威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

黑产大数据

2026年上半年互联网黑灰产趋势研究报告

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。

基于对黑灰产生态的持续监测，威胁猎人反欺诈情报研究团队发布《2026 年上半年互联网黑灰产研究报告》，系统呈现黑产资源变化、产业链演进及典型作恶场景。除本报告外，威胁猎人还将陆续发布《2026 年上半年信贷欺诈风险研究报告》和《2026 年上半年品牌外部风险研究报告》，分别聚焦信贷欺诈、数据泄露，以及钓鱼仿冒、品牌侵权等重点风险场景。

这是威胁猎人连续多年发布的互联网黑灰产行业研究报告，也是威胁猎人面向行业固定推出的年度趋势观察成果。作为专注于黑灰产情报与业务反欺诈的安全厂商，威胁猎人已在黑灰产情报领域深耕 10 年，依托长期积累的风险数据、真实攻击样本与企业治理实践，持续追踪黑产资源、攻击手法与产业链变化，持续为企业判断风险趋势、制定治理策略提供参考。

目录

前言

2026 年上半年，在监管打击、平台治理与企业风控持续加强的背景下，传统黑产资源有所收缩，但风险并未消退，而是加速向境外资源、更隐蔽的基础设施和更复杂的作恶链路迁移。

报告内容关键点总结：

- **传统黑产资源整体收缩，但风险正在发生结构性迁移。** 新增国内风险手机号较 2025 年下半年下降 53.6%，日均活跃风险 IP 下降 16.31%，洗钱对公账户和洗钱商户分别下降 70.81%和 48.23%；与此同时，非中国大陆地区猫池卡增长 110.55%。资源总量下降并不等同于风险消退，黑产供给正在向境外资源及更隐蔽的代理方式迁移。

- **业务欺诈仍处于高活跃状态，电商成为最集中的攻击场景。** 上半年累计捕获业务欺诈风险线报约 9 亿条，预警风险事件 2088 起，二季度事件量较一季度增长 65.54%。电商风险占比居首，达到 27.44%，相关风险线报较 2025 年下半年增长 83%，表明大促、补贴和高频交易仍是黑产重点套利目标。

- **黑产作恶已从单点攻击转向多环节、产业化运作。** 从品牌回收、窜货、假货和恶意拉踩，到赛事赌博引流、快消代下及电商套利，黑产正在整合获客、账号、支付、物流和变现等环节，并根据平台规则快速调整手法，攻击链路更加完整、专业且隐蔽。

- **企业品牌风险的核心，正从“发现仿冒”扩展到“保护用户与官方渠道之间的可信连接”。** 上半年确认有效数据泄露事件 23,645 起，同比增长 6.98%，其中重大风险事件增长 22.90%，且 95.02%的重大风险记录集中于暗网；同期记录钓鱼仿冒与品牌滥用事件 45,321 起，主要分布于搜索结果、仿冒网站、社交媒体、客服电话及下载渠道等用户入口。

- **信贷黑产规模呈现分化，高压治理正在淘汰低端参与者，但核心团伙仍在升级。** 恶意贷款欺诈舆情较 2025 年下半年增长 2%，活跃群组增长 17%，但欺诈账户下降 3%；职业背债舆情和服务账户均下降 31%，活跃群组却增长 3%。这表明黑产服务端有所收缩，但留存团伙正转向真实补缴、长期数据养护及技术与关系相结合的精细化欺诈。

01

2026 年上半年
黑产攻击资源分析

一、2026 年上半年黑产攻击资源分析

1.1 2026 年上半年风险手机卡资源分析

1.1.1 2026 年上半年新增国内风险手机号总量较 2025 年下半年环比下降 53.6%

2026 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 351.6 万，较 2025 年下半年环比下降 53.6%。

从风险类型结构看，本轮总量下滑与国内猫池卡、拦截卡两类核心黑卡资源同步收缩高度相关：2026 年上半年国内猫池卡较 2025 年下半年减少 26.7%，国内拦截卡较 2025 年下半年减少 68.35%。其中，拦截卡降幅更为显著，对整体新增风险手机号规模下降形成主要拉动。

1.1.2 2026 年上半年猫池卡资源变化趋势

（1）2026 年上半年国内猫池卡较 2025 年下半年减少 26.7%

据威胁猎人情报平台数据显示，2026 年上半年捕获新增猫池卡 91.19 万例，较 2025 年下半年环比下降 26.7% 。

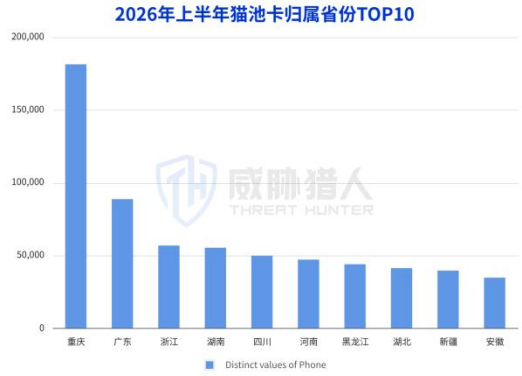
经威胁猎人情报专家分析，出现这一趋势的主要原因是：

1. 黑产供给侧遭遇攻击，导致服务稳定性下降。 2026 年上半年，发卡平台出现被攻击、站点异常、服务切换等情况。这类事件会导致发卡平台短期暂停销售或迁移站点，进而导致黑灰产侧可采购、可投放的猫池卡数量阶段性下降。
2. 部分接码平台暂停服务，影响下游代理和买家采购链路。 除发卡平台遭遇攻击外，部分主流接码平台在上半年也出现服务器异常等问题，导致下游代理商和买家无法稳定获取号码资源。

综合来看，发卡平台被攻击与主流接码平台阶段性停服共同削弱了国内猫池卡供给能力，是 2026 年上半年新增猫池卡规模下降的重要原因。

（2）2026 年上半年新增猫池卡归属最多的三个省份为：重庆、广东、浙江

威胁猎人对 2026 年上半年新增国内猫池卡进行统计分析，发现重庆、广东、浙江三省（含直辖市）为猫池卡归属地最多的三个省份。



省份	2026年上半年猫池手机卡新增数量排名	年度趋势
重庆	第一	维持
广东	第二	维持
浙江	第三	上升2位
湖南	第四	维持
四川	第五	上升7位
河南	第六	上升1位
黑龙江	第七	上升6位
湖北	第八	下降5位
新疆	第九	上升2位
安徽	第十	下降2位

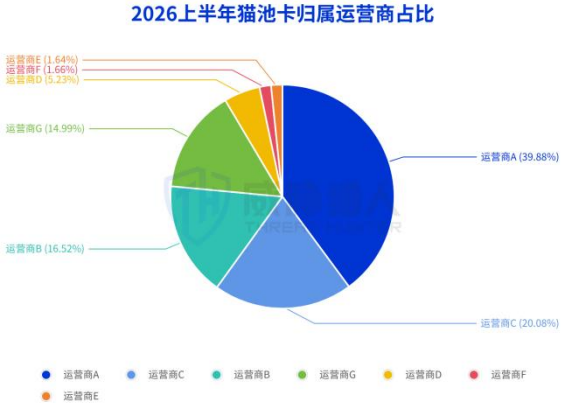
（3）2026 年上半年新增猫池卡归属最多的三个城市为：重庆、长沙、成都

威胁猎人对 2026 年上半年新增国内猫池卡进行统计分析，发现重庆、长沙、成都三地为猫池卡归属地最多的三个城市。

城市	2026年上半年猫池手机卡新增数量排名	年度趋势
重庆	第一	维持
长沙	第二	上升1位
成都	第三	上升7位
乌鲁木齐	第四	上升3位
杭州	第五	维持
北京	第六	上升15位
合肥	第七	上升2位
郑州	第八	上升4位
广州	第九	下降3位
上海	第十	下降6位

（4）2026 年上半年捕获的新增猫池卡中，归属国内四大运营商的占 81.71%

威胁猎人情报数据显示，2026 年上半年监测到新增猫池卡 91.19 万例，其中归属国内四大运营商的猫池卡占比 81.71%，归属虚拟运营商的猫池卡占比为 18.29%。

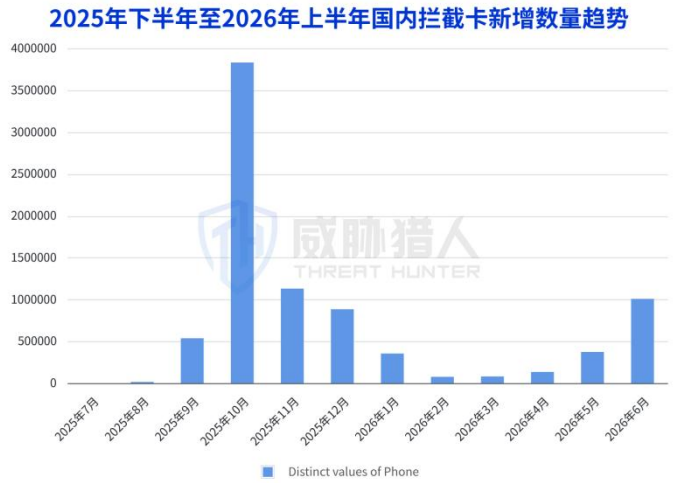


1.1.3 2026 年国内拦截手机卡资源变化趋势

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。

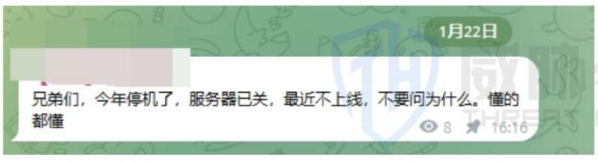
（1）2026 年上半年国内拦截卡较 2025 年下半年减少 68.35%

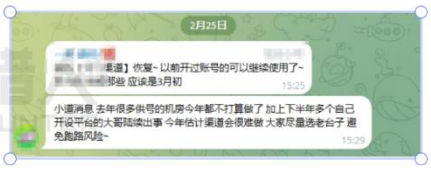
据威胁猎人情报平台数据显示，2026 年上半年，威胁猎人捕获新增拦截卡达 202.3 万，较 2025 年下半年减少 68.35%。



对黑灰产拦截卡供给情况的进一步分析显示：

2026 年上半年国内拦截卡新增规模大幅下降，核心原因之一是拦截卡供给侧在年初出现了明显收缩。多个拦截卡相关群组在 1 月至 3 月期间陆续发布"停机"、"关服"等公告，说明部分拦截卡平台、号商和通道在年初主动停服、暂停更新或退出供给，导致拦截卡新增供给断档。与此同时，6 月下旬群组中又出现"拦截卡商被监管打击"、"市面号商、卡量较少"等信息，反映拦截卡市场仍处于供给不稳定、可信货源减少的状态。





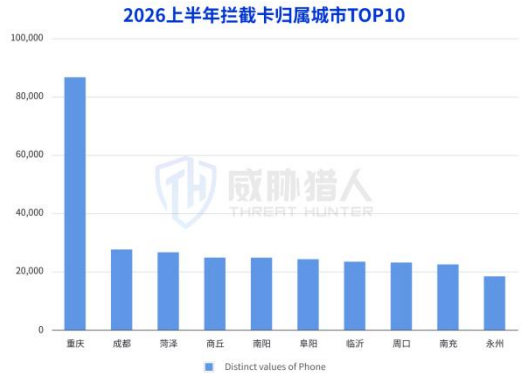
（2）2026 年上半年拦截卡归属最多的三个省份为：四川、河南、山东

针对 2026 年上半年捕获到的国内拦截卡统计分析发现，四川、河南、山东三省为拦截卡归属地最多的三个省份。

省份	2026年上半年拦截手机卡新增数量排名	年度趋势
四川	第一	上升2位
河南	第二	维持
山东	第三	上升1位
安徽	第四	上升1位
湖南	第五	上升1位
河北	第六	上升1位
广东	第七	下降6位
湖北	第八	维持
重庆	第九	维持
江西	第十	上升1位

（3）2026 年上半年新增拦截卡归属最多的三个城市为：重庆、成都、菏泽

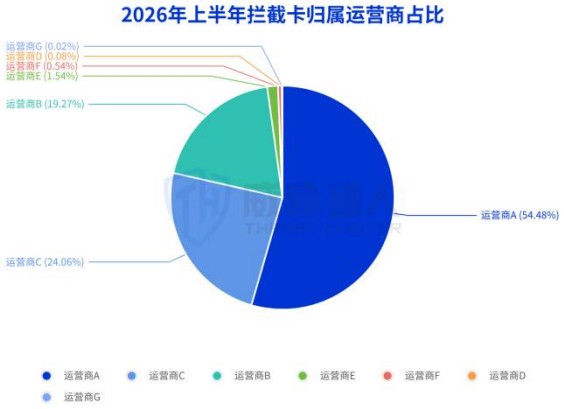
威胁猎人对 2026 年上半年新增国内拦截卡进行统计分析，发现重庆、成都、菏泽三地为拦截卡归属地最多的三个城市。



城市	2026年上半年拦截手机卡新增数量排名	年度趋势
重庆	第一	维持
成都	第二	上升4位
菏泽	第三	上升1位
商丘	第四	上升1位
南阳	第五	上升3位
阜阳	第六	上升1位
临沂	第七	上升2位
周口	第八	上升2位
南充	第九	上升6位
永州	第十	上升9位

（4）2026 年上半年捕获的新增拦截卡中，归属国内四大运营商的占 97.89%

2026 年上半年威胁猎人情报运营平台捕获新增拦截卡达 202.3 万张，归属国内四大运营商的拦截卡占比达 97.89%，虚拟运营商拦截卡占比为 2.11%。



1.1.4 2026 年[非中国大陆地区恶意手机卡]资源变化趋势

非中国大陆地区：包含中国香港、中国澳门、中国台湾及其他海外地区。

（1）2026 年上半年非中国大陆地区猫池卡较 2025 年下半年增长 110.55%

据威胁猎人情报平台数据显示，2026 年上半年捕获新增猫池卡 294 万例，较 2025 年下半年环比增长 110.55%。

经威胁猎人情报专家分析，出现这一趋势的主要原因是：

结合黑灰产侧情况，2026 年 5 月海外某头部接码平台集中上线了一批猫池卡，短期内显著扩大了可用卡源供给，使大量新增号码进入接码流通链路并在平台被捕获。观察该平台，呈现每年规律性批量放卡特征，并非偶发性异常批量放卡，反映非中国大陆地区黑产供给侧较为稳定。

（2）2026 年上半年非中国大陆地区新增猫池卡归属地 TOP3：美国、加拿大、沙特阿拉伯

威胁猎人情报数据统计显示，2026 年上半年非中国大陆地区新增猫池卡归属地主要集中在美国、加拿大、沙特阿拉伯。

1.2 2026 年上半年风险 IP 资源分析

1.2.1 2026 年上半年日均活跃风险 IP 总量较 2025 年下半年环比下降 16.31%

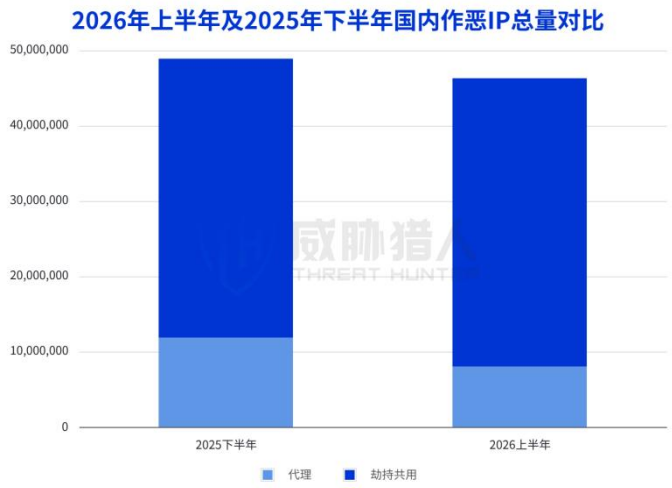
2026 年上半年，威胁猎人监测发现日均活跃风险 IP 数量持续下降，风险 IP 数量达到 1165 万，较 2025 年下半年下降 16.31%。

经威胁猎人情报专家分析，出现这一趋势的主要原因是：

2026 年上半年海外作恶 IP 数量下降，与全球住宅代理网络及海外代理平台基础设施遭到集中打击有关。2026 年 1 月，某头部全球大型住宅代理网络平台关闭了数十个用于控制设备和代理流量的域名，部分代理节点失效，代理服务可用性下降，黑灰产可调用的代理资源受到压缩。

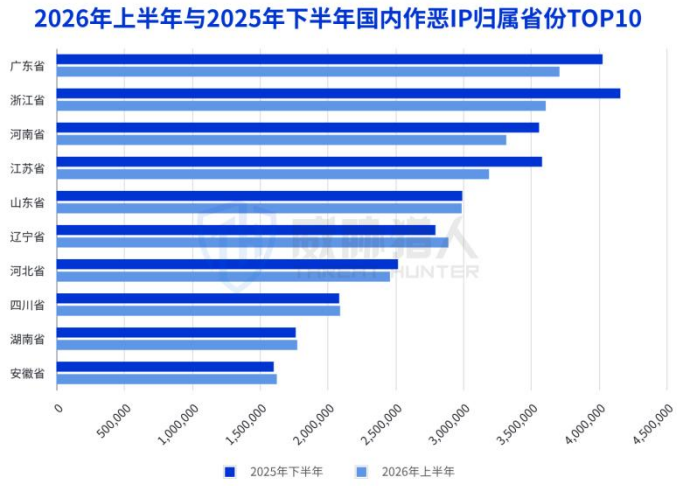
1.2.2 2026 年上半年国内作恶 IP 资源分析

（1） 2026 年上半年国内作恶 IP 有 4631 万个，环比 2025 年下半年下降 5.3%



（2）2026 年上半年国内作恶 IP 归属省份 TOP3：广东、浙江、河南

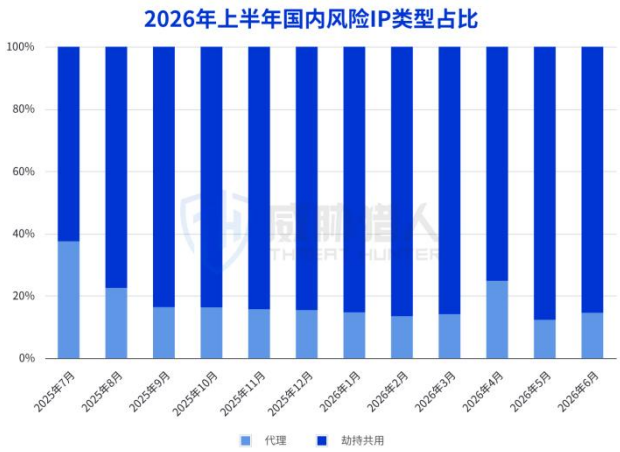
威胁猎人情报数据统计显示，2026 年上半年国内活跃的作恶 IP 归属省份（含直辖市）主要集中在广东省、浙江省和河南省。



（3）2026 年上半年“劫持共用代理”IP 攻击占总量 83.91%，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 2026 年上半年捕获数据来看，“劫持共用代理”IP 月均捕获数量达 1630 万。

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。



（4）IP 画像升级：新增静态代理 IP 覆盖能力

针对黑产利用静态代理 IP 伪造用户位置、规避风控策略并发起批量攻击的风险场景，威胁猎人 IP 画像能力新增静态代理 IP 识别覆盖。该能力通过持续沉淀静态代理 IP 资源特征与行为模式，实现对异常代理网络的精准识别与覆盖。

数据显示，静态代理 IP 月度去重覆盖规模整体保持在 40 万以上，并在 2026 年 5 月提升至 52.5 万，较 2025 年 11 月增长约 26.6%，覆盖能力持续增强。该能力可辅助客户识别虚假注册、刷单、薅羊毛、批量登录等风险行为，提升业务风控拦截的准确性与前置识别能力。

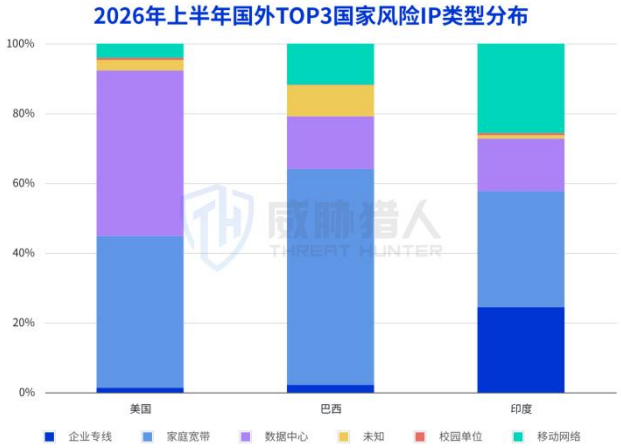
1.2.3 2026 年上半年国外作恶 IP 资源分析

（1）2026 年上半年捕获国外作恶 IP 974 万个，环比 2025 年下半年下降 16.1%

（2）2026 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，2026 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作恶 IP 类型分布存在差异，如下是国外 TOP3 国家的黑 IP 类型分布。



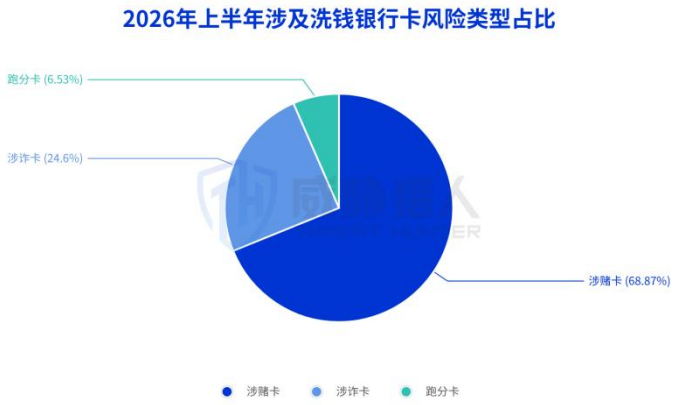
1.3 2026 年上半年网络洗钱资源分析

1.3.1 2026 年上半年洗钱银行卡资源分析

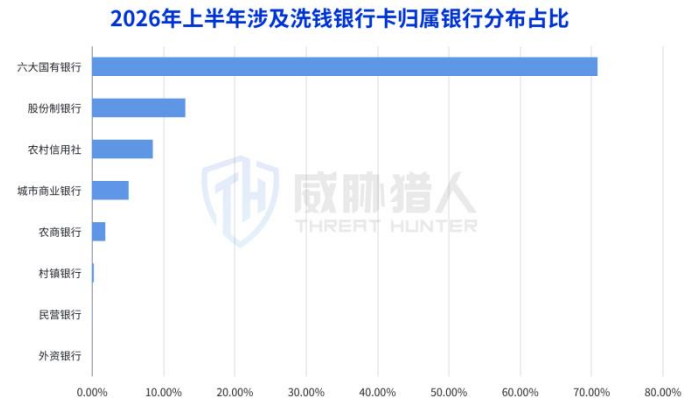
（1）2026 年上半年涉及洗钱的银行卡中，涉赌卡占比最大，占比 68.87%

威胁猎人对 2026 年上半年监控到的 8 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 68.87%。

- **涉赌卡**：黑产用于转移赌博资金的银行卡，常被用于赌博资金的收取、分流和流转。
- **涉诈卡**：黑产用于转移诈骗资金的银行卡，常被诈骗团伙用于涉诈资金的接收、分流和转移。
- **跑分卡**：黑产用于非法资金流转的银行卡，常被跑分团伙用于代收代付，转移各类非法来源资金。



（2）2026 年上半年洗钱银行卡中六大国有银行占比保持稳定，较 2025 年下半年变化不大



（3）2026 年上半年涉及洗钱的银行卡归属城市中，TOP3 城市分别是：深圳、重庆、广州

1.3.2 2026 年上半年洗钱对公账户资源分析

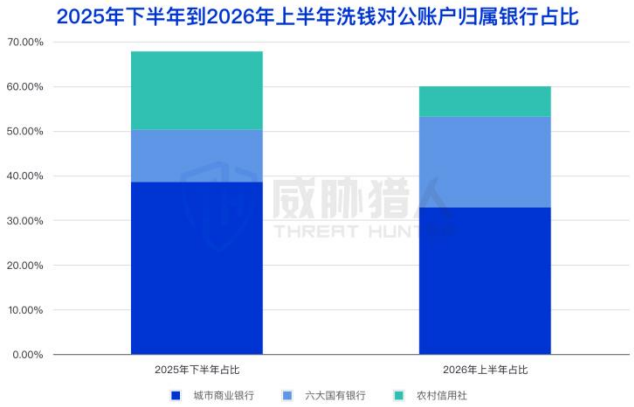
（1）2026 年上半年洗钱对公账户新增环比下降 70.81%，相关洗钱团伙减少 21.29%

2026 年上半年威胁猎人监测数据显示，用于洗钱的对公账户新增数量较 2025 年下半年下降 70.81%，相关洗钱团伙数量同步减少 21.29%。整体来看，对公洗钱活动规模和组织化程度均明显收缩。

威胁猎人分析发现：主要原因是黑产资金通道连续受挫：2025 年 5 月“好旺”、2026 年 1 月“土豆担保”先后被连续打击，黑产资金流转渠道被反复切断；同时担保体系频繁出问题，黑产内部信任下降，协作受阻，进一步压缩了洗钱活动空间。

（2）2026 年上半年洗钱对公账户所属银行中，呈现从农村信用社转向六大国有银行的趋势

2026 年上半年威胁猎人监测数据显示，洗钱对公账户的银行分布发生明显变化：农村信用社占比由 2025 年下半年的 17.55%下降至 6.78%；六大国有银行占比则由 11.66%上升至 20.34%。整体来看，洗钱对公账户出现从农村信用社向六大国有银行转移的趋势。



（3）2026 年洗钱对公账户归属省份中，TOP3 省份是广东、江苏、浙江

（4）2026 年洗钱对公账户归属城市中，TOP3 城市是深圳、上海、成都

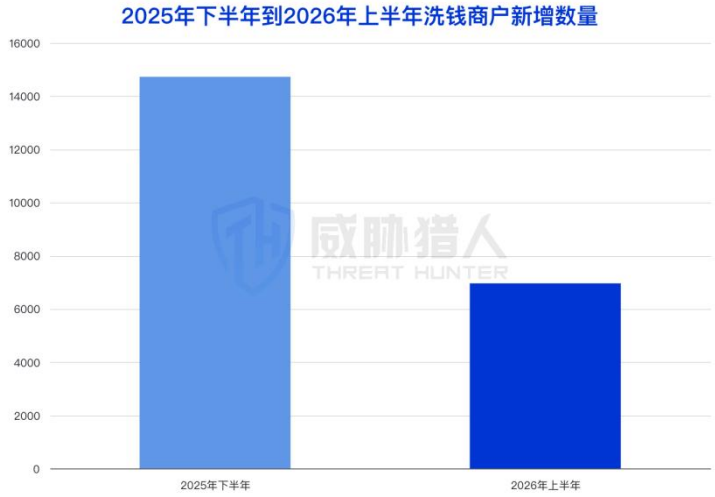
（5）2026 年洗钱对公账户归属行业中，TOP3 行业是批发业、商务服务业、零售业

1.3.3 2026 年上半年洗钱商户资源分析

“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）2026 年上半年被黑产用来洗钱的商户数量环比下降 48.23%

2026 年上半年，黑产用于洗钱的商户数量环比 2025 年下半年下降 48.23%，呈明显下降趋势。主要与上述担保类黑产通道被打击有关。



（2）2026 年上半年洗钱商户归属省份中，TOP3 省份是广东、广西、湖北

（3）2026 年上半年洗钱商户归属城市中，TOP3 城市是广州、武汉、深圳

（4）2026 年上半年洗钱商户归属行业中，TOP3 行业是零售业、批发业、餐饮业

1.3.4 2026 年上半年洗钱受害人资源分析

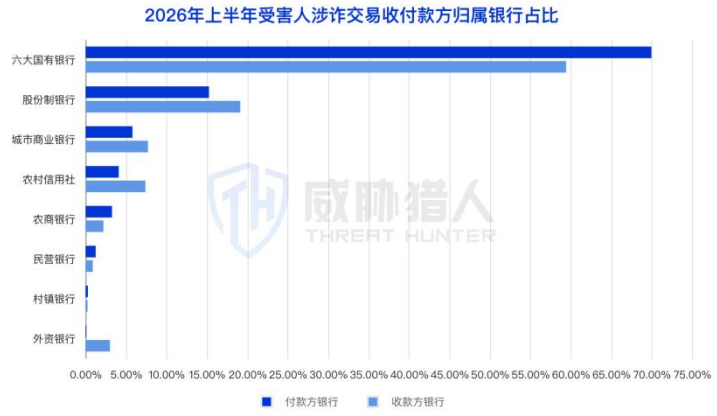
受害人涉诈交易数据：在各类匿名社交黑产群聊中，受害人被诈骗团伙实施诈骗转账的交易订单信息。威胁猎人通过自动化的方式，从各大匿名社交黑产群聊中发送的记录中，提取出受害人（付款方）、洗钱账户（收款人）和诈骗金额、时间等交易信息。

（1）2026 年上半年涉诈交易以手机银行转账为主，占比达 72.46%

威胁猎人基于上半年新增监测到的 3.5 万笔受害人涉诈交易数据分析，手机银行转账在诈骗资金流转环节中占据主导地位，占全部涉诈交易的 72.46%，是黑产引导受害人完成资金转出的主要渠道。

（2）2026 年上半年涉诈交易中，资金转出方与黑产收款方银行均高度集中于六大国有银行

威胁猎人监测涉诈交易数据显示，受害人资金转出银行中，六大国有银行占比达 69.97%；黑产洗钱收款银行中，六大国有银行占比达 59.43%。数据显示，涉诈资金流转链路中的收付款双方银行均呈现较高集中度。

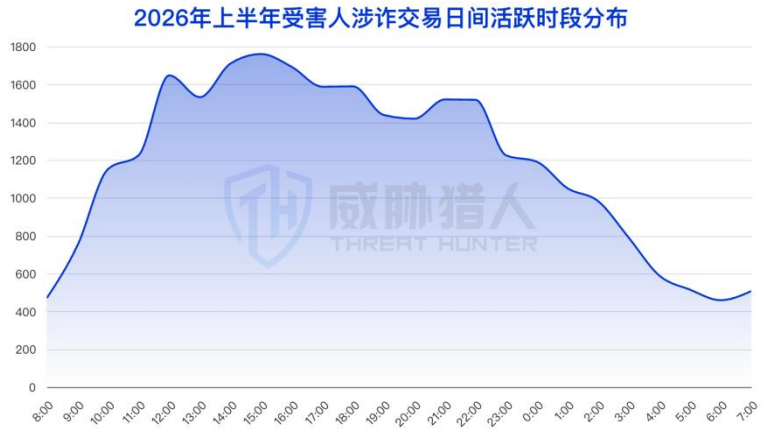


（3）2026 年上半年涉诈交易峰值集中在 14:00–16:00

威胁猎人分析发现，2026 年上半年涉诈交易时间分布呈现 2 个特征：

1. 交易高峰集中在 14:00–16:00，其中 15:00 最高（1488 笔），14:00（1440 笔）和 16:00（1446 笔）次之，形成连续高位区间。

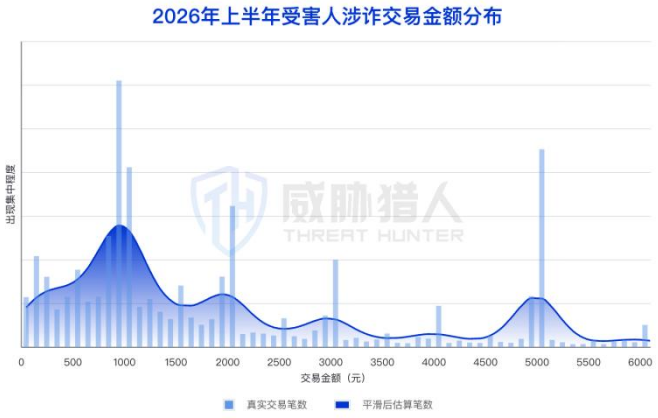
2. 整体分布上，涉诈交易自上午逐步上升（10:00 后增幅明显），午后达到峰值后回落；晚间（19:00–22:00）仍保持相对较高水平，凌晨至清晨（0:00–7:00）为低谷。整体分布与国内人员作息时间基本一致。



（4）2026 年上半年涉诈转账金额集中于千元整数档，1000 元和 5000 元最明显

威胁猎人对涉诈交易金额分布分析发现，受害人涉诈转账金额并非随机分布，而是在多个整数金额区间出现明显聚集，主要集中在约 1000 元、2000 元、3000 元、4000 元和 5000 元附近。

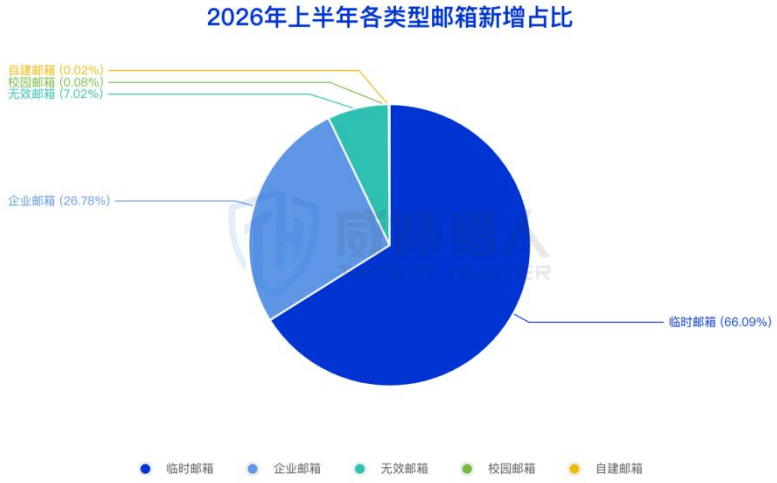
其中，1000 元和 5000 元附近的交易数量更为突出，表明黑产在引导受害人转账时，倾向于围绕特定金额区间进行操作，部分金额档位可能已成为涉诈资金转移中的常见额度。

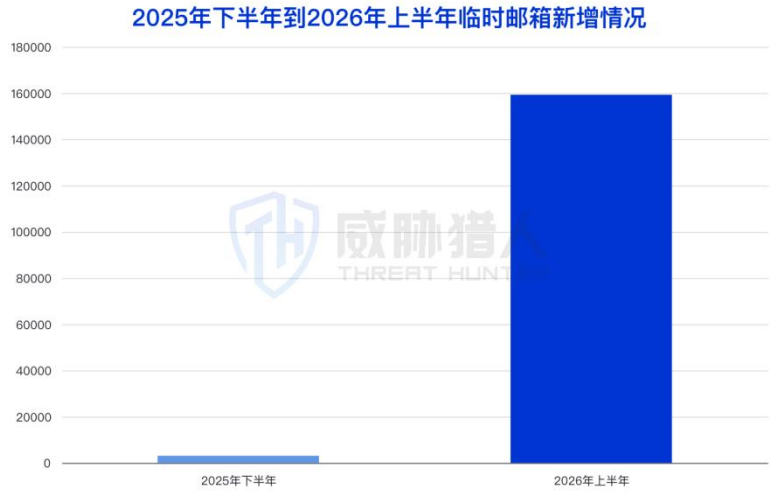


1.4 2026 年上半年风险邮箱资源分析

1.4.1 2026 年上半年临时邮箱域名占比达 66.09%，新增规模较 25 年下半年增长 50 倍

威胁猎人在 2026 年上半年新增临时邮箱域名 15.92 万个，占新增邮箱域名总量的 66.09%。较 2025 年下半年，新增规模增长约 50 倍。增长主要来源于全球 400+主流临时邮箱服务站点，显著提升了临时邮箱识别能力。





02

2026 年上半年
黑灰产攻击场景分析

二、2026 年上半年黑灰产攻击场景分析

2.1 业务欺诈场景分析

2.1.1 2026 年上半年业务欺诈风险态势

2.1.1.1 2026 年上半年线上业务欺诈风险热度延续，风险线报量累计约 9 亿条

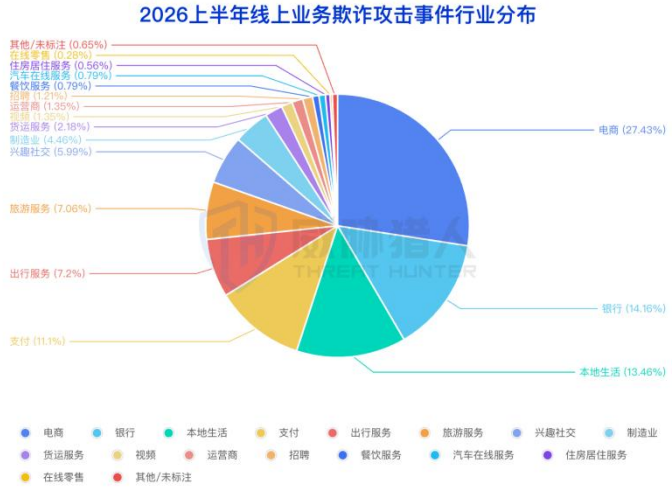
2026 年上半年，威胁猎人反欺诈情报平台累计捕获业务欺诈风险线报约 9 亿条。峰值出现在 6 月，约 2.43 亿条，占上半年超四分之一。黑产活动量本质上跟随平台营销预算的投放节奏：补贴集中投放的大促节点，就是黑产集中收割的节点。

2.1.1.2 2026 年上半年预警业务欺诈风险事件达 2088 起

上半年共预警业务欺诈风险事件 2088 起，二季度 1302 起，较一季度（786 起）增长约 65.54%。与线报量的单点冲顶不同，事件量自 4 月起连续三个月维持在 400 起以上；黑产不是在大促节点爆发一次，而是整个二季度都保持了高强度攻击

2.1.1.3 黑产攻击行业分布集中于高频交易、高补贴、高流量的互联网业务场景，电商占比居首达 27.44%

电商以 27.44% 居首；金融板块（银行 14.16% + 支付 11.10%）合计 25.26% 紧随其后；本地生活（13.46%）与出行旅游（14.26%）分列其后——四大板块合计占比 80.24%。补贴和流量在哪里，黑产就在哪里：大促补贴、营销权益、高频订单，构成上半年黑产套利的三条主要现金流入口



2.1.1.4 电商黑灰产风险情报规模跃升至 1615 万条，环比增长 83%

2026 年上半年电商风险情报量为 1615 万条，较 2025 年下半年的 883 万条增加 732 万条，环比增长 83%。

2.1.1.5 2026 年上半年捕获作恶黑产群组及论坛数量月均约 8 万个

威胁猎人反欺诈情报平台上半年月均捕获黑产作恶群组及论坛约 8 万个，6 月骤增至约 13.8 万个，接近此前月份的两倍。群组是黑产的组织动员单元，这次放量说明大促前黑产进行了有组织的临时扩编——而非存量团伙的自然活跃，节后是否回落、留存多少，是下半年值得跟踪的信号

2.1.1.6 2026 年上半年捕获作恶黑产账号数量月均约 115 万个

上半年月均捕获活跃作恶账号约 115 万个，6 月峰值约 135 万个。账号是黑产的作案耗材，对比 5 月份，其增幅远小于同时间黑产群组的扩张速度——大促节点黑产主要靠新建群聊作恶，账号池本身是长期养成的存量资产，这正是平时养号、大促集中变现数据印证。

2.1.2 2026 年上半年黑产攻击重点趋势与典型案例

2026 年上半年，业务欺诈黑灰产呈现出更强的"产业化、组织化、对抗化"特征。本章选取了几个最具代表性、且在过往报告中较少系统披露的产业趋势：品牌"回收—窜货—假货—拉踩"一体化侵权链、世界杯赛事赌博引流的"代发产业化"、快消品牌代下单产业链，并逐一拆解其产业结构、规模演进与作案链路，并附实捕案例。

2.1.2.1 品牌"回收—窜货—假货—拉踩"一体化黑产链

1. 趋势判断

威胁猎人监测发现，2026 年上半年，针对母婴保健、服饰等高客单价、强渠道管控品类的品牌侵权，已不再局限于零散的假货或窜货，而是逐步形成“正品回收—低价窜货—假货混售—竞品拉踩”的一体化链路，并辅以黄牛代下、优惠套利等手段。

这类风险同时影响品牌的渠道价格、产品口碑和知识产权，已由单点侵权演变为系统性的品牌经营风险。以某母婴保健品牌为例，可以较完整地还原该链路的运作方式。

2. 产业链拆解

针对某母婴品牌（高客单价、强渠道管控品类）的侵权，已从零散的假货、窜货，演化为"回收—窜货—假货—拉踩"四段协同、长期稳定运转的一体化产业链：

上游回收正品。黑产长期在社交平台和二手交易平台发布“高价回收”信息，明确标注回收价格、起收数量及联系方式，并在多地设置收货点和集散仓。回收的正品集中汇集后，持续流入非授权销售渠道。

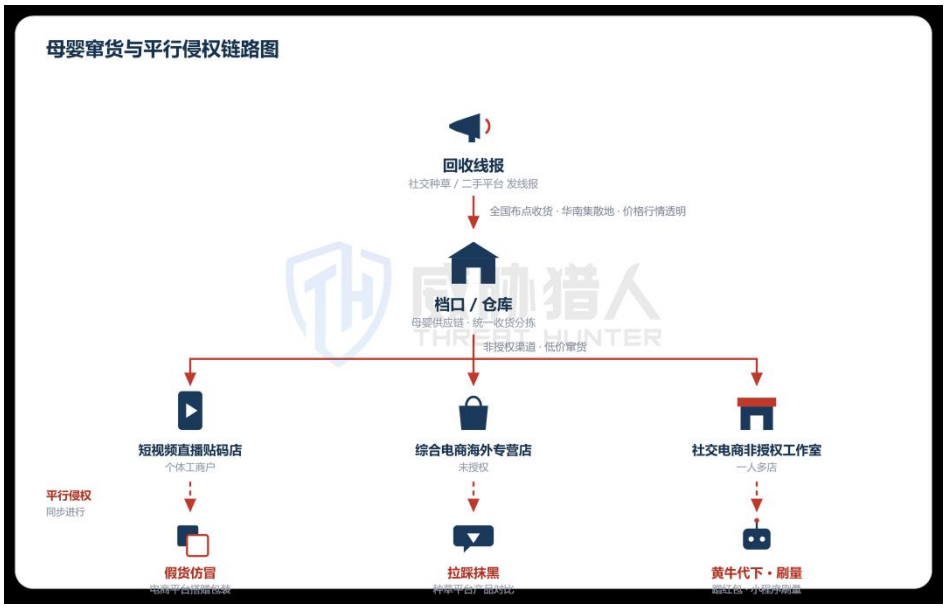
中游低价窜货。回收商品主要通过抖音直播间、综合电商平台新开店铺及社交电商“工作室”等非授权渠道销售。部分商家通过商品贴码、同一主体注册多家店铺等方式规避品牌核查，并以明显低于官方渠道的价格销售，冲击品牌正常价格体系。

下游假货混售与仿冒。部分非授权渠道存在正品与假货、高仿品混售的风险，消费者评价中出现“产品质量与官方自营不同”“使用后出现不适”等真伪质疑。同时，部分第三方商家通过模仿产品名称、包装和视觉设计，搭蹭品牌知名度与流量。

内容拉踩引流。部分账号以产品测评、竞品对比等形式，持续发布贬低该品牌的内容，并将消费者引导至其推广的其他品牌或非授权商品，进一步影响品牌口碑和购买决策。

此外，黑产还通过领取直播间红包、叠加平台优惠券和黄牛代下等方式进行套利，进一步扩大低价商品的流通规模。

整体来看，各环节之间呈现出较强的协同特征：上游负责回收和组织货源，中游通过非授权渠道低价变现，下游掺杂假货扩大获利空间，同时借助内容拉踩和黄牛套利获取流量、压低成本，最终对品牌价格体系、消费者信任和知识产权形成持续侵蚀。



3. 作恶链路分析

以威胁猎人监测到的某一品牌为例，2026 年上半年，威胁猎人在种草平台、二手交易平台等渠道持续发现该品牌的回收信息。相关信息普遍公开标注回收价格、起收数量和联系方式，收货地址高度集中于深圳龙岗布吉，部分回收方自称拥有固定档口并长期收货。

威胁猎人通过持续监测与历史情报关联发现，6 月捕获的一条回收信息，其收货人与地址与 3 月发现的黑产信息高度重合；7 月再次出现的另一名收货人，也与 2 月实际交易过的回收方一致。说明相关团伙并非短期零散作案，而是在持续运营稳定的回收网络。

以下是案例相关情况：

非授权渠道低价窜货。黑产在头部综合电商平台开设多家“海外专营”店铺，相关店铺均于 2026 年 4 月至 5 月新开，经品牌官方核查均未获得授权。6 月，威胁猎人研究人员实测发现，部分商品叠加优惠券后的到手价低至约 77.66 元/罐。与此同时，威胁猎人还分别于 1 月和 5 月发现多个抖音母婴直播账号以“贴码”方式销售该品牌商品，相关发货店铺多为个体工商户，其营业执照及法人信息均已完成取证。

恶意仿冒。3 月 20 日，威胁猎人在社交电商平台发现一款高仿商品，其产品名称、包装设计与该品牌正品高度相似。当消费者询问两者区别时，客服刻意回避相关问题。目前，仿冒店铺的经营主体及营业执照信息已完成取证。

竞品拉踩。自 2025 年 1 月起，部分账号持续发布该品牌与两款竞品的对比内容，相关话术、内容结构和发布节奏高度一致。其主要通过对比产品成分含量等方式贬低该品牌，并引导消费者转向其他品牌，具有较明显的组织化营销特征。

黄牛优惠套利。2026 年 2 月至 3 月，威胁猎人连续发现部分微信群发布该品牌商品的黄牛代下任务。可通过叠加直播间红包、平台优惠券等方式降低购买成本，部分订单甚至实现“0 元购”，随后可能进入转售或其他非授权流通渠道。

风险研判：该链条同时冲击品牌价格体系、产品口碑和知识产权。非授权低价销售扰乱渠道价格，假货混售损害消费者信任，仿冒包装则进一步放大品牌侵权风险。由于相关主体多为真实在营个体工商户，具有较强隐蔽性，治理应重点围绕回收集散地、非授权店铺和仿冒商品链接开展持续监测与联动处置。

2.1.2.2 世界杯黑产专题：体育赛事赌博引流的"代发产业化"

1. 趋势判断

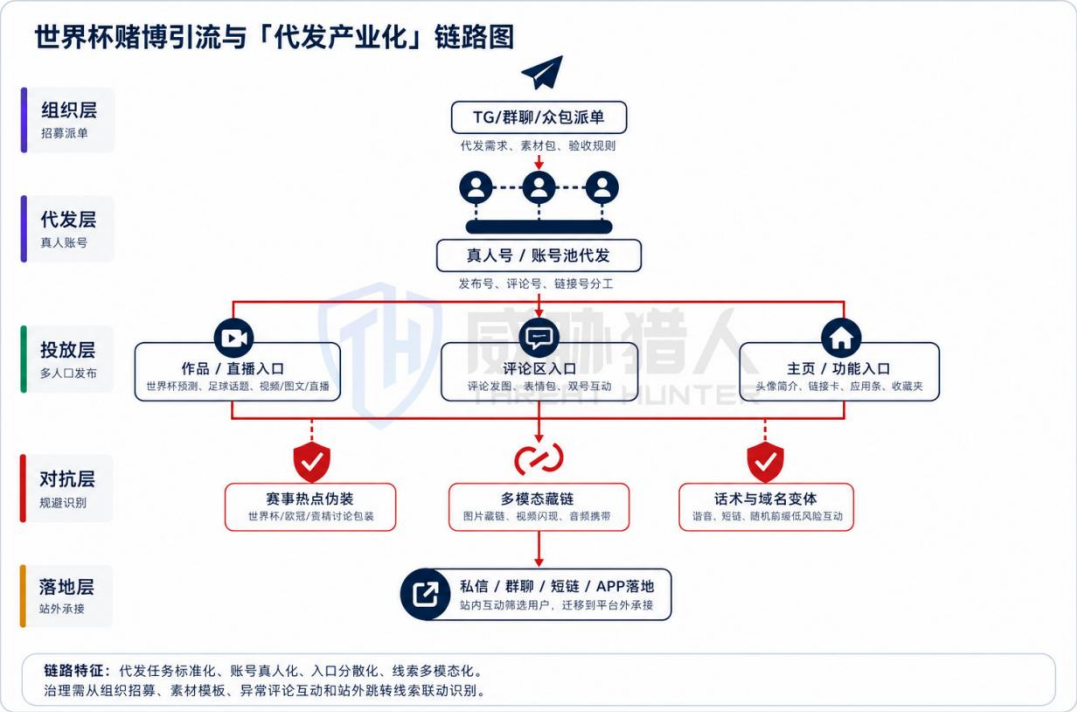
2026 年世界杯催生了一轮体育赛事相关黑产爆发，其核心是赌博（及色情）引流的"代发产业化"——黑产不再自建账号引流，而是通过押金制公群规模化招募真实用户的账号进行"代发"，借真人账号的活跃度规避平台风控，在各类短视频社交平台的体育内容下完成涉赌引流，形成"组织招募—真人代发—对抗风控—落地赌博—跑分洗钱"的完整链条。规模与演进：相关事件上半年达 130+ 起，呈现极强的赛事时效性——随世界杯临近月度陡增

2. 产业链拆解

- **组织层：** 黑产通过 TG/群聊/众包渠道发布代发任务，将赌博引流需求拆解为标准化任务包，任务包通常包含代发素材、入口要求、账号要求、发布位置、截图回传及验收规则。
- **代发层：** 通过真人号、小号、他人号或账号池承接代发任务，形成发布号、评论号、链接号等角色分工。相比黑产自营账号，真人账号具备更强的自然活跃特征，可降低单点账号被识别和封禁的风险。
- **投放层：** 代发内容不再集中于单一入口，而是分散投放至作品/直播、评论区、主页资料及平台功能入口等场景。例如以世界杯预测、足球话题、视频/图文/直播作为内容外壳，在评论区发布图片或表情包，或通过头像简介、链接卡、应用条、收藏夹等入口承载引流线索。
- **对抗层：** 黑产通过“赛事热点伪装 + 多模态藏链 + 话术/域名变体”规避识别。一方面将跳转线索隐藏在图片、视频闪现、音频或主页资料中，并配合谐音、短链、随机前缀、低风险互动话术等方式降低关键词和正则命中（域名如 sm84.my、sw33.me、7sx.my、22xx.me 等）。另一方面评论区采用"双簧+域名拆分"——A 号晒盈利、B 号追问，A 号再把域名拆成两段分别回复以规避正则检测。

- **落地层**： 站内内容主要承担筛选和触达作用，后续通过评论互动、私信、群聊、短链或 APP/网站完成站外承接，形成“站内种草/互动筛选 - 站外转化承接”的赌博引流链路。

- **作案链路：**



3. 作恶链路分析

- 评论代发 + 双簧拆域名：

6 月 9 日，威胁猎人在境外某群组中发现评论代发招募信息。黑产组织真人账号在世界杯相关视频评论区进行“双号配合”：A 账号先发布“我先买了，西班牙冠军 3k”等带有投注暗示的评论，B 账号随后追问“哪里买的”，A 账号再将域名“2**7.tw”拆分为“2**7.”和“tw”两次回复，以规避平台对完整域名和敏感内容的检测。招募信息中还附有多条指定快手视频链接，说明该类引流具有明确的任务分发和定向执行特征。

次日，威胁猎人再次捕获采用相同手法的案例，相关人员将域名“4**.vin”拆分发布，并在快手评论区完成实际投放。整体形成了“群组招募—任务分发—真人评论—双号互动—域名拆分—站外赌博引流”的作恶链路。

风险研判：该手法将真人代发、双号互动和域名拆分结合，使恶意评论更接近正常用户交流，传统关键词和正则检测容易出现漏判。平台应重点识别异常评论互动关系、连续回复中的域名片段、重复话术和账号协同行为，并结合世界杯等重大赛事节点提前布设风险策略。

2.1.2.3 快消品牌代下产业链剖析

1. 产业链概述：从单点薅羊毛到工厂化"代下单"平台

快餐、咖啡、新茶饮等品牌的数字化增长，普遍依赖新人赠礼、储值返利、会员折扣、订阅卡和社群优惠券等营销活动。由于这些权益主要绑定在会员账号上，而账号注册门槛较低，逐渐催生出一条工厂化的“代下单”黑产链。

其核心模式是：黑产批量获取并运营带有储值余额、优惠券和会员权益的账号，再以低于官方原价、但高于实际成本的价格向消费者出售套餐，将品牌投入的营销补贴转化为自身收益。消费者获得了低价商品，品牌后台则显示新增会员、储值和订单增长，但实际利润和经营数据正在被持续侵蚀。

2026 年上半年，威胁猎人监测并获取到一个正在运营的多品牌代下单平台样本，较完整地还原了其技术链路、分销模式和上下游生态。

2. 四层生态：上游供应商 → 核心平台 → 代理分销 → 终端消费者

当前代下单已不再是个人零散操作，而是形成了分工明确的产业链。

- **上游供应商主要提供账号注册、接码取号、OAuth 授权代理和动态代理 IP 等基础资源。**部分供应商以正常注册的科技公司为主体，通过“卡密 + 项目”的方式对外出售账号授权和接口能力，为下游平台提供持续供给。
- **核心平台负责批量管理会员账号、同步账户余额和权益**、模拟品牌点餐系统下单、生成兑换码，并完成代理管理和订单结算，已经形成一套较为成熟的黑产系统。
- **代理分销商则通过平台后台生成套餐兑换码，再借助微信群、电商店铺等渠道向消费者销售。**消费者打开平台自建的 H5 页面，输入兑换码、选择门店并完成下单，多数消费者并不知道订单实际由黑产账号代为提交。

整体来看，核心平台只是产业链的中间环节，其账号、接码、IP 和授权能力均由专业化供应商提供，产业链成熟度已明显超过传统的个人薅优惠模式。

3. 攻击链路：逆向小程序 + 持账号下单 + 自动化支付

代下单平台的技术链路主要包括四个环节。

- 首先，黑产通过接码平台和账号授权服务批量注册品牌会员账号，并利用充值返利、新人活动和订阅卡等方式，将账号培养成持有余额和优惠权益的“资产账号”，再按照品牌、权益和使用场景分类管理。
- 其次，由于品牌通常不会公开下单接口，黑产会逆向分析微信或支付宝点餐小程序，获取其接口地址、请求参数和业务流程。
- 随后，平台利用持有的账号登录凭证和用户身份信息，模拟小程序客户端向品牌后端发起订单请求。由于请求使用的是真实会员账号和有效权益，品牌后台较难仅凭单笔订单判断其为机器代下。
- 最后，平台通过运行在真实手机上的自动化脚本轮询待支付订单，自动唤起支付软件完成付款，并配合动态代理 IP 切换网络出口，降低同一 IP 高频下单被识别的风险。

4. 商业模式：自建 H5 + 兑换码分销

该类平台不依赖品牌官方销售渠道，而是自建完整的交易和核销流程。

- **代理生成兑换码**：代理在后台选定套餐、点击生成，系统产出一个指向自建 H5 站点的兑换码链接。该"兑换码"是平台自造的电子提货凭证，与品牌官方券码无关，仅能在平台自有站点核销。
- **对外分销出货**：代理通过社群、电商店铺将兑换码售卖给消费者，套餐命名常嵌入营销渠道标记，伪装成"品牌活动福利"。
- **消费者核销**：打开 H5 链接 → 输入兑换码 → 选城市/门店 → 确认下单 → 获得真实取餐码 → 到店取餐。
- **盈利本质**：并非赚订单差价，而是把品牌贴钱的储值与权益资产，通过代下单低价变现为现金；平台的核心"家底"即是养号沉淀的资产规模。

5. 多品牌横向复制：一套中台可复制至多个头部快餐品牌场景

威胁猎人发现，该平台并非只针对单一品牌，而是已经形成可横向复制的多品牌代下单矩阵。相关系统部署在多台服务器及不同云服务商环境中，同一套技术和分销体系可以快速接入不同品牌的点餐场景，具备明显的规模化扩张能力。

部分品牌的代下单能力已不再局限于到店取餐，还能够支持外卖配送，意味着其攻击范围正从门店自提进一步扩展到线上配送场景。

6. 三重危害：远不止"被薅一点优惠"

- **直接财务失血：**品牌用于拉新、储值和提升复购的营销预算被系统化套现，最终需要以真实商品、门店人工和履约成本完成兑付，形成直接财务损失。
- **幽灵会员污染数据资产**：大量通过接码平台注册和批量运营的账号进入会员体系，会污染新客数量、活跃用户、复购率和储值增长等关键经营指标，使品牌难以准确判断真实用户增长和营销活动效果。
- **价格体系与品牌声誉冲击**：商品长期通过非官方渠道以明显低于原价的价格销售，也会冲击品牌价格体系和加盟商利益。消费者一旦发现低价订单来自黑产渠道，还可能进一步引发对品牌管理能力和会员安全的质疑。

7. 为什么传统风控难以拦截

- **单笔行为合规：**每一笔下单在品牌后端看都是"一个有效会员用自己的余额买了一单"，孤立看毫无破绽，问题只存在于跨账号、跨订单的关联分析；
- **风控与营销的内部博弈：**被薅的优惠从营销预算列支，营销侧看到的是增长，缺乏整改动力；
- **黑产的反侦察投入：**动态代理 + 设备分散 + 余额支付（不触发异常支付风控），系统性规避现有规则；
- **黑产具备应急响应能力**：监测中发现，平台在感知异常后会快速下线、迁移、重建资产；一次性安全评估难以捕捉，必须依托持续威胁情报监测形成发现—溯源—处置闭环。

2.1.2.4 电商业务风险场景演变

2026 年上半年，电商黑灰产呈现出明显的链路化和服务化趋势。营销权益、店铺账号、企业主体、收款账户、设备环境和售后凭证不再被单独使用，而是被拆分、组合并作为标准化服务交易。

其中，营销作弊正在向“权益账号化”演变，店铺交易正在向“经营资格一体化”演变，恶意退款则开始向“生成式 AI 辅助的证据伪造”演变。

1. 电商平台营销作弊售卖风险：优惠权益被包装为可交易、可复制的平台帐号出售

威胁猎人监测发现，电商营销作弊正在从零散的优惠券滥用，演变为围绕“带权益账号”生产、养号和交易的供应链。

黑灰产利用邮箱、接码及自动化工具批量注册账号，通过人工操作或脚本模拟浏览、搜索、收藏、加购和活动互动等正常行为，完成营销任务。帐号获得优惠券、积分或免邮权益后，再以“账号整体交付”的方式进行销售。

与直接出售优惠信息相比，这种模式能够将账号、营销权益和部分行为记录一并转移，使优惠权益脱离原始获取者，增加平台识别异常流转的难度。

（1）“带券账号”成为营销权益交易的主要载体

相关账号通常根据优惠折扣、积分余额、任务完成情况和有效期限进行差异化定价。交易完成后，卖方向买方交付账号及相关登录信息，由买方绑定支付方式并完成下单。

营销作弊的交易对象因此不再是单张优惠券，而是包含账号、营销权益和行为记录的组合资产。

该模式可能绕开部分平台对优惠券转赠和异常流转的限制，使营销权益进入可定价、可批量交易的外部市场。

（2）模拟真实行为提升营销任务通过率

为了降低批量注册账号被风控系统识别的概率，黑灰产会主动为账号补充正常用户行为轨迹，常见行为包括：

- 完成新用户引导和活动页面浏览；

- 模拟商品搜索、浏览、收藏和加购；
- 按任务要求完成签到、答题或互动。

部分团伙将这一过程称为“做卷子”或“打积分”。其核心目的，是提高批量账号与正常消费者的行为相似度，使账号更容易获得营销权益。

对平台而言，仅根据某一次浏览、签到或领券行为，通常难以识别此类风险。治理重点需要转向注册资源、设备复用、行为节奏、账号关系和权益使用路径的综合分析。

2. 电商平台店铺账号售卖风险：从单一账号交易向“企业主体—店铺—收款—售后”一体化服务演化

电商店铺交易已经不再局限于账号和密码，而是逐步形成覆盖身份协作、企业注册、店铺开设、收款配置、环境迁移和持续身份验证的一体化服务链。

黑灰产交易的对象不再只是登录权限，而是一个能够通过审核、接收货款并持续经营的“经营资格包”。其主要特征是名义登记主体、实际控制人和实际经营者可能相互分离。

（1）名义主体与实际控制人分离

部分服务商通过有偿方式招募自然人提供身份及税务资料，并配合企业注册、银行开户和后续身份验证。店铺完成注册后，实际经营权和控制权可能被转移给其他主体。

随后，中介或服务商负责完成企业注册、税务登记、银行账户配置和电商平台入驻，将相关资料组合为具备本地经营外观的店铺资产。

店铺交易时通常可能包含：

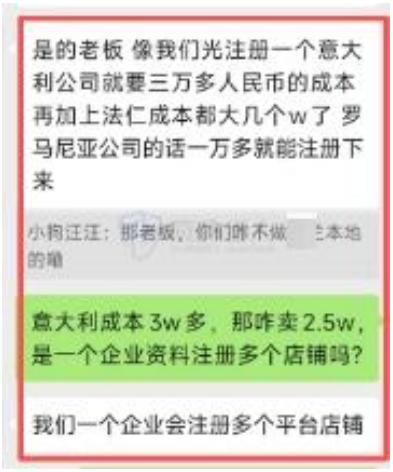
- 店铺账号及登录权限；
- 企业和税务登记资料；
- 企业收款账户；
- 浏览器会话及相关环境信息；
- 后续身份验证和资料补充服务。

（2）“一企多店”提高同一套资质的变现效率

服务商可能利用同一企业主体、登记人员和税务资料，在多个电商场景申请店铺，并将不同店铺分别出售或投入经营。

这种“企业主体复用、店铺拆分销售、多场景变现”的模式，能够分摊企业注册和维护成本，使同一套主体资质被重复利用。

即使单个店铺的交易价格无法覆盖全部注册成本，服务商仍可能通过出售多个店铺实现成本回收和利润放大。

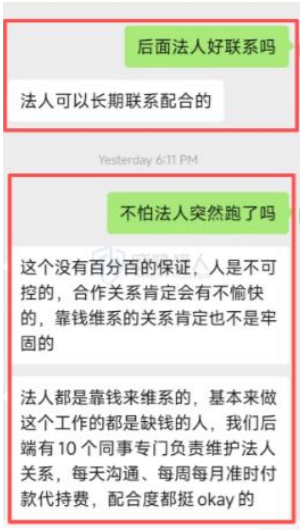


（3）持续身份验证被包装为售后服务，保证帐号存活

店铺出售后，原登记人员可能不会完全退出，而是继续作为账号维护资源，配合视频认证、身份复核、资料补充和账号申诉。

相关服务可能按照单次、按周或按月收费，使自然人的身份配合能力成为可以持续购买的资源。

这意味着，平台在经营过程中再次发起真人验证，也未必能够识别店铺控制权已经转移。身份验证正在从一次性的准入机制，被黑灰产转化为可按需调用的售后服务。



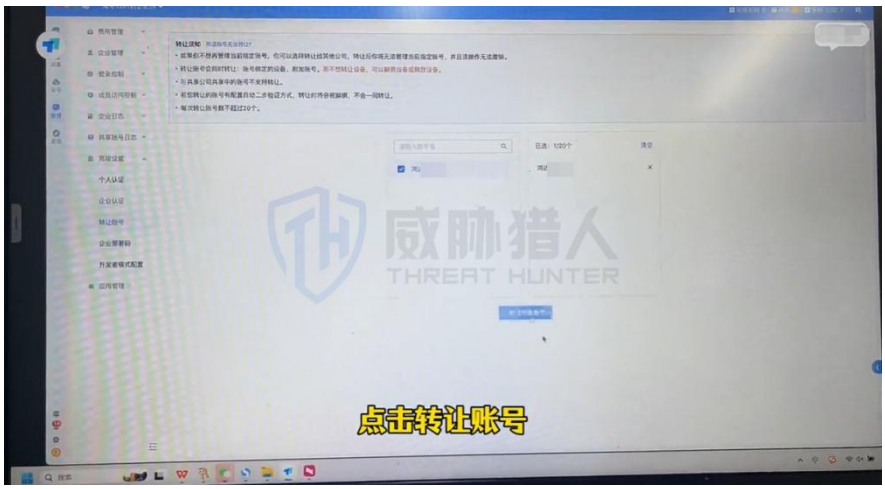
（4）指纹浏览器迁移降低账号交付过程中的异常暴露

部分账号服务商会同步转移浏览器会话、设备指纹、Cookie 及网络环境，使买方能够在接近原有经营环境的状态下接管店铺。

买方完成购买后，服务商通过浏览器内置的 账号迁移 功能，将店铺会话、浏览器指纹及 IP 环境同步至买方。买方无需在新的环境中重新输入账号密码，即可直接接管店铺。

这一交付方式能够降低传统账号买卖中常见的异地登录、设备突变、Cookie 失效及 IP 变化等异常特征，使账号控制权转移在平台侧表现为原有经营环境的延续。

平台需要重点识别环境迁移后的细微变化，包括操作时区、输入习惯、访问节奏、收货关系、商品变化和资金流向，而不能只依赖 IP 或设备是否发生突变。



3. 生成式 AI 推动售后欺诈向证据伪造演化

威胁猎人监测发现，当前电商平台恶意退款欺诈已不再仅依赖客服话术、物流漏洞和规则施压，而是引入 AI 生成图片等能力，将虚假的商品破损、设备故障和异常状态包装为可提交、可验证、可推动售后流程的“证据材料”。

黑灰产通过 AI 生成破损、故障图片及客诉凭证，配合退货标签诱导、调查周期拖延、监管投诉施压等传统恶退手法，形成“虚假证据生成、售后流程触发、客服规则博弈、退款结果兑现”的作弊链条。

该模式降低了恶意退款对真实商品状态、真实拍摄环境和真实物流异常的依赖，使售后风险从单一的规则滥用，进一步演化为 AI 辅助下的证据型欺诈。

（1）AI 生成图片成为恶意退款的关键凭证

在针对某电商平台相关黑产交流的监测中发现，黑灰产可能根据商品品类、退款理由和售后审核要求，生成具有破损、变形、泄漏或污染特征的图片，以增强客诉材料的表面可信度。比如：有

黑产使用 AI 生成“iPhone 锂电池泄漏”等商品异常图片，向平台提交售后申请，并最终实现无需退货的退款结果。

（2）AI 作弊与传统恶退链路结合，放大售后风控压力

疑似 AI 生成内容通常不会单独发挥作用，而是与虚假客诉理由、物流标签规避、调查周期拖延、重复申诉和投诉施压等方式结合使用。

在这一链路中，生成内容主要用于补充“证据材料”，传统话术和流程操作则用于推动售后处理。相关人员可能通过反复沟通和申诉延长处理周期，增加平台客服和风控团队的核验成本。

2.2 品牌外部风险场景分析

2.2.1 品牌外部风险全景

企业外部风险并非只集中于某一个仿冒页面或某一次数据泄露事件。数据和身份可能在企业控制范围之外持续流通，用户触点也可能分散在搜索、内容、社交、下载和私域渠道之中。品牌保护

面对的核心问题，正在从“是否存在假冒资产”扩展为“企业与用户之间的可信连接是否仍然可识别、可控制”。

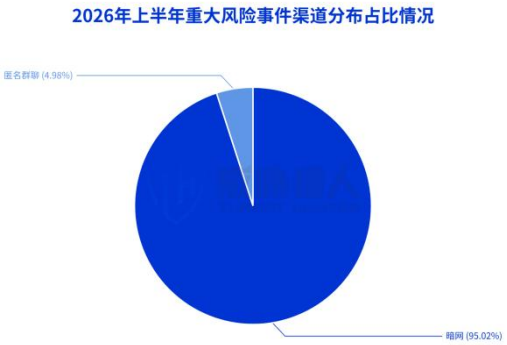
2.2.1.1 品牌保护围绕四类对象展开

保护对象	主要外部风险	典型影响
品牌身份	企业名称、产品名称、标识、域名、应用程序和官方账号被冒用	用户难以判断服务主体，企业授权关系和品牌辨识度受损
官方渠道	搜索结果、网站、客服电话、下载入口、内容账号、活动页面和二维码被截流	用户在到达官方服务前进入虚假联系方式、非授权下载或欺诈页面
客户关系	贷款、支付、订单、会员、退款和催收等真实业务记录进入外部渠道	业务背景被还原，目标被筛选，冒充客服或催收的话术更具针对性
公共声誉	暗网披露、攻击声明、数据样本和侵权内容公开传播	客户质疑、合作伙伴审查、舆情压力和业务连续性风险上升

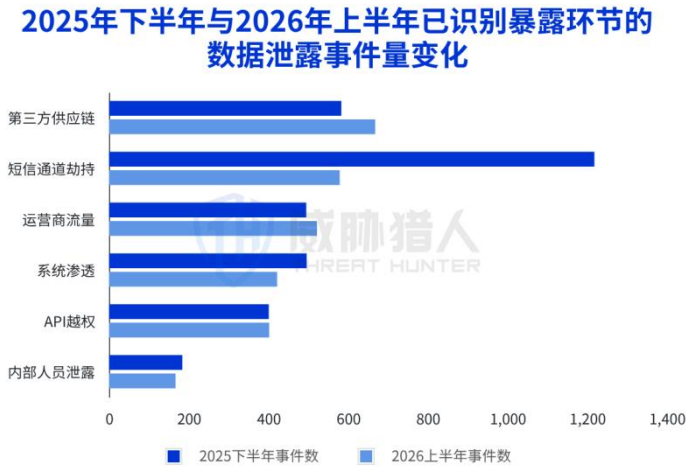
围绕上述四类保护对象，企业面临的外部风险可以概括为两类相对独立的风险面：数据、身份与权限暴露，以及品牌、渠道与流量滥用。二者既可独立发生，也可能相互叠加，共同影响客户关系、用户信任和品牌声誉。

2.2.1.2 数据与身份暴露：事件总量小幅增长，重大风险向暗网集中

2026 年 1 月至 6 月，经验证确认的有效数据泄露事件共 23,645 起，较 2025 年下半年的 22,102 起增长 6.98%。其中，暗网渠道记录由 2,353 起增至 4,952 起，增幅明显高于整体事件增幅。暗网已成为重大数据泄露风险公开披露和传播的主要外部渠道。



从已识别的风险来源看，数据泄露记录涉及第三方服务、短信通道、运营商流量、系统渗透、API 越权和内部权限等多个环节，反映出企业数据暴露面已从单一系统安全问题，延伸至供应链、通信链路和权限管理等多类外部及内部节点。



2.2.1.3 品牌与渠道滥用：用户接触风险分布在多类入口

2026 年上半年共记录钓鱼仿冒与品牌滥用风险事件 45,321 起。相关风险出现在搜索结果、仿冒网站、社交媒体、客服电话、应用程序和下载渠道等多类用户入口。

从本期风险分布看，SEO 污染记录 20,726 起，占 45,321 起主体样本的 45.73%；仿冒网站占 29.56%。搜索结果和仿冒页面仍是品牌被滥用的重要位置：前者可能在用户寻找客服电话、账户

异常处理、退款理赔、贷款办理或应用下载时截获需求，后者则可能承担信息收集、恶意下载、假客服联系或资金欺诈等承接作用。

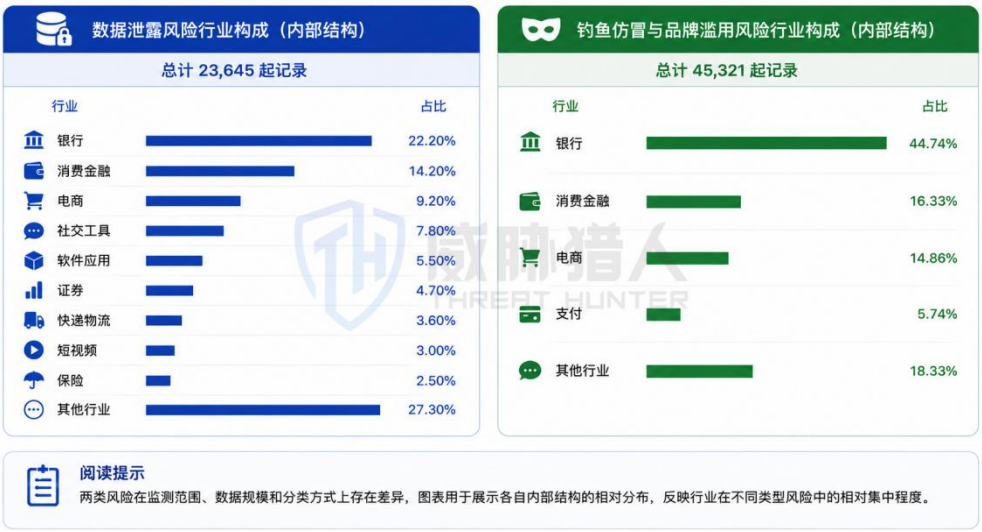
2026 年上半年，SEO 污染、仿冒网站、仿冒社交媒体、仿冒客服电话、仿冒应用、非授权下载渠道和侵权网站等多类入口在半年内并行存在。月度分布显示，多类风险入口在半年内持续并行，品牌滥用并未集中于单一渠道。

2.2.2 重点行业的品牌风险差异

2.2.2.1 行业分布：同一行业可能从不同外部位置暴露风险

2026 年上半年，金融相关行业在数据泄露风险和品牌滥用风险中均处于较高位置。在 23,645 起数据泄露事件中，银行记录 5,251 起，占 22.2%；消费金融记录 3,359 起，占 14.2%。在 45,321 起钓鱼仿冒与品牌滥用事件中，银行和消费金融分别占 44.74%和 16.33%，支付行业占 5.74%。

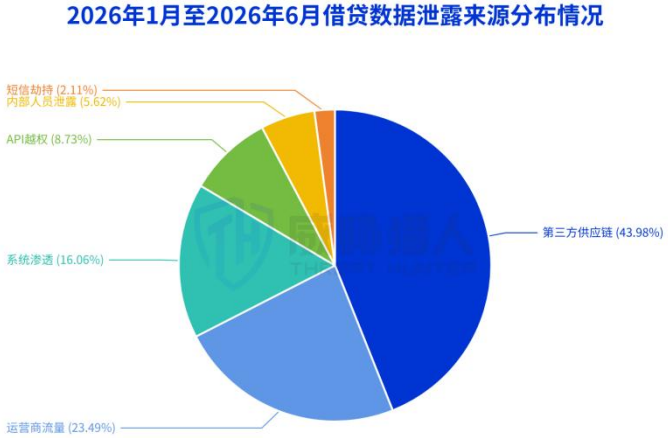
这一分布反映出，金融行业既面临客户和业务信息进入外部渠道的风险，也长期受到仿冒网站、虚假客服、搜索引流和非官方应用等身份冒用问题影响。除金融行业外，电商、社交工具、软件应用、证券、快递、短视频和保险等行业也呈现不同规模的外部暴露。



2.2.2.2 金融与借贷：业务数据暴露加剧身份冒用风险

金融与借贷业务覆盖申请、放款、支付、还款和催收等多个环节，相关数据一旦进入外部渠道，可能被用于还原客户真实业务关系，增强虚假客服、假催收及仿冒渠道的可信度。

2026 年上半年泄露的借贷数据样本中，放款料约占 64.6%，申请料约占 28.6%，风险涉及银行、消费金融、网络小贷、助贷平台等多类机构，并可能来源于第三方服务、接口权限、通信链路及内部人员等多个环节。金融机构面临的品牌风险因此不只表现为网站、客服电话和企业身份被冒用，也与客户业务信息是否脱离控制密切相关。



2.2.2.3 游戏行业：社交传播与商品侵权形成独立生态

2026 年上半年，威胁猎人专项监测到游戏行业相关风险 77,816 起，其中仿冒社交媒体 56,071 起、商品侵权 19,350 起。由于游戏行业采用独立监测对象和统计口径，相关数据不与前述风险总量直接加总或横向比较。

游戏行业风险主要集中在两类场景：一类是通过福利、兑换码和稀缺资源等内容吸引玩家进入私域渠道；另一类是围绕私服、账号交易、外挂、辅助和脚本形成的商品侵权生态。相关风险具有平台分散、内容变体多、账号重建快和商品反复上架等特点。

关于不同行业所面临的品牌保护风险，**威胁猎人将于后续发布《2026 年上半年中国企业品牌外部风险趋势报告》。**报告将围绕数据泄露、身份冒用、渠道截流和公开披露等外部风险展开分析，系统呈现品牌保护如何从处置单一仿冒资产，扩展至品牌身份、官方渠道、客户关系与公共声誉等关键对象。

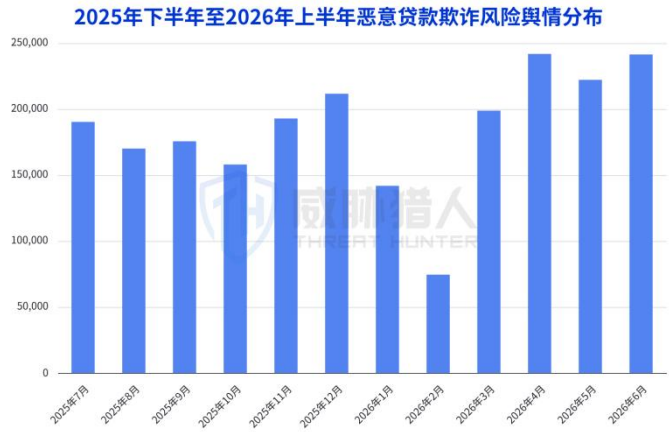
报告还将进一步拆解金融与借贷、电商、制造与零售、游戏等重点行业的风险差异，并结合典型案例，还原真实业务信息与仿冒身份、非官方渠道结合后，如何增强欺诈可信度，以及黑灰产如何借助搜索、内容平台、社交媒体、客服入口和动态二维码实施引流与身份冒用。

2.3 信贷欺诈场景分析

2.3.1 2026 年上半年金融贷款恶意欺诈舆情发展持稳，但规模有所收缩

2.3.1.1 2026 年上半年恶意贷款欺诈风险舆情较 2025 年下半年增长 2%

2026 年上半年，威胁猎人共捕获恶意贷款欺诈舆情 112 万条，月度风险舆情呈持续增长态势，较 2025 年下半年增长 2%。

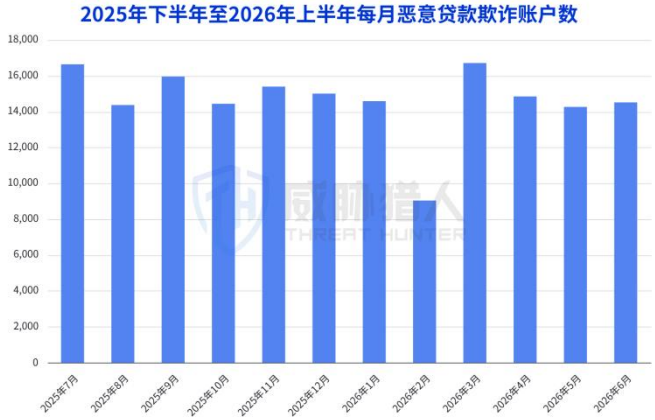


2.3.1.2 2026 年上半年恶意欺诈群组数较 2025 年下半年增长 17%

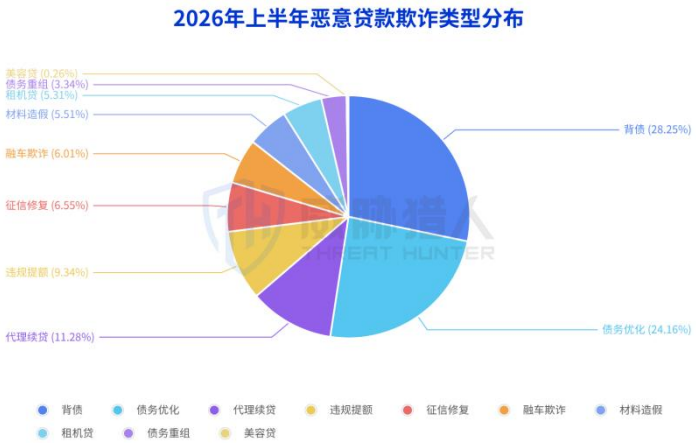
2026 年上半年威胁猎人共监控到活跃恶意欺诈群组 1.4 万个，较 2025 年下半年增长 17%

2.3.1.3 2026 年上半年恶意贷款欺诈账户数环比下降 3%

2026 年上半年，威胁猎人共监控到提供恶意贷款服务的欺诈账户（信贷黑中介/黑产）5.6 万个，较 2025 年下半年下降 3%。

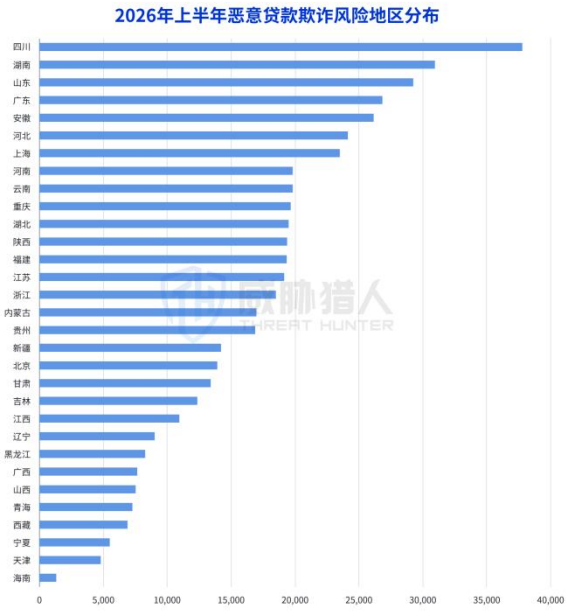


2.3.1.4 2026 年上半年恶意贷款主要欺诈类型 TOP5：职业背债、债务优化、代理续贷、违规提额、征信修复



2.3.1.5 2026 年上半年恶意贷款欺诈风险地区 TOP5：四川、湖南、山东、广东、安徽

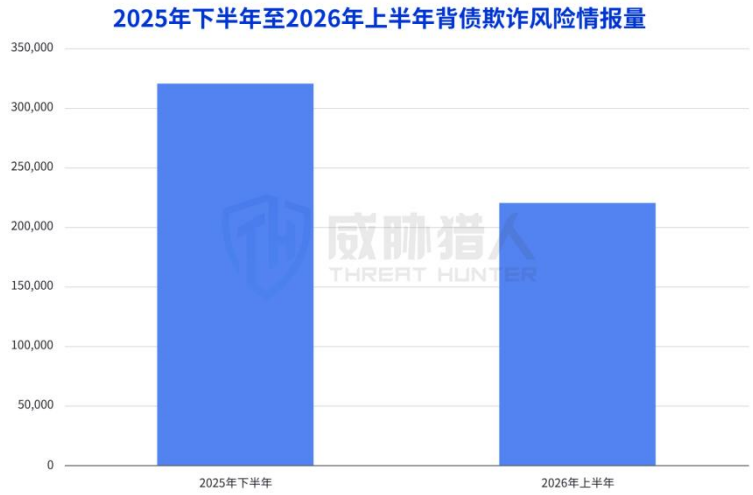
威胁猎人情报数据显示，2026 年上半年恶意贷款欺诈活跃热度 TOP5 的省份 (含直辖市) 是四川、湖南、山东、广东、安徽。



2.3.2 2026 年上半年职业背债风险有所遏制

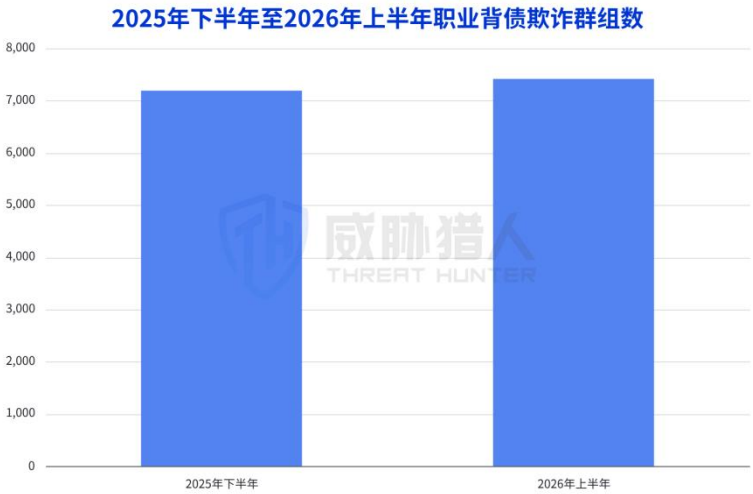
2.3.2.1 2026 年上半年职业背债风险舆情较 2025 年下半年下降 31%

2026 年上半年，威胁猎人共捕获职业背债风险舆情 22 万条。整体来看，在监管持续严打的态势下，职业背债风险得到一定遏制，上半年舆情量较 2025 年下半年下降 31%。



2.3.2.2 2026 年上半年活跃背债群组数较 2025 年下半年增长 3%

2026 年上半年监测数据显示，活跃背债群组数量超 7400 个，较 2025 年下半年小幅增长 3%，黑产线上聚集态势依然活跃。



2.3.2.3 2026 年上半年背债服务账户数较 2025 年下半年下降 31%

2026 年上半年，活跃背债服务账户数超 1.3 万个，较 2025 年下半年下降 31%，表明黑产服务端活跃度有所收缩。

2.3.2.4 2026 年上半年背债地区热度 TOP5 省份：四川、重庆、广东、山东、河南

威胁猎人情报数据显示，2026 年上半年背债相关的贷款欺诈，活跃热度 TOP5 的省份（含直辖市）是四川、重庆、广东、山东、河南。

2.3.2.5 高压之下背债黑产的生存现状

职业背债产业链已高度组织化、规模化，并呈现跨地域化、技术化与产业化并存特征。近年来，该产业链引发的金融不良资产持续攀升，已成为威胁金融稳定的重要风险源。

2026 年上半年，监管持续加码、刑事震慑力不断增强，在监管与风控政策收紧双重挤压下，黑产作恶通过率明显受限，整体利润大幅下滑，生存空间显著收窄。批量黑产团伙被依法捣毁，业内出现“各地经侦关押场所中挤满了金融从业者”的说法。

在强监管环境下，背债黑产的生存现状主要呈现以下三个方面：

- **黑产主体加速出清**

强监管背景下，相当一部分黑产团伙因当前业务或历史作恶行为被查处。近一年来，各地经侦部门查办的金融犯罪案件中，涉及背债、AB 贷、融车套现、包装骗贷、债务重组、科技提额、伪造材料商等金融黑产从业人员的比例明显上升，监管与刑事执法的组合拳，正在加速清洗行业中的低端、高风险参与者。

- **被迫转型或退出**

在刑事震慑力与银行等金融机构信贷政策持续收紧双重夹击下，大量黑产面临“无单可做、无利可图”的困境，不少黑产月收入归零成为常态，越来越多的黑产从业者开始主动或被动转型、退出行业，部分黑产甚至转向其他灰产领域以求生存。

- **自我迭代、伺机牟利**

尽管高压态势持续，仍有大量黑产人员继续活跃于背债贷款欺诈业务，呈现出明显的分层分化：

- **守旧派：**部分黑产抱有侥幸心理，延续传统的粗暴式欺诈手法（如纯虚假材料包装）、或铤而走险攻击高风险业务场景，试图以“量大面广”的方式继续作恶。这类黑产面对的是“露头即打”的局面，生存空间日益收窄。
- **迭代派：**相当一部分黑产群体已意识到传统手法难以为继，主动加速技术升级与模式迭代，转向精细化、高仿真的欺诈手法，以真实补缴、长周期数据养护、技术+关系复合攻击等方式突破风控防线。这批黑产具备更强的组织能力与技术储备，是当前威胁最大的群体，也是下一阶段防御的重点。

总体来看，高压之下，背债黑产正经历一轮深度的洗牌与重塑。低端参与者被加速出清，但留存下来的黑产团伙手段更精细、更隐蔽，会持续衍生出新的欺诈手法，攻防博弈仍在持续升级。

2.3.3 各贷款场景风险及变化

在当前严打整治环境下，2026 年上半年房贷、消费贷、企业贷、车贷等主要贷款场景的风险舆情较 2025 年下半年整体有所回落，黑产活动面临一定阻力。但面对多重压力，黑产在各场景中的欺诈手法与表现亦呈现差异化演变，具体如下：

贷款场景	欺诈类型	核心态势与变化
房贷	• 融房套现 • 房信企车组合背债 • 开发商假按揭	高评高贷受限，利润空间收窄，黑产转向差价空间较大的“不良”房源； 客户资质门槛提高，可操作资源持续收缩
消费贷	• 包装骗贷(背债) • 债务重组 • AB贷	包装骗贷中“真实补缴”成为主流 债务重组因风险暴露，黑产开展职能切割以规避追责 客户资质整体下滑背景下，AB贷猖獗，多地已掀起专项打击浪潮
企业贷	• 职业背债 • 科技提额 • 码牌增量 • 经营贷款诈 • 材料包装	开票经济环境下黑产主动避险，转向商户端实施码牌增量欺诈 利用区域性政策差异及银行间口径不一致，开展针对性攻击 欺诈模式以真实经营+“真实数据”或辅助包装为主
车贷	• 融车套现 • 顶名车 • 传销购车 • 套路运	目标车型集中于高保值率热门车型，以保障套现空间及流转效率 变现折损率高、风险暴露快，部分黑产被迫转型

2026 年上半年，信贷欺诈风险呈现出跨场景蔓延、专业化升级、产业化运作的显著特征，职业背债、房贷、企业贷、消费贷等领域手法不断翻新、变体层出不穷，整体防控形势依然严峻复杂。

威胁猎人将于后续发布《2026 年上半年信贷欺诈风险趋势报告》。进一步分析信贷欺诈风险的变化趋势、重点场景差异及典型攻击链路。

本报告由反欺诈情报研究团队基于长期监测数据、真实风险样本与行业治理实践编写。黑灰产对抗没有终点，黑产攻击手法会持续演变，黑产攻击技术也会继续迭代。面对不断变化的黑灰产生态，威胁猎人将会持续和各行业企业紧密协同，共同守护企业业务安全与用户权益。

希望本报告能够帮助反欺诈、安全、风控及业务从业者更准确地理解黑灰产生态变化，识别风险迁移与手法升级，并为企业制定更具前瞻性和针对性的治理策略提供参考。

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