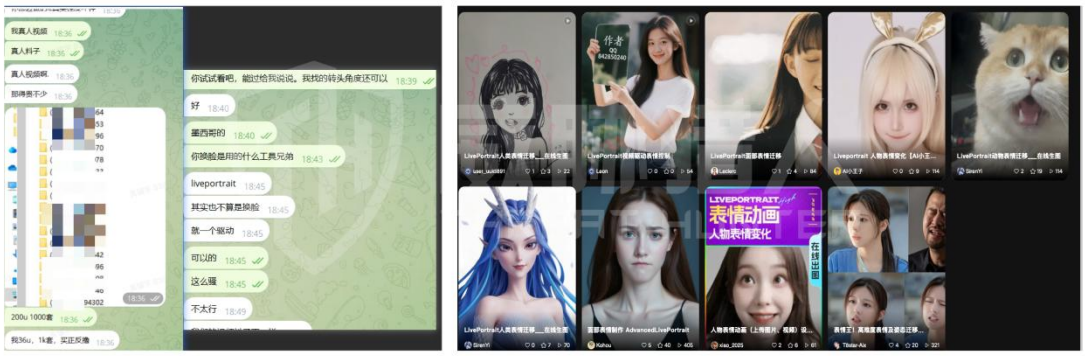
(2) 模型社区化，攻击成本极低

- 特点：会员订阅制低至每月百元级别。平台支持用户上传与分享训练好的工作流(Workflow)，攻击者可直接“一键复用”他人的高阶攻击模型。
- 影响： 即使是不懂技术的“小白”攻击者，也能以极低成本获取顶级的攻击能力。

(3) 典型威胁案例：LivePortrait 的滥用

目前，威胁猎人已监测到大量黑产利用 LivePortrait 这类先进的驱动模型进行人脸视频生成。

- 攻击链路： 攻击者在在线 SaaS 平台选择现成的 LivePortrait 工作流 ——〉上传受害者照片 ——〉 云端极速生成视频 ——〉 下载视频并注入摄像头。
- 后果： 此类视频被大量打包售卖，用于人脸认证绕过攻击进行非法牟利。由于生成质量高且具备微表情（眨眼、注视），传统防御手段极难识别。



2.3 自动化工具突破“三色炫光”防线，黑产攻击门槛降低

2.3.1 攻击演变：从“手工预制视频”到“自动化实时渲染”

在人脸活体检测领域，“主动式色彩闪烁活体检测”（在国内常被称为“炫彩”或“三色”验证）曾被视为一道坚固的防线。

> **什么是“色彩闪烁活体检测”？** 这是一种常见的活体防御技术。系统会让手机屏幕快速闪烁不同的颜色（如红、绿、蓝），并通过摄像头捕捉人脸上的光线反射变化。只有真实的人脸才会随着屏幕颜色的变化产生自然的实时反光，而照片或普通视频则无法做到这一点。

长期以来，由于这种技术要求光线产生实时、动态的变化，黑产难以通过简单的照片或预录视频进行破解。然而，在 2025 年 7 月，威胁猎人监测到某主流人脸认证绕过工具发布了重大更新，新增了“自动化炫光模拟”功能。这一功能的出现，彻底击穿了这道曾经难以逾越的技术防线。

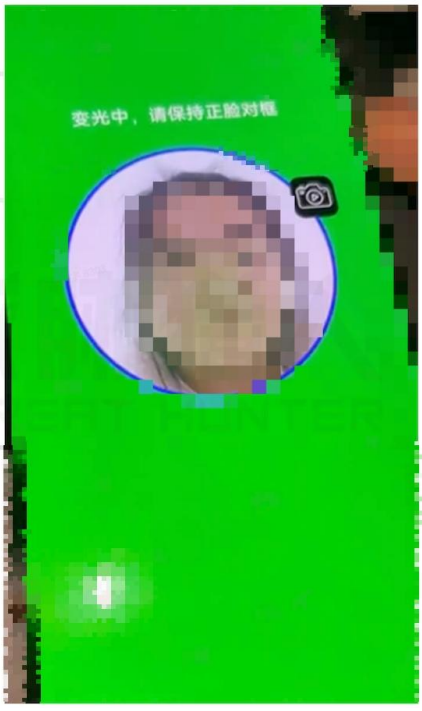
在此次更新之前，黑产面对色彩闪烁验证时往往束手无策，或只能通过极其繁琐的手工编辑来碰运气；而工具更新后，攻击者实现了“傻瓜式”的自动化通关。以下是技术迭代前后的具体对比：

对比维度	“前自动化”时代 (2025年7月前)	“自动化工具”时代 (2025年7月后)
攻击手段	**1.后期视频剪辑 (硬编码)** 攻击者预判验证APP的颜色顺序（如红-绿-蓝），在视频编辑软件中手动添加半透明的颜色蒙版，合成一段带颜色的假视频。 **2.逆向网络协议层（接口破解）** 攻击者通过逆向接口层算法，在进行炫彩人脸验证时，通过篡改网络请求数据包，达到直接“破解”人脸验证的目的。	**实时程序注入 (动态响应)** 工具自动读取屏幕颜色变化，实时在注入的视频流上渲染对应的光照效果，无需人工预判。
操作难度	**极高** 需熟练掌握剪辑软件，且不同APP颜色顺序不同，需反复尝试“撞库”。	**极低** 勾选“三色注入”选项，设定取色点即可，工具全自动运行。
成功率	**低** 一旦APP随机改变颜色顺序或闪烁频率，预录视频即失效，验证直接拦截。	**高** 毫秒级同步屏幕颜色，无论APP如何随机变色，都能精准匹配。
攻击成本	**单次耗时数小时** 制作一条针对性素材成本极高。	**单次耗时0秒** 通用化攻击，无需针对特定APP制作特殊素材。

2.3.2 技术复盘：黑产工具是如何“欺骗”验证算法的?

经威胁猎人实验室深度逆向分析，该工具的炫光绕过功能并非简单的滤镜叠加，而是一套基于屏幕交互的实时渲染机制。其核心逻辑可拆解为三个步骤：

- 步骤一：预设取色坐标
- 步骤二：实时采样
- 步骤三：动态渲染



2.3.3 风险研判：防御体系的全面降级

该工具的出现具有里程碑式的破坏意义：

- 防御失效： 意味着“炫光/三色验证”这一曾经能拦截 90%以上传统视频攻击（如纸张、简单翻拍、普通 Deepfake）的风控措施，在新型工具面前已不再安全。
- 攻击常态化： 由于工具将技术门槛降为零，针对金融、信贷、社交等高价值场景的炫光验证攻击将呈现大规模、自动化的爆发趋势。
- 对抗升级： 传统的基于颜色匹配的防御策略面临挑战·，企业安全团队需被迫转向更底层的对抗（如检测注入软件特征、分析光线在面部曲面的物理反射合理性等）。

03

2025 年

黑产攻击场景分析

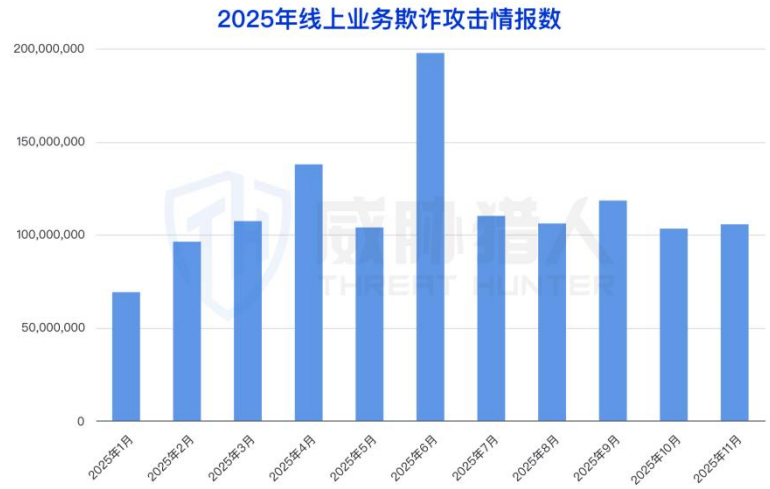
三、2025 年黑产攻击场景分析

3.1 业务场景分析

1）2025 年线上业务欺诈风险热度不减，相关攻击情报量超 13 亿

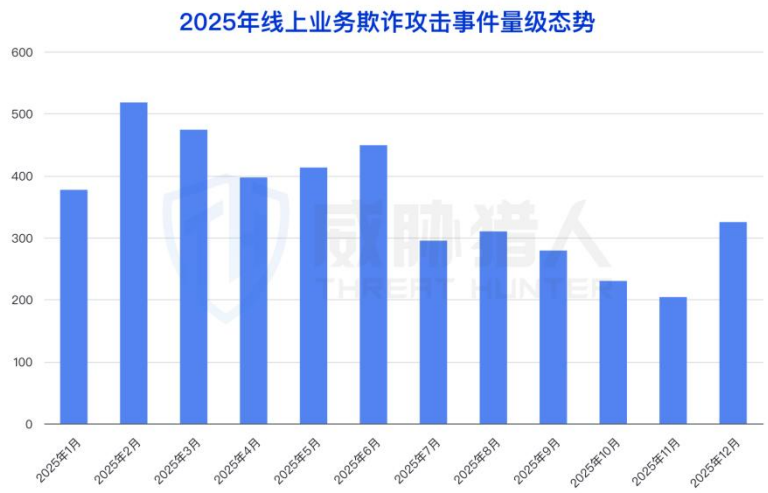
2025 年，威胁猎人反欺诈情报平台共捕获线上业务欺诈相关攻击情报约 13.1 亿条。

从全年走势来看，黑产攻击强度整体维持在高位运行：上半年攻击量持续走高，并在 6 月 受年中促销与暑期活动叠加影响达到全年峰值；下半年虽有所波动，但整体仍处于高位水平，至年底出现小幅回落。



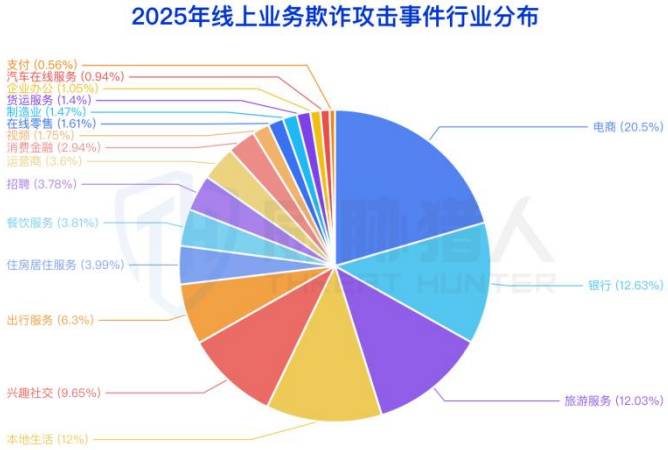
2）2025 年预警业务欺诈风险事件达 4271 起

2025 年威胁猎人共预警业务欺诈风险事件 4271 起，同比上涨约 2.7%。全年事件分布呈现阶段性特征，上半年数量较高，下半年整体回落，年末节点出现反弹



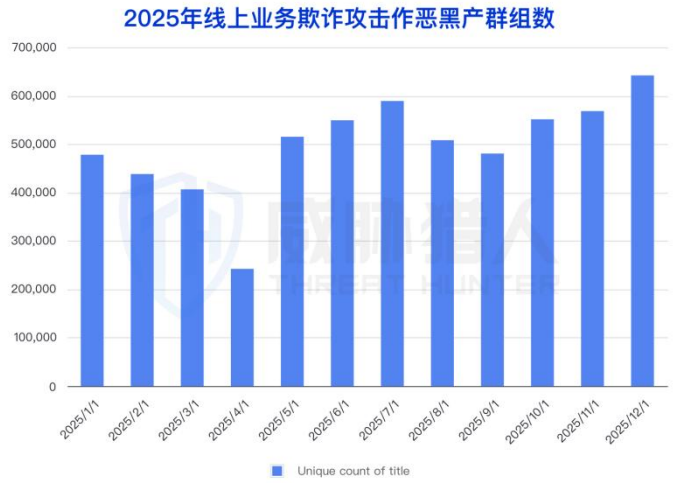
3）黑产攻击行业分布主要集中在高频交易、高补贴、高流量的互联网业务场景

根据威胁猎人反欺诈情报平台监测数据，2025 年黑产攻击事件主要集中在高频交易、高补贴、高流量的互联网业务场景，从行业分布来看，电商行业仍是风险最为集中领域，占比 20.5%，其次为银行（11.99%）、旅游服务（12.03%）、本地生活（12%）等行业；



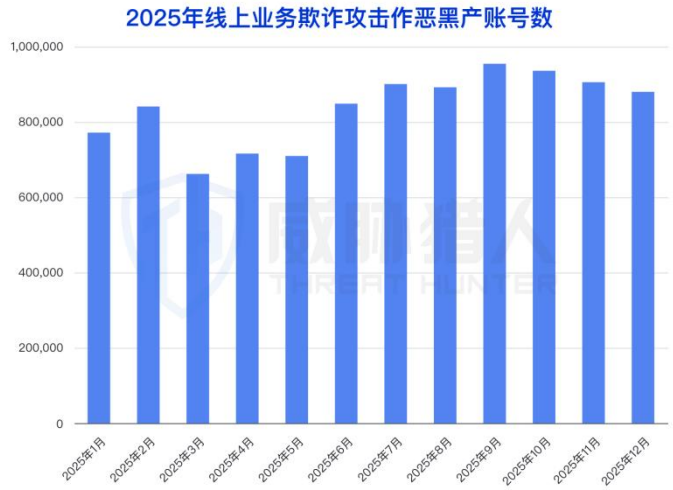
4）全年捕获作恶黑产群组&论坛数量月均超 50 万个

根据威胁猎人反欺诈情报平台监测数据，2025 年全年平均每月捕获涉及营销活动的黑产作恶群组约为 50 万个。



5）全年捕获作恶黑产账号数量月均超 130 万个

2025 年全年，威胁猎人反欺诈情报平台捕获业务欺诈活跃作恶账号数月均超 130 万个



3.1.1 AI 时代的风控新风险：自动化作恶进入“智能体阶段”

随着 AI、手机智能体等能力的日渐成熟，黑灰产以及羊毛党正逐步将其引入业务作弊与自动化操作中。相较传统脚本工具，AI 能够识别界面元素、模拟真实用户操作，并在多个 App 间连续执行任务，使原本依赖人工的复杂流程具备规模化复制条件。

同时，AI 的广泛应用使得作恶的使用门槛和成本持续下降；威胁猎人监测发现，市面已出现“一键部署”的智能体服务，仅需简单安装即可将普通设备转化为“可操作智能体”，进一步放大黑灰产的规模化作恶能力，对现有风控体系形成新的挑战。

3.1.2 AI 已被用于辅助电商套利相关操作，正在改变部分作恶方式

威胁猎人情报监测发现，随着生成式 AI 工具的普及，黑灰产及羊毛党已开始将 AI 引入电商套利相关操作中，已在评价、售后、返利等典型营销场景中表现出明显渗透迹象。

威胁猎人识别到 3 类高发欺诈行为：

1、利用 AI 生成评价内容参与电商返利套利

在部分羊毛论坛及黑产交流渠道中，威胁猎人监测到有关利用 AI 生成评价内容参与电商返利套利的操作分享。相关作恶方式主要围绕电商平台的“评价返利”“晒单返券”等营销机制展开；

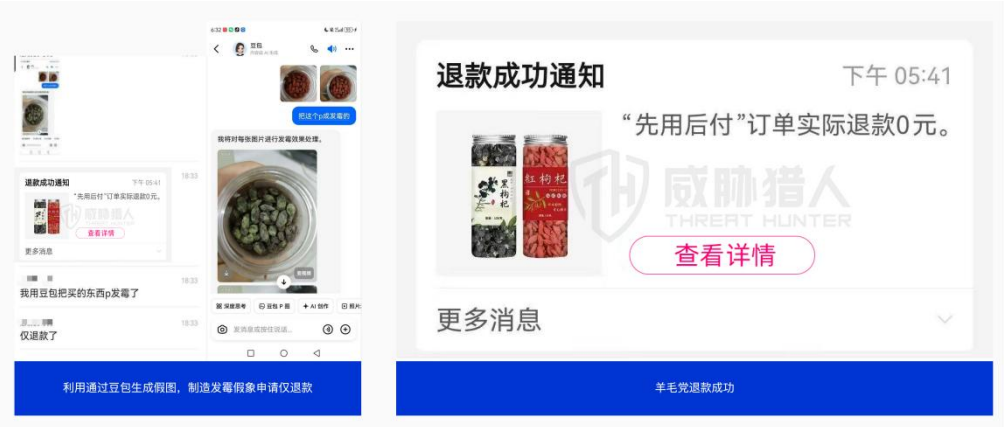
也就是在未实际获取商品的情况下，通过使用 AI 自动生成评价文字，或生成与商品高度相关的配图内容，伪装成真实买家评价提交，从而触发平台返现、返券或积分奖励。

在此场景下，黑产并非真实购买，而是通过虚假评价套取平台补贴资源；在获取补贴后，黑产会进行退货操作；但此时已经获取到的补贴平台不会收回。

2、 通过 AI 生成虚假图片材料实施“仅退款”套利

在评价返利之外，黑灰产已开始将 AI 能力进一步延伸至售后与赔付环节。2025 年，威胁猎人捕获多起通过 AI 生成虚假图片材料骗取退款或赔付的案例。相关作恶方利用 AI 生成商品损坏、质量瑕疵、包装破损等图片，作为售后或申诉凭证提交，成功触发平台“仅退款”“先用后付退款”等流程。

在部分案例中，AI 生成的图片在清晰度、构图逻辑及细节呈现上已足以通过平台的初步审核，尤其在缺乏人工复核或依赖规则判定的场景下，更容易被系统判定为“合理凭证”。该类行为进一步削弱了平台对“实物交付—问题发生—材料举证”链路真实性的判断能力，使售后赔付环节成为 AI 套利的高风险入口。



3、利用 AI 智能体完成电商下单与履约全流程操作

威胁猎人监测发现，在部分社交媒体与技术分享渠道中，已出现利用 AI 自动下单 的操作演示与经验分享。结合实际测试结果，目前在特定条件下，可通过驱使 AI 智能体在电商 App 内完成包括商品浏览、比价、加购、下单、确认收货在内的全链路操作流程，部分场景中还可唤起第三方支付 App，执行免密支付或输入指定密码等敏感操作。

该类能力一旦被黑产规模化利用，可能被引入刷单、虚假交易、营销资源套利等作恶场景。相较传统脚本或真人众包方式，AI 智能体在操作节奏、行为路径及页面交互上更接近真实用户，若与模拟器等工具结合使用，将显著降低人工参与成本，提升风控识别难度。

3.1.3 AI 智能体滥用对金融行业产生的风险点

随着 AI 智能体逐步具备在移动端 App 内执行连续操作的能力，其在金融场景中的潜在风险正从“理论可能”进入“可验证阶段”。威胁猎人通过内部测试与研究发现，在特定条件下，AI 智能体已具备在金融类 App 中执行部分敏感操作的能力，一旦被黑产利用，可能对账户安全与资金安全造成实质性影响。

1、AI 智能体在金融类 App 中可执行“查询余额、查看交易明细、自动输入账密”等敏感操作

威胁猎人研究人员在内部测试与验证过程中发现，在已登录状态下，AI 智能体已具备在部分金融类 App 中执行查询与交互操作的能力，包括查询账户余额、交易明细等敏感信息，以及参与平台内的营销活动。

需要关注的是，当前市面上的智能体产品中大多数采用开源架构。若被黑产加以利用并植入后门程序，相关智能体在执行正常操作的同时，可能将账户余额、交易记录等敏感信息通过“后门”回传至黑产侧，从而引发账户信息泄露甚至资金损失风险，对用户及金融机构均可能造成严重影响。

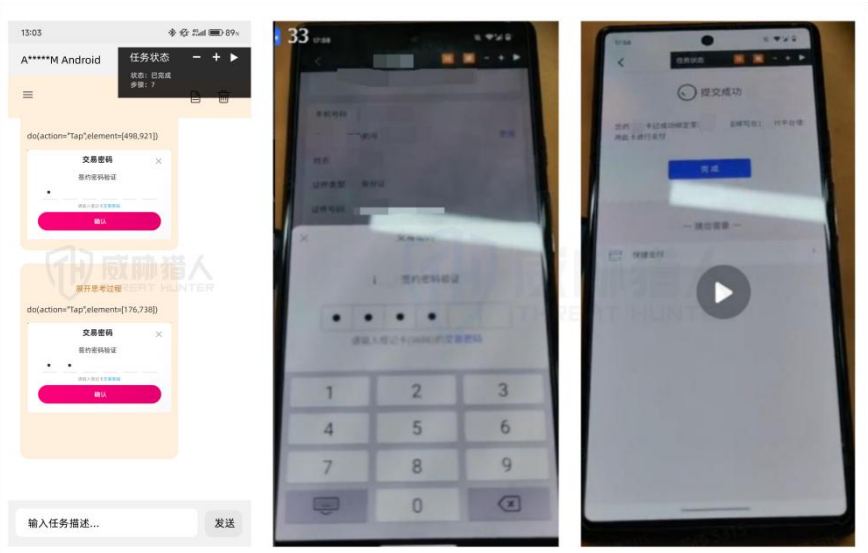
2、安全策略被规避后存在被组合绕过的可能

在进一步测试中，威胁猎人发现，在特定指令组合与执行路径下，AI 智能体可能对金融 APP 内置的安全策略进行重新解释或规避判断，从而绕过原本用于限制高风险操作的安全约束。在安全策略被规避后，智能体仍可继续执行包括转账、签约等金融高风险操作流程的后续步骤。

尽管大多数厂商已经限制了 AI 在金融领域的能力，但是威胁猎人研究发现，在通过对提示词的绕过以及安装插件获取原本被限制的截图权限后，AI 智能体依旧可以模拟正常人进行转账、签约等需要银行取款密码才能执行的高度敏感操作。

以下是威胁猎人研究人员的相关测试情况：

(安全策略被规避后，AI 可执行银行转账流程)



(安全策略被规避后，AI 执行第三方快捷支付签约与授权操作)

该测试现象反映出：

- 基于提示词或策略约定的安全机制，本质上仍属于“软约束”；
- 当智能体被允许“重解释规则”时，其安全边界将高度依赖使用者意图；
- 金融机构的“黑屏风控”策略并非坚不可破，可以依赖外部的插件进行破解。

威胁猎人内部测试表明，AI 智能体在金融场景中已具备理解并执行部分敏感操作流程的技术可行性，在特定条件下对安全策略的约束依赖存在不确定性。尽管尚未发现相关能力被实际滥用的案例，但其对以人工操作为前提的传统风控假设已构成潜在冲击，金融机构值得提前评估与应对。

3.1.4 “国补”欺诈产业现状

2025 年，在“国补”政策监管下，威胁猎人情报平台仍监测到黑灰产利用国补漏洞获利。黑灰产通过联合快递员违规验收、资格转卖、违规核验操作、伪造回收刷单套利、招募个人回收国补等多种手法套取国补优惠。

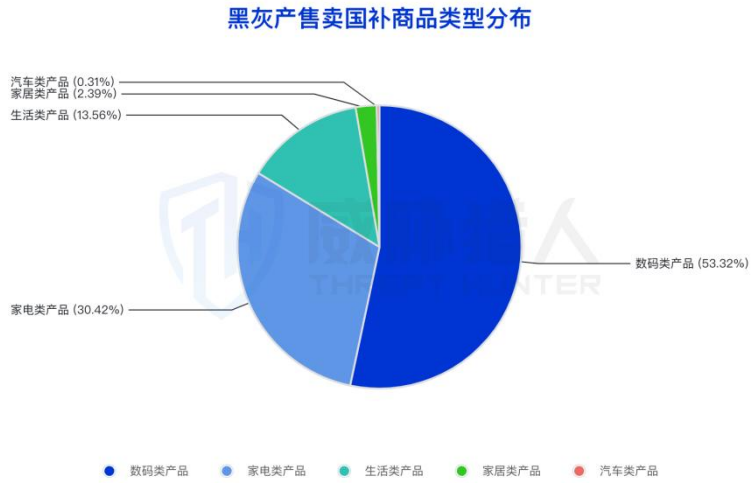
这些手法涉及多个角色，包括黑灰产、商家和个人用户，具体涉及作弊用户、转卖资格用户、商家、代销商、黄牛、快递员等。这些角色相互配合，通过代买、转寄、代激活等方式绕过国补地区和用户监管，形成了一个复杂的利益链条。

多角色协同牟利点及手段如下：

主要群体	核心手段	牟利点
黄牛	招募散户回收国补资格，大量“撸取”国补商品并进行二次转卖	套取补贴倒卖
作弊商家	在用户未实际到店的情况下，通过远程扫码伪造设备违规核验，完成国补核销。	获得商户补贴、提升销量
代销商	利用多重优惠组合套利、包装产品低价引流，骗取补贴资金。	获得商户补贴、提升销量
个人用户	贩卖个人国补资格并协助购买者激活	赚取跑腿费及贩卖资格费用
快递员	协助伪造签收、收取一定好处费协助违规用户转寄	赚取小额佣金

1、数码家电产品成为国补商品贩卖重灾区

威胁猎人对交易市场黑灰产贩卖国补相关商品的种类数据进行统计，交易热度 TOP 的商品类别分别为：数码类产品、家电类产品、以及生活类产品，占比分别为 53.32%、30.42%和 13.56%。



数码类产品	手机、平板电脑、智能手表、耳机等产品，以电子设备为主
家电类产品	冰箱、电视机、洗衣机、空调、洗碗机等大型电器类
生活类产品	吹风机、冲牙器、脱毛仪、电脑外设等
汽车	汽车，汽车用品类

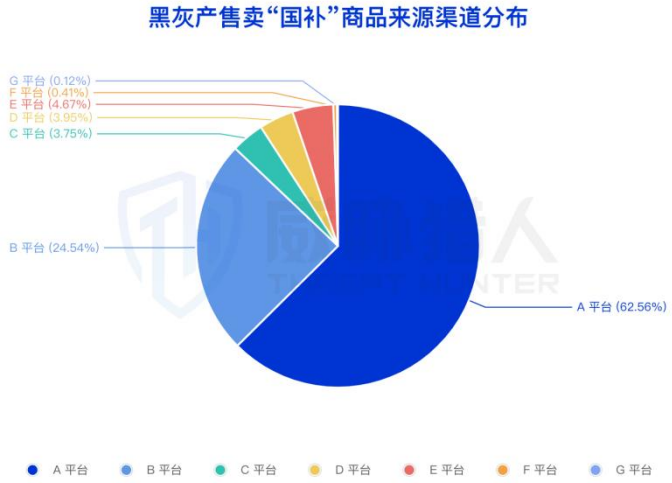
2、售卖国补商品的黑灰产主要分布地区 TOP3：上海市、北京市、深圳市

威胁猎人研究人员根据监测到的各大交易平台中贩卖国补商品的个体黑灰产店铺注册地分析发现，售卖国补商品的黑灰产主要分布在上海、北京、深圳、广州等经济发达地区。

3、售卖国补产品来源渠道主要来源国内两大头部电商平台

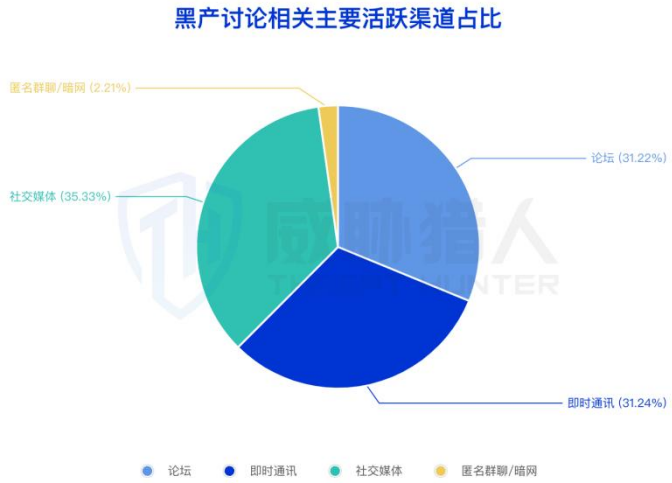
注：以下报告内容已做脱敏处理（相关电商平台用 A、B、C 等代称）

威胁猎人从捕获周期样本数据中对黑灰产售卖的国补产品来源渠道信息进行统计，其中 87.1%的国补产品来源国内两大头部电商平台。



4、 黑灰产在论坛和社媒进行广告发布后引流到私域完成交易

威胁猎人监测到，围绕国补“代购、转寄、返现、回收”相关的风险的讨论渠道中，黑产常伪装成“省钱攻略”，在社交媒体、论坛和即时通讯软件等渠道发布、引流以及交易。



5、国补产业链各类角色套取国补优惠手法分析

2025 上半年，威胁猎人通过多渠道监控发现，黑灰产围绕“国补”形成了多种作弊手法，主要包括以下五类：

- **黄牛在社交平台招募，快递员成违规帮凶**

  黄牛通过社交平台召集用户并引导其通过微信群填写个人信息、选择商品下单，再通过快递员违规验收设备回收国补资格。这一手法利用了社交平台和快递员协作的漏洞。

- **商家远程非本人异地代激活**

  部分商家通过微信视频远程让购买者激活设备，绕过了线下门店要求的身份证核验和设备核验，直接通过快递将设备送达购买者。

- **代销商利用三重优惠贩卖国补**

  代销商通过三重优惠（国补补贴、以旧换新、平台优惠）低价销售国补商品，并通过虚假回收旧品方式绕过以旧换新的规定，进一步降低成本。

- **社交平台招募转卖国补资格，线下违规核验与邮寄交易**

  用户将国补资格转卖给他人，并通过家人或朋友在门店代为购买设备、核验后通过邮寄完成交易，绕过了国补的资格和地域限制。

- **快递员协助转寄绕过国补地区限制**

  用户通过与快递员协商，将设备转寄到异地完成交易，绕过了国补的地域限制，继续套取补贴。

6、近期新增：两类“异地套取国补”手法拆解

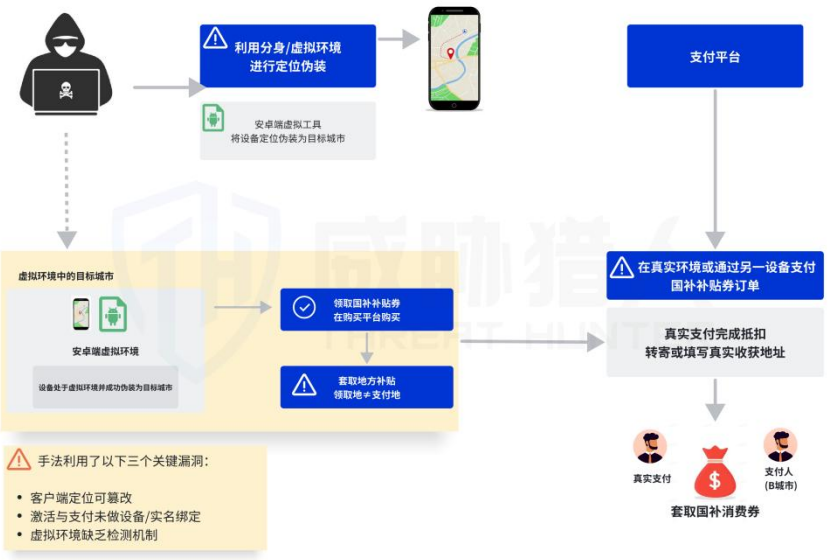
2025 年下半年，随着传统模式被持续打击，传统手法的活跃度在 2025 年下半年有所减少，黑灰产不断创新，研究出新的“异地套取国补”手法，近期威胁猎人发现了以下两种新型手法：

1）利用发券平台和支付平台校验链路解耦漏洞

这一手法主要利用了发券平台与支付平台校验链路解耦，即发券平台和支付平台之间的补贴领取和支付环节缺乏严格的核查与验证，使得黑灰产可以“在 A 城市的发券平台领取国补，在 B 城市的支付平台完成支付”，绕过双方风控措施，实现了跨地区国补领取。

2）虚拟环境+定位伪装型

这一手法主要利用“安卓端虚拟环境和定位伪装”技术，修改设备地理位置实现异地补贴领取，再切回真实环境或者用另一台设备完成支付，最终完成国补套取。



3.2 金融信贷欺诈分析

威胁猎人观察到，因 2025 年 8 月腾讯微信平台响应 “清朗行动” 的专项治理，聚焦黑灰产与违规群组实施相关风控政策，以及 2025 年下半年以来，公安部和国家金融监管总局联合部署开展金融黑灰产打击活动，2025 年下半年金融贷款舆情量较 2025 年上半年有所下降，但其中恶意贷款欺诈风险舆情整体仍有所上升。

相关名词定义：

恶意贷款欺诈：是指从事冒充银行名义进行虚假宣传贷款业务、包装骗贷、违规提额、违规转贷、违规套现、诱导性贷款、收取客户高额手续费、卷款跑路、诈骗客户谋利、发放高利贷等违规业务以谋取私利的金融欺诈行为。如背债、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、债务优化等业务行为。

债务优化：通常指通过代理投诉、代理维权等手段，对债务人的债务结构、还款方式、利息成本等进行调整和优化，以减轻债务人的还款压力、改善财务状况的过程。债务优化与逃废债存在关联，主要表现为通过黑产代理投诉等方式，实现分期还款、延期分期、减免结清等，从而达到缓还、少还债务的目的。

融车套现：也称 套车 或 融车 ，是指急需用钱的客户主动找到黑产或黑产招募客户贷款购车后将车辆转卖套现的行为。

职业背债：是指完全没有贷款资质（如征信为纯白、小白、小花，文化程度较低）或资质较低

且有背债意愿的人在黑产的包装下，申请银行大额贷款。职业背债以高额利益为目的，不打算偿还债务。职业背债主要分为 2 类： 一类是 “包装贷”， 另一类是 “背坏账”

包装贷 ：通过捏造身份伪造材料骗取银行高额贷款的行为，比如 “房”、“信”、“企”、“车” 贷款

背坏账 ：企业名下有坏账或不良资产影响企业经营或声誉，企业通过股权转让、资产处置、抵押等方式，背债人独自背负企业债务的行为，比如 “企业直背”、“银行直背”

3.2.1 2025 年金融贷款恶意欺诈舆情和黑灰产规模保持高速增长

3.2.1.1 2025 年下半年金融恶意欺诈舆情较 2025 年上半年增长 32%

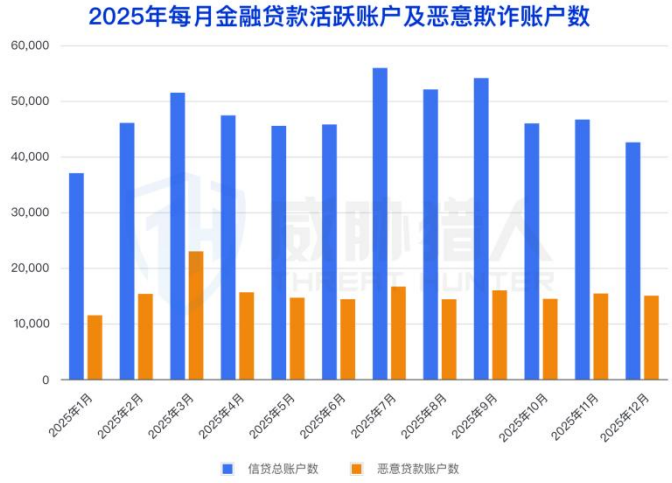
2025 年威胁猎人监控捕获金融贷款风险舆情达 680 万条，其中恶意贷款欺诈舆情 189 万条，占总量 27%。

2025 年下半年金融贷款舆情较 2025 年上半年下降 12%，2025 年下半年恶意贷款欺诈风险舆情较 2025 年上半年增长 32%。

3.2.1.2 2025 年威胁猎人共监控到活跃金融贷款群组 3.7 万个，其中恶意欺诈群组 1.8 万个，占总量 50%

3.2.1.3 2025 年恶意贷款欺诈账户数占金融贷款帐户的 30%

2025 年威胁猎人共监控捕获活跃贷款服务账户 33 万个，其中提供恶意贷款服务的欺诈账户（信贷黑中介/黑产）10 万个，占总量 30%。



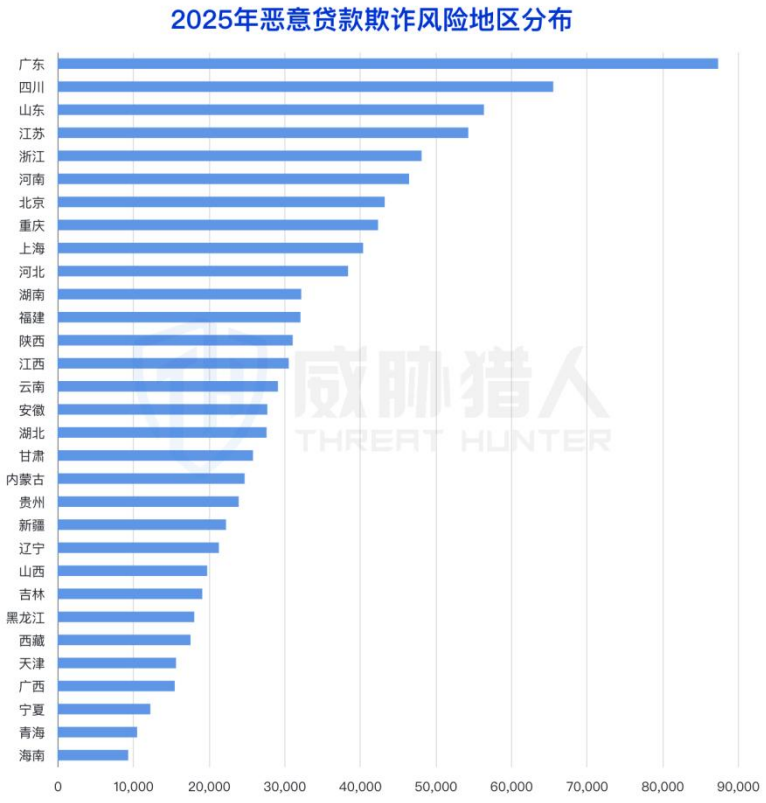
3.2.1.4 2025 年恶意贷款主要欺诈类型 TOP3：职业背债、债务优化、征信修复

2025 年数据显示，恶意贷款主要涉及职业背债、债务优化、征信修复、材料造假、融车欺诈、债务重组等超过 9 类欺诈行为，其中职业背债占比高达 37%，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，其中债务优化代理投诉类业务占比，出现成倍增长。

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。

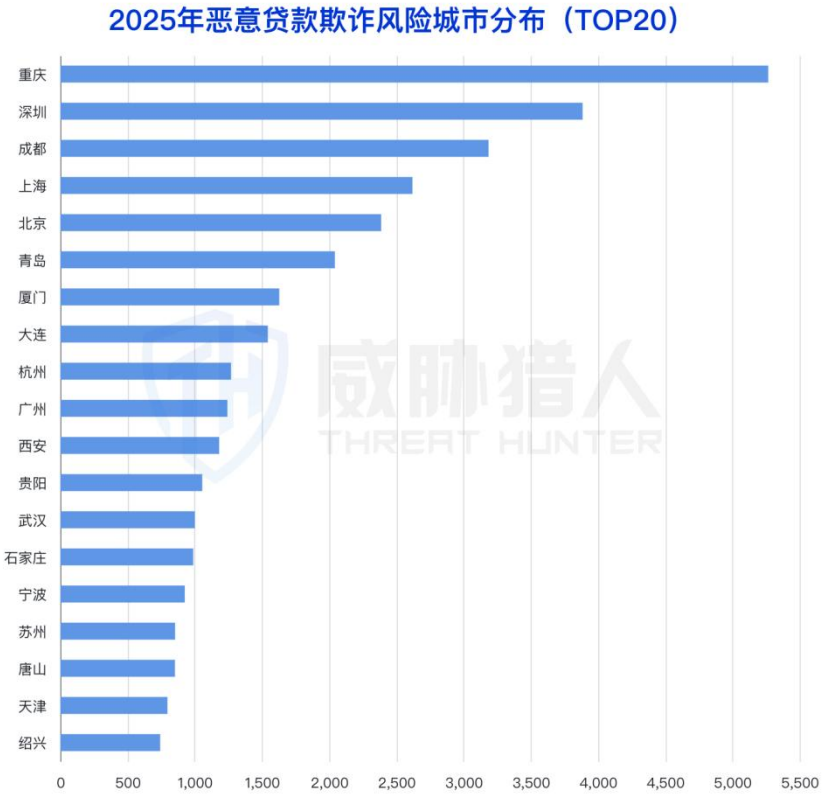
3.2.1.5 2025 年恶意贷款欺诈风险地区 TOP5：广东、四川、山东、江苏、浙江

威胁猎人情报数据显示，2025 年恶意贷款欺诈活跃热度 TOP5 的省份（含直辖市）是广东、四川、山东、江苏、浙江，其中广东地区风险值远高于其他地区。



3.2.1.6 2025 年恶意贷款欺诈风险城市 TOP5：重庆、深圳、成都、上海、北京

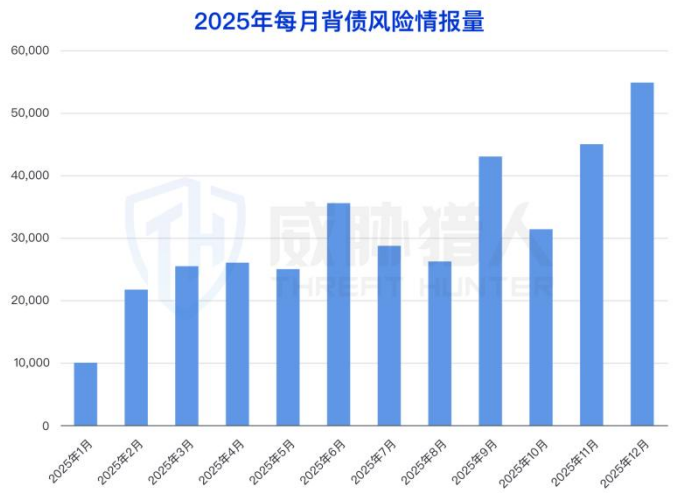
威胁猎人情报数据显示，2025 年恶意贷款欺诈活跃热度 TOP5 的城市（含直辖市）是重庆、深圳、成都、上海、北京。



3.2.2 2025 年职业背债风险舆情仍保持较快增速

3.2.2.1 2025 年每月职业背债风险舆情量持续增长，下半年较上半年增长 59%

2025 年威胁猎人监控捕获职业背债风险舆情量达 37 万条，从整体来看，每月风险舆情持续增长，2025 年下半年较上半年增长 59%



3.2.2.2 2025 年背债地区热度 TOP5 省份：广东、四川、山东、河南、重庆

威胁猎人情报数据显示，2025 年背债相关的贷款欺诈，活跃热度 TOP5 的省份（含直辖市）是广东、四川、山东、河南、重庆。

3.2.2.3 2025 年背债城市热度 TOP5 城市：重庆、广州、成都、上海、深圳

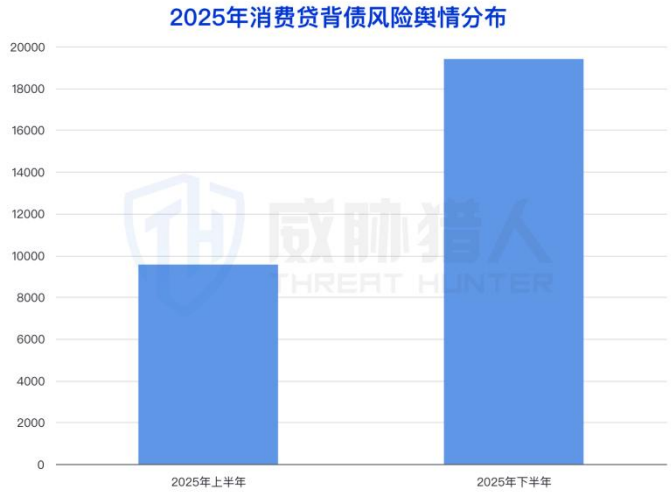
威胁猎人情报数据显示，2025 年背债相关的贷款欺诈，活跃热度 TOP5 的城市（含直辖市）是重庆、广州、成都、上海、深圳。

3.2.2.4 2025 年职业背债黑产策略升级与贷款场景风险分化

2025 年，职业背债黑产的运作策略进行全面升级：操作模式从单打独斗转向黑产间的资源共享与利益最大化合作；目标客群从重点挑选征信“纯白户”转向拥有良好信贷记录的“优质小白”；攻击场景则从“房信企车”的全覆盖，转为根据背债人资质精准挑选最优场景。

从背债攻击的风险舆情增速看，不同场景在 2025 年下半年呈现显著分化。其中，消费贷与企业贷场景风险高涨，下半年环比增长率均超过 80%，是主要的增长领域；相较而言，房贷与车贷场景增速相对平缓，环比增长率分别为 46.2%和 13.1%。

2025 年消费贷背债风险舆情激增，下半年较上半年翻倍增长达 103%



2025 年企业贷背债风险舆情高位运行，下半年环比增长 87.8%

3.2.3 金融贷款不同场景中的典型欺诈风险类型介绍

当前，房贷、车贷、消费贷及企业贷作为核心信贷场景，已成为黑产的重点攻击目标。不同贷款场景因产品特性与风控逻辑各异，不仅受攻击程度不同，其欺诈风险类型存在差异。

以下是各贷款场景中当前面临的主流欺诈方式：

贷款场景	房贷	消费贷	企业贷	车贷
欺诈类型	融房套现 房信企车组合背债 开发商假按揭	包装骗贷（背债） 债务重组 AB贷	职业背债 科技提额 经营贷欺诈 材料包装	融车套现 顶名车 传销购车 套路运

围绕这一领域，威胁猎人将于后续发布《2025 年中国信贷欺诈风险趋势报告》，对上述相关问题进行更为系统、深入的研究与解读。

3.3 钓鱼仿冒场景分析

3.3.1 风险事件类型分布：仿冒网站风险占比三成，社媒与客服仿冒风险增长明显

2025 年全年，威胁猎人共捕获到钓鱼仿冒风险事件 17W 例，涉及 237 家企业，整体呈现出显著的季节性爆发与手段更替趋势。

从风险事件的类型来看：

- **仿冒网站风险稳居“基石”地位，Q1 爆发明显：** 2025 年共捕获仿冒网站攻击 5 万起（占比 33.2%）。尽管下半年增速放缓，但其在第一季度占据绝对主流。作为诈骗链路的基础设施，搭建虚假站点套取敏感数据仍是攻击者的核心手段。
- **社媒与客服仿冒风险增长明显：**值得关注的是，仿冒社交媒体与仿冒客服电话相关攻击事件在第三季度出现明显增长，并与“暑期经济”带来的社会活跃度提升高度相关，反映出黑产团伙对阶段性流量热点的快速响应能力。

仿冒社交媒体（分布式裂变传播）： 针对暑期游戏市场的热潮，黑产团伙采取了“自持高权重号+分布式裂变”的组合手段。除了传统的自运营账号矩阵外，利用大量看似普通用户的账号在社交平台发布高度同质化的仿冒诱导内容（如虚假福利、高比例返利等）。这种模式极大地提升了违规内容绕过平台审核机制的存活率，其核心目的在于将官方流量精准拦截并导流至非法游戏私服，实现快速套现。

仿冒客服电话（GEO 投毒）：2025 年第三季度期间，攻击团伙针对借贷类 APP 的“客服、退息、解冻”等高频搜索词，利用搜索引擎算法漏洞进行区域性霸屏，直接将虚假客服电话嵌入搜索结果的显眼位置。这种技术手段不再依赖被动的短信广撒网，而是实现对主动寻求帮助用户的精准流量“截杀”，极高的攻击触达率直接推动该时段风险数据的爆发式增长。

3.3.2 金融行业为黑产攻击的主要目标

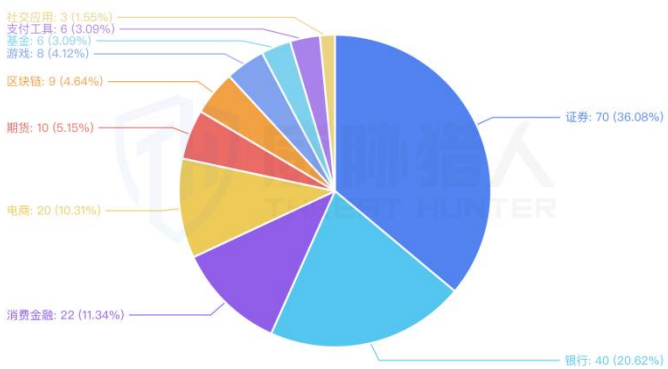
2025 年监测数据显示，钓鱼仿冒风险呈现出“高度金融化、金融内广谱覆盖”的特征，黑产攻击策略由聚焦少数头部机构，转向对金融行业的规模化覆盖与分层收割。

从行业分布来看，金融领域（证券、银行、消费金融、基金等）合计占比高达 76.28%。其中，银行、证券及消费金融等可直接导向资金损失或账户接管的核心业务场景，仍是黑产优先攻击的重点目标；

但与此同时，黑产攻击范围不再局限于少数头部机构，而是通过域名批量注册、模板化站点复用及脚本化投放等方式，将大量中小金融机构系统性纳入仿冒范围。

而非金融交易场景，则聚焦引流与变现 ：如电商行业（10.31%）主要作为支付与退款诱导的入口；而区块链行业（4.64%）与游戏行业（4.12%）则利用资产高波动的特性，实施空投或充值拦截。

2025年钓鱼仿冒风险行业占比



总体来看，攻击者系统性利用金融品牌信任与用户对“官方通知、账户异常、合规验证”的心理预期，推动仿冒从“做得更像”升级为“覆盖更广、触达更频繁”，并在登录、转账、验证码/授权等关键环节形成闭环变现。

3.3.3 AI 大模型时代的新型品牌风险：仿冒客服电话的 GEO 投毒

3.3.3.1 从“仿冒客服电话”升级为“污染 AI 的信息供给”

过去，黑灰产获取用户主要依赖仿冒网站、短信钓鱼、搜索广告等方式，其攻击链路集中在“链接层”。

随着 AI 搜索、智能问答逐步成为用户获取官方信息与联系方式的重要入口，攻击面发生了根本性变化——黑产不再只是“仿冒企业官网”，而是转向污染 AI 会引用的信息源，使用户在询问“客服电话”“官方联系方式”等问题时，直接获得错误答案并主动拨打。

威胁猎人监测发现，2025 年第三季度，多家高权重内容平台集中出现高度同构、批量生成的文章。这些内容正文大多为正常资讯，但在关键位置被系统性植入虚假客服电话。该现象并非普通违规内容，而是典型的 GEO 投毒 行为。

3.3.3.2 什么是 GEO 投毒：利用“生成式搜索”的引用机制做定向欺骗

GEO 投毒是指黑灰产借鉴并利用生成式搜索的“引用与综合”机制，刻意构造并大规模投放虚假或误导性内容，使大模型在检索与生成答案时优先引用这些信息，从而在 AI 搜索、智能问答等场景中输出错误结果（如仿冒客服电话），最终将用户引入诈骗链路。

其本质区别在于：

传统攻击影响的是“用户点到哪里”，而 GEO 投毒影响的是“AI 直接告诉用户什么”。

3.3.3.3 新型 GEO 投毒相对传统钓鱼仿冒的四个变化

- **攻击入口变化：从“点链接”转为“信答案”**

在生成式搜索场景下，用户不再判断链接是否可疑，而是直接采信系统生成的答案。攻击入口从可识别的仿冒页面，转移为“权威、自然的咨询结果”，显著降低了用户的防范与核验概率。

- **攻击目标变化：从“流量劫持”升级为“认知劫持”**

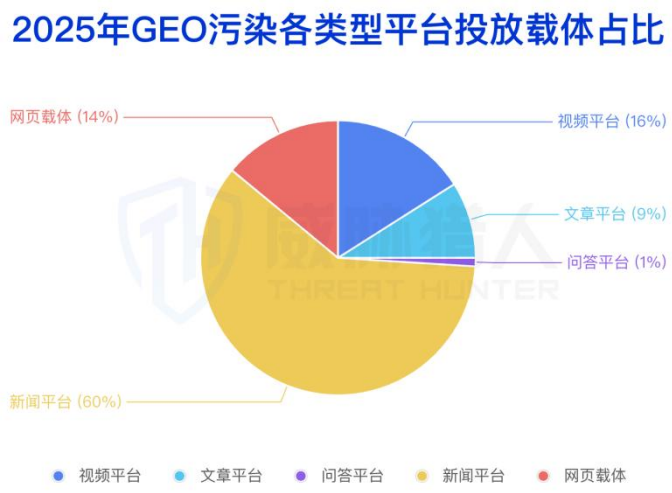
GEO 投毒并非追求单次曝光，而是通过反复铺量制造“多数一致”的错误信息，让 AI 在综合多个来源时形成稳定的错误判断，直接操纵用户的决策路径。

- **攻击载体变化：从低质站群转向“高权重内容平台”**

威胁猎人监测数据显示，GEO 投毒内容已明显集中于更容易进入模型引用体系的平台，其中

- 新闻平台占比 60%
- 视频平台 16%、文章平台 9%
- 问答平台仅 1%，已不再是主要阵地

高权重平台合计占比达 86%，成为影响 AI 检索与生成结果的主要污染源。这意味着，即便企业官网信息完全正确，仍可能在 AI 场景中被“权威平台的错误信息”所覆盖。



- **攻击方式变化：黑产攻击方式更加规模化、模板化、可复用**

黑产围绕 GEO 投毒已形成一套高度标准化、可规模复制的“三件套”打法：

1、利用高权重平台，提高进入模型引用库的概率；

2、利用脚本化批量生成内容，其核心策略是，使用同一个仿冒号码（如“XXX 人工专线 00xx-6xxx-73xx”），并通过脚本自动替换上百个不同的金融品牌名称，实现极低成本的跨平台“投毒矩阵”。

3、以标准化新闻体裁包装内容，文章约 95% 为真实但无关信息，仅在关键位置嵌入伪造联系方式，利用模型对“权威叙事”的信任偏好，提升投毒内容的隐蔽性。

3.3.3.4 AI 搜索结果被污染后的四类直接影响

在 GEO 投毒行为持续作用下，其危害已不再停留在内容层面，而是直接体现在 AI 搜索与智能问答的最终输出结果中，对用户决策与品牌安全产生实质性影响。

以威胁猎人监测到的一个真实案例为例：

如下图所示，当用户通过 AI 搜索场景查询某品牌“客服电话” “官方联系方式”等高频需求时，AI 并未仅引用品牌官网或权威渠道信息，而是综合调用了多个被污染的高权重平台内容作为“参考资料”，并在生成式答案中对这些信息进行了结构化整合与再输出。

在上述案例中，使用 AI 搜索结果呈现出以下明显风险特征：

1、虚假客服电话被当作“官方信息”展示

被植入的号码未以广告或异常内容形式出现，而是被整理进客服信息列表、公告说明或参考资料中，整体呈现方式接近官方渠道，普通用户难以区分真伪。

2、重复引用放大错误信息影响

AI 在生成答案时同时引用多个来源，而这些来源中存在被批量投放的相同虚假号码。当同一信息在不同页面中反复出现时，错误内容被进一步放大并固化。

3、用户直接被引导至高风险联系方式

在 AI 搜索场景下，用户通常直接采信生成结果中的联系方式，较少再进行二次核验。一旦拨打虚假客服电话，极易进入诈骗或信息窃取环节。

4、品牌官方渠道被弱化甚至替代

即使品牌已公开正确的官方客服信息，在 AI 输出结果中仍可能被覆盖或挤出，导致用户优先接触到错误内容。

3.3.3.5 治理思路：源头处置 + AI 端纠偏的“双管齐下”

威胁猎人 DRP 品牌保护团队针对 GEO 投毒风险，采用“源头与终端双管齐下”的治理策略，不仅压缩了黑灰产的空间，还保障了品牌在 AI 搜索与问答中的权威性和安全性。

- **切断污染源头：**对投毒内容快速取证并向相关渠道发起下架申请，覆盖社交媒体、问答、视频、文章等平台。监测实践显示，下架成功率可达 93%，能直接阻断扩散链路。
- **推动 AI 平台纠偏：**同步向 AI 平台提交投毒线索与证据，要求修正检索结果与引用库，降低错误信息继续被生成的概率；结合自动化巡检 + 人工复核，持续监控“品牌名+客服电话/官方联系方式”等高频查询词，形成长期防护闭环。

3.4 数据泄露场景分析

3.4.1 2025 年全年数据泄露事件共 41644 起，较 2024 年全年环比上升 10.83%

威胁猎人数据泄露风险监测平台数据显示，2025 年 1 月至 12 月全网监测了 7.67 亿条关于数据泄露的情报，基于威胁猎人真实性验证引擎以及 DRRC 专业人工分析验证出有效的数据泄露事件共计 41644 起，涉及金融、电商、快递等关键行业共 2120 家企业。

*本报告中的年度数据未纳入部分海外及无明确企业主体的数据泄露事件，统计口径相较上半年有所收敛，相关指标变化主要由此产生。

3.4.2 银行业数据泄露风险连续三年排行第一，软件应用行业首次登上前10

3.4.2.1 金融行业风险"断层式"领先

2025 年数据泄露重灾区进一步向资金密集型行业集中。银行业 数据泄露事件稳居榜首，消费金融行业则强势反超电商行业，跃升至第二位。加上排名大幅前移的支付（升至 Top 4）与证券（升至 Top 5），"泛金融"板块已占据 Top 5 中的四席，显示黑产攻击重心在于高变现价值的信贷与资金流数据。

3.4.2.2 本地生活“强登”情报大幅下降，软件应用取代本地生活成为新靶点

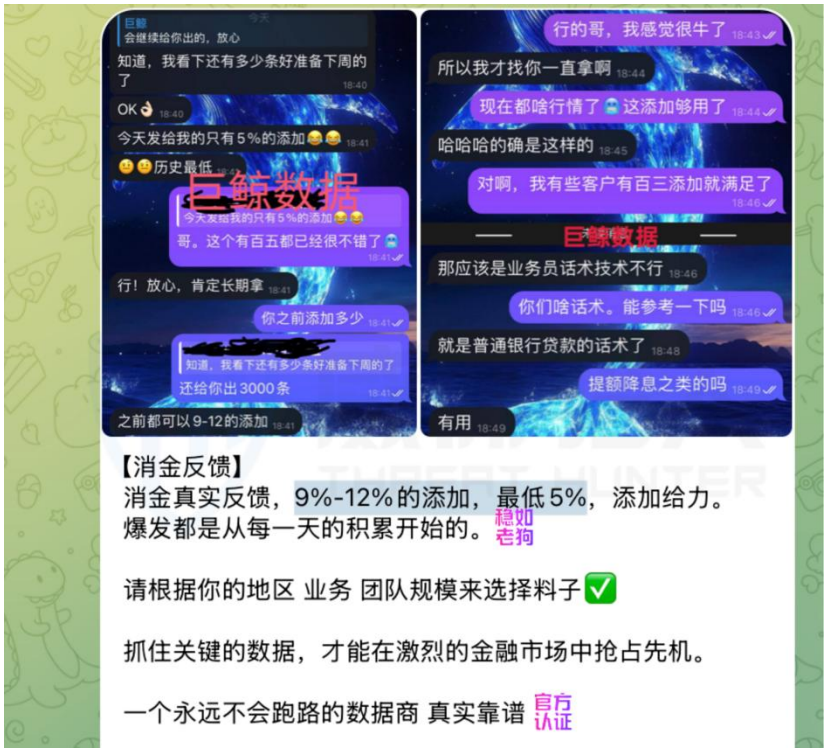
"软件应用"行业取代了"本地生活"行业，首次跻身 Top 10。据威胁猎人观察发现，一方面 2024 年本地生活行业火热的“强登”查档泄露在 2025 年出现大幅下降（-61.38%），推测涉及到的本地生活企业针对该泄露风险做了对应的风控措施，提高了黑产窃取数据的门槛。因此窃取数据的上游黑产将攻击重心转向具有动态价值的移动端用户行为数据，如应用内交互行为、位置与轨迹信息等。

3.4.3 消金贷款用户信息泄露事件持续上涨，新型泄露方式多样化

从时间分布来看，2025 年消费金融行业非法数据交易事件呈现出明显的阶段性上升趋势。年初至上半年，相关事件数量整体处于相对低位并缓慢增长；进入下半年后，事件量开始明显抬升，并在 10—11 月达到全年高点；通过深入分析，威胁猎人发现消费金融非法数据交易事件上涨主要集中在几类新兴数据类型中。

在黑产频道中提及到“热销数据类型”名单中，“消金申请”“银行扫码”“多头贷款”等数据类型频繁出现。尤其是“消金申请”类数据；以某黑产频道每周更新的热销榜单为例，该类数据产品自 2025 年 8 月至 2025 年 12 月期间持续位列热销 Top，显示其已在非法数据交易市场中形成稳定且活跃的交易需求。同时，从下游作恶场景中的使用反馈，也从侧面反映出该类数据在真实性与可用性方面具有较高价值。

（某黑产团伙频道每周更新的数据类型热销榜单中，“消金申请”数据长期高居第一）



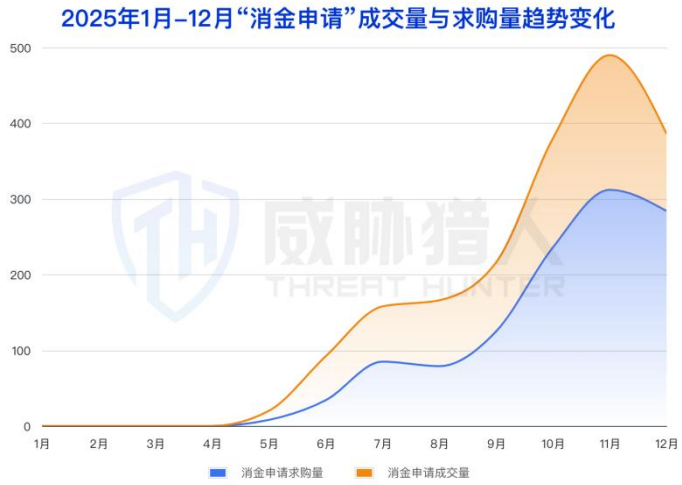
（下游作恶效果反馈，侧面反映了数据的真实性）

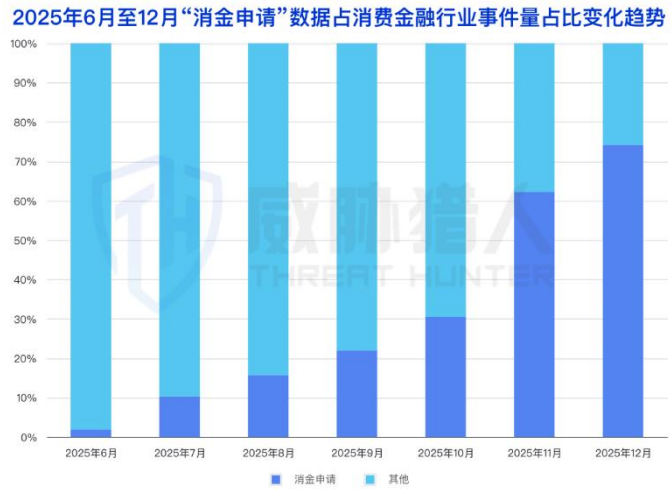
3.4.3.1 “消金申请”风险趋势与产业生态解析

1、消金申请数据泄露事件持续上涨，至 2025 年 12 月超 600 起，占整体贷款信息数据类型的 70%

威胁猎人监控发现，“消金申请”类数据最早于 2025 年 5 月底在部分数据交易黑产群中出现，而后经过 2 个月的“试水”阶段浅尝到甜头，在 2025 年 7 月底正式上线大规模被非法数据交易

黑产中介推广，并在 2025 年 12 月达到顶峰，在非法数据交易市场上的贷款数据类型占比中高达 70%。同时从成交与需求变化来看，“消金申请”类数据的成交量与求购量走势高度一致，并在下半年同步呈现爆发式增长。





据威胁猎人观察，泄露的“消金申请”数据，其泄露的数据样例格式字段主要以用户手机号、平台名称、姓名、地区以及申请贷款成功的状态信息，其中姓名信息并非都具备的信息内容，威胁猎人研究人员跟进和售卖数据的黑产中介了解到，确认部分姓名信息为后期清洗加工补充的信息。

phone	product	name	province	city	isp
13	融		福建	龙岩	申请成功
15	融		福建	龙岩	申请成功
18	融		福建	龙岩	申请成功
19	融		福建	龙岩	申请成功
15	融	肖	福建	龙岩	申请成功
13	融	陈 华	福建	龙岩	申请成功
15	融		福建	龙岩	申请成功
13	融	王	福建	龙岩	申请成功
13	融	廖 鑫	福建	龙岩	申请成功
13	融		福建	龙岩	申请成功
13	融	陈 峰	福建	龙岩	申请成功
13	融	林 琴	福建	龙岩	申请成功
18	融	范 圣	福建	龙岩	申请成功
13	融	林 灿	福建	龙岩	申请成功
13	融	钟 凯	福建	龙岩	申请成功
13	融	李 闽	福建	龙岩	申请成功
18	融	黄 兰	福建	龙岩	申请成功
17	融		福建	龙岩	申请成功
13	融	钟 生	福建	龙岩	申请成功
18	融	吴 秀	福建	龙岩	申请成功
18	融		福建	龙岩	申请成功
13	融		福建	龙岩	申请成功
15	融	吴 旺	福建	龙岩	申请成功
15	融	程 珍	福建	龙岩	申请成功
15	融		福建	龙岩	申请成功
15	融		福建	龙岩	申请成功
13	融	林	福建	龙岩	申请成功
15	融	王 玉	福建	龙岩	申请成功
18	融		福建	龙岩	申请成功
15	融	杨 辉	福建	龙岩	申请成功
13	融	卢 杰	福建	龙岩	申请成功
13	融	林 国	福建	龙岩	申请成功
13	融	沈 锋	福建	龙岩	申请成功
13	融	傅 龙	福建	龙岩	申请成功

（左图为消金申请数据格式，右图为黑产反馈姓名字段为清洗添加的）

2、“消金申请”产品数据不断迭代，涉及国内绝大多数消金、贷款平台

威胁猎人针对“消金申请”进行了深入分析发现，该款产品类数据主要分为四个阶段，分别是测试阶段（5 月-6 月）、正式上线（7 月-8 月）、精细化运营（9 月-10 月）、AI 模型提升阶段（11 月），以下是具体的产品发展时间线情况。

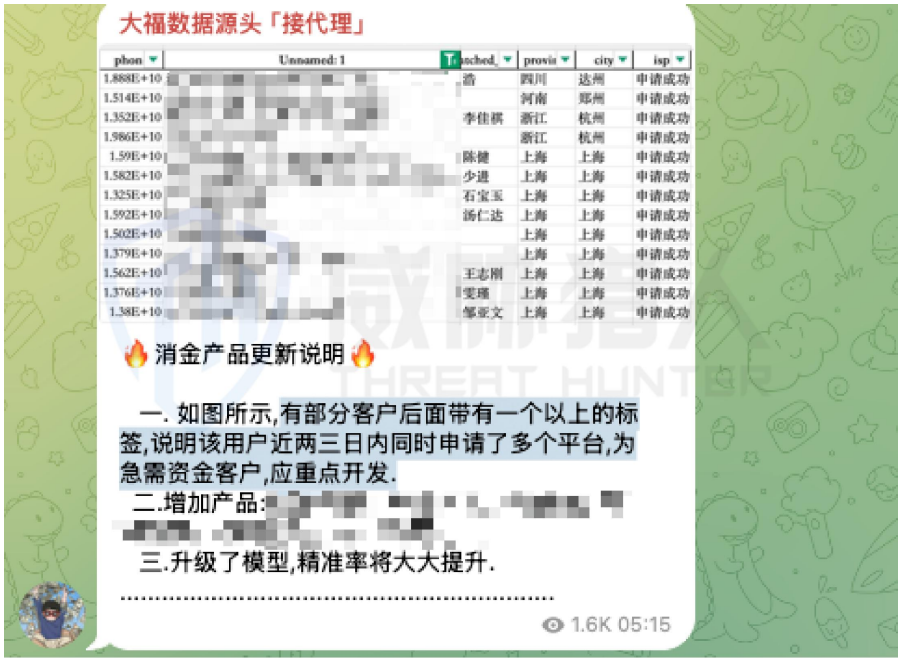
（消金申请产品发展时间线）

- **测试阶段：（5 月底 - 6 月）**

最早于 2025 年 5 月底首次有黑产提出明确的“消金申请”产品，其数据类型涉及部分消金平台以及银行贷款平台，数据时效性为隔夜（T+1），不支持指定平台，但可支持筛选用户所在地区，仅涉及 24 家持牌消金机构以及银行贷款产品。

- **正式上线：（7 月-8 月）**

“消金申请”产品数据于 7 月初开始新增企业贷类型数据，不再局限于 C 端贷款需求用户，补充了 B 端或小微企业主的信息数据；同时梳理出部分用户在短时间内在多个贷款平台申请的行为特征，标记为急需资金客户，供下游购买者进行精准作恶，涉及消金/贷款平台达 27 家。



（图为黑产正式上线消金产品后，补充了多平台标签特征以及模型优化）

- **精细化运营：（9 月-10 月）**

黑产针对持牌消金机构、银行系贷款、网贷平台、企业贷等不同类型平台进行划分拆解，以便满足下游不同贷款中介（资方）的作恶用户画像需求；同时数据类型共涉及消金/贷款平台达 40 家，支持可筛选具体平台。

产品类型	产品真实名称	所属银行/机构	银行/机构性质
消金产品	消费金融		全国性银行
	消费金融		全国性银行
	金融		全国性银行
	消费金融		全国性银行
	消费金融		全国性银行
	消费金融		全国性银行
	消费金融		全国性银行
	银行		全国性银行
	消费金融		地方性银行
	消费金融		地方性银行
	金融		地方性银行
	消费金融		地方性银行
	消费金融		地方性银行
	消费金融		地方性银行
	消费金融		地方性银行
	消费金融		地方性银行
	消金		地方性银行
	消费金融		地方性银行
	消费金融		地方性银行
	消费金融		地方性银行
			互联网科技背景
			互联网/电商背景
银行产品	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	银行-贷款		全国性银行
	商银行-贷款		地方性银行
	银行-贷款		地方性银行
	银行-贷款		地方性银行
	银行-贷款		地方性银行
	银行-贷款		地方性银行
	银行-贷款		地方性银行
网贷产品			互联网/媒体背景
			互联网金融背景
			互联网/游戏背景
			互联网/电商背景
			互联网/电商背景
			产业集团背景
			互联网科技背景
			互联网科技背景
			产业/消费场景背景
			互联网金融背景
			互联网金融背景
			互联网科技背景
			互联网金融背景
			互联网金融背景
			互联网/旅游背景
企业贷款产品	银行		全国性银行
	银行		全国性银行

（图为黑产精细化整理的平台清单）

- **数据中介黑产利用 AI 模型对原数据进行清洗，提高数据价值（11 月）**

于 11 月初，非法数据交易黑产中介反馈“消金申请”数据交易量达顶峰，导致服务器内存极限，并针对性进行优化清理；涉及消金贷款、银行产品、网贷产品、企业贷款产品高达 60 家平台。在 11 月底，引入了 AI 大数据识别，从单纯的数据售卖转向“数据清洗+质量控制”，试图通过剔除劣质用户数据来维持数据的高价格和高转化率。

（黑产不断优化升级消金申请模型）

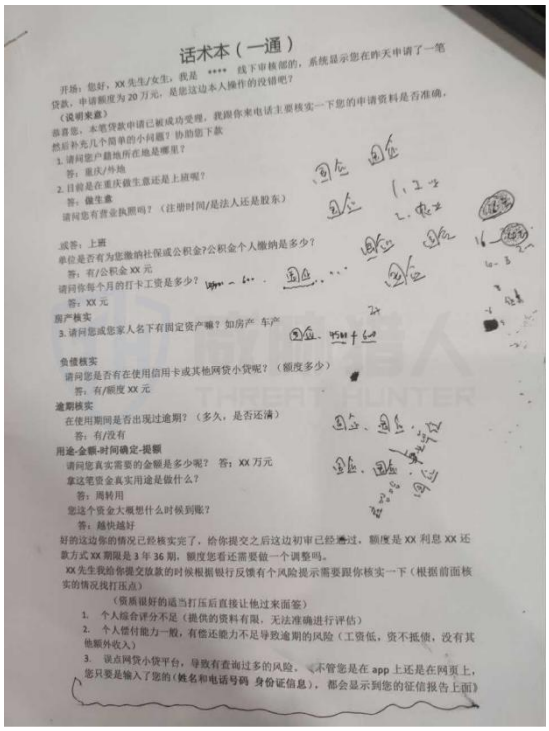
- **下游作恶：黑产获取数据后会针对性进行贷后营销作恶**

威胁猎人监测发现，黑产在获取“消金申请”类数据后，主要将其用于针对性较强的贷后营销类作恶行为。该类作恶通常围绕“已提交贷款申请”的用户展开，通过冒充官方或合作方身份，实施误导性引流与产品推广。

以下是威胁猎人监测到的两个案例：

例 1：威胁猎人运营人员从 Telegram 上监控到某数据交易黑产中介发布的“消金售卖测试话术”截图，主要是电话联系申请贷款人员，伪装成是对应消金贷款平台合作的客户经理，声称对方的贷款或业务已转由他负责，然后引导用户换产品或推广其他贷款业务产品。

例 2：威胁猎人运营人员从某贷款电销团伙获取到话术本内容，主要是伪装成对应消金贷款平台的线下审核部（回访部）员工的身份，以跟客户确认贷款资质信息等方式，最后引导到其线下门店推广其他贷款产品。


话术本（一通）

开场：您好，XX 先生/女生，我是 **** 线下审核部的，系统显示您在昨天申请了一笔贷款，申请额度为 20 万元，是您这边本人操作的没错吧？

（说明来意）

恭喜您，本笔贷款申请已被成功受理，我跟你来电话主要核实一下您的申请资料是否准确，然后补充几个简单的小问题？协助您下款

1. 请问您户籍地所在地是哪里？

答：重庆/外地

2. 目前是在重庆做生意还是上班呢？

答：做生意

请问您有营业执照吗？（注册时间/是法人还是股东）

或答：上班

单位是否有为您缴纳社保或公积金？公积金个人缴纳是多少？

答：有/公积金 XX 元

请问您每个月的打卡工资是多少？

答：XX 元

房产核实

3. 请问您或您家人名下有固定资产嘛？如房产 车产

负债核实

请问您是否有在使用信用卡或其他网贷小贷呢？（额度多少）

答：有/额度 XX 元

逾期核实

在使用期间是否出现过逾期？（多久，是否还清）

答：有/没有

用途-金额-时间确定-提额

请问您真实需要的金额是多少呢？ 答：XX 万元

拿这笔资金真实用途是做什么？

答：周转用

您这个资金大概想什么时候到账？

答：越快越好

好的这边您的情况已经核实完了，给你提交之后这边初审已经通过，额度是 XX 利息 XX 还款方式 XX 期限是 3 年 36 期，额度您看还需要做一个调整吗。

XX 先生我给你提交放款的时候根据银行反馈有个风险提示需要跟你核实一下（根据前面核实的情况找打压点）

（资质很好的适当打压后直接让他过来面签）

1. 个人综合评分不足（提供的资料有限，无法准确进行评估）
2. 个人偿付能力一般，有偿还能力不足导致逾期的风险（工资低，资不抵债，没有其他额外收入）
3. 该点网贷小贷平台，导致有查询过多的风险，不管您是在 app 上还是在网页上，您只要是输入了您的（姓名和电话号码 身份证信息），都会显示到您的征信报告上面）

围绕这一领域，威胁猎人将于后续发布《2025 年中国数据泄露风险趋势报告》，对上述相关问题进行更为系统、深入的研究与解读。

写在最后：

回顾 2025 年，黑灰产通过引入更贴近真实用户的攻击资源、利用生成式 AI 与智能体等新技术，黑灰产不断抬高作恶隐蔽性与成功率，使企业在风险感知、识别与响应层面承受更大的压力。

安全的本质是对抗成本的博弈。我们无法彻底消灭黑灰产， 但可以通过系统化的防御体系，持续抬高其攻击成本与失败风险。当攻击者在资源获取、技术突破与规模化作恶上的投入，显著高于其潜在收益时，黑灰产的作恶动机与可持续性将被根本削弱，这正是“不对称对抗”中防守方能够取得优势的关键所在。

防御的下半场，不仅是技术的角力，更是情报与认知的比拼。这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

扫码关注
获取行业最新反欺诈报告

服务热线：400-809-3699
官方网址：www.threathunter.cn
联系邮箱：marketing@threathunter.cn
总部地址：广东省深圳市南山区粤海街道科技园社区科苑路15号科兴科学园B2栋1705