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年全球电商业务欺诈风险研究报告

前言

过去一年，威胁猎人基于对全球电商黑灰产情报体系的持续监测发现：2025年，黑灰产正从"单点违规、规则绕过"的低阶作恶模式，全面转向围绕平台业务系统进行持续攻击的"全生命周期、模块化、服务化"的攻击方式。

从整体规模看，2025年全球电商领域监测到的黑灰产风险线索量达**1500万条**,同比增长**226%**;共捕获黑灰产相关帐号**160万个**,同比增长**55%**,风险规模显著扩大。

从核心演化趋势来看，2025 年电商黑灰产呈现出三项具有结构性意义的变化：

AI 驱动的"证据工业化"：

随着生成式 AI 的普及，身份材料、申诉证据、物流凭证等关键物料，正从以往的人工定制，转向模板化、脚本化和规模化生成。这一变化显著提高了黑灰产在 **KYC 审核、申诉对抗及售后环节** 中的通过率。

物流作弊风险加剧：

物流作弊风险不局限于卖家用作规避运费的单一履约违规点，而是演变为同时支撑了假货倾销与恶意退款的基础物料；

攻击资源的真人化：

在平台持续强化设备与环境识别能力的背景下，黑灰产系统性引入真实人类参与作恶，**通过真实设备与真实网络环境**降低风控命中率，提升关键环节成功率。

基于上述发现，威胁猎人发布《2025 年全球电商欺诈风险研究报告》，依托覆盖多区域、多平台的海量情报数据与典型案例，从**宏观态势、全生命周期攻击路径、关键能力演化与典型风险场景**等维度，系统呈现当前电商黑灰产的发展趋势，旨在为电商平台与相关行业提供可落地的情报洞察与风控决策参考。

一、2025年全球电商平台风险整体态势

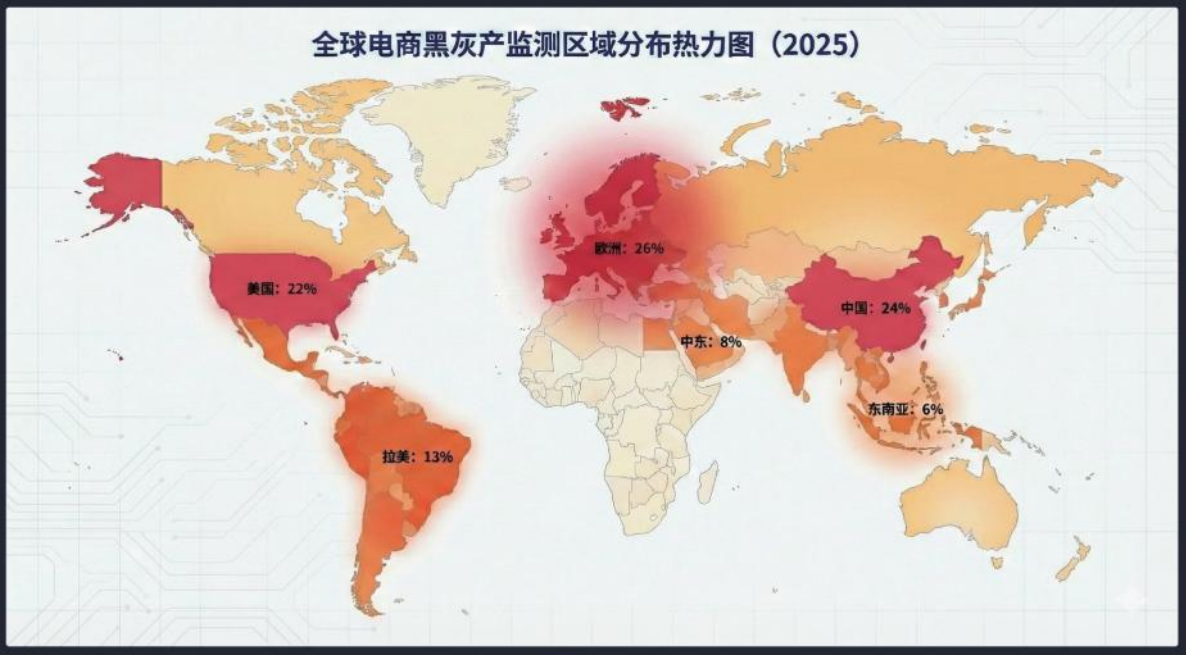
1.1、电商黑灰产风险线索规模跃升至 1500 万条，同比增226%

2025年，威胁猎人反欺诈情报平台捕获的电商黑灰产风险情报总量达 1500万条，同比增226%，捕获相关作恶黑灰产帐号 160万个，同比增55%。

2025 年，威胁猎人持续加强对**海外黑灰产活动**的监控力度以及**本地化情报源建设**，重点覆盖不同国家与地区的地下社群、交易渠道及关键活跃节点，逐步形成跨区域、多语言的情报采集与分析能力，为客户提供更具区域指向性与可研判价值的核心情报支撑。

1.2、全球电商平台攻击风险高度集中于欧洲、中国与美国

欧洲、中国及美国三大区域合计贡献了全球 70% 以上 的电商风险线索，构成当前全球电商风险的核心集中区。上述区域同时也是全球最重要的电商经济体，风险分布与业务体量高度重合，符合“黑产跟着钱走”的基本规律。



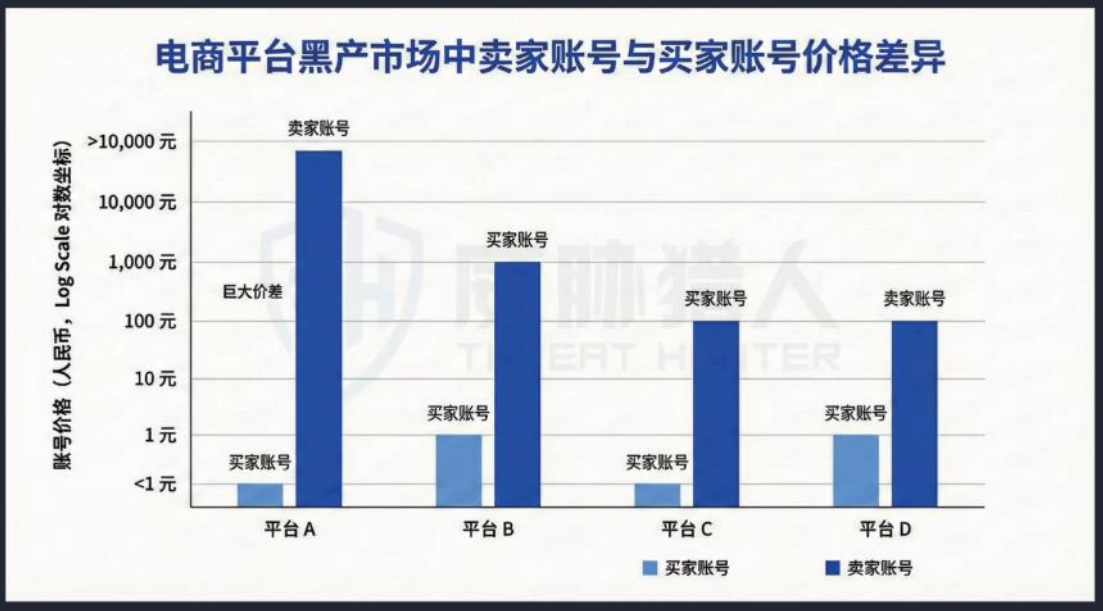
1.3、全球渠道做引流，本地化渠道做成交的黑灰产运作模式

在各重点区域，黑灰产普遍采用“全球渠道引流 + 本地化渠道成交”的双层运作模式：也就是黑产先在全球性社交平台进行扩散获客与导流，再转入本地即时通讯工具、本地论坛及区域交易平台完成私域承接、交易撮合与交付闭环。

针对这一跨平台、跨区域的运作链路，威胁猎人于本年度同步推进**本地化情报源拓展**，强化在不同区域生态内对关键渠道和活跃节点的持续获取与监测能力。

1.4、不同平台买卖双方账号定价差异明显，价格与平台门槛高度相关

无论是卖家账号还是买家账号，其在黑产市场中的定价均存在明显差异，主要受平台所在地区、商家等级体系及账号所具备的经营权限影响。 从本质上看，账号价格反映的是黑产对平台账号准入成本与风控强度的反向评估：地区属性、等级体系和经营权限越稀缺，平台风控门槛越高，对应账号在黑产市场中的定价也越高。



1.5、全球电商黑灰产攻击呈现显著的跨区域攻击特征

全球黑灰产活动呈现出显著的跨区域、网络化特征。

相关犯罪团伙已不再局限于单一国家或地区，而是充分利用互联网的无国界属性，在A国家完成信息收集、技术研发，然后在B国家攻击实施及资金变现等环节，形成分工明确、协同运作的黑产链条，并持续将攻击目标指向全球重点市场。

举例：威胁猎人监测发现，在黑灰产群组中有缅甸黑产人员宣称“通过该方法可每日稳定获取积分，只需按步骤操作即可完成”。结合其发布的配图可见，所涉 App 界面为日文环境，表明相关黑灰产正在跨区域参与日本地区 App 的活动及积分任务，以实现激励套利。

类似模式也出现在其他区域，例如越南黑灰产针对韩国地区 活动进行跨区域参与。

此外还发现中国区黑灰产针对美区活动进行批量薅取优惠券，声称月产10万u。

二、2025年全球电商平台黑产攻击链路

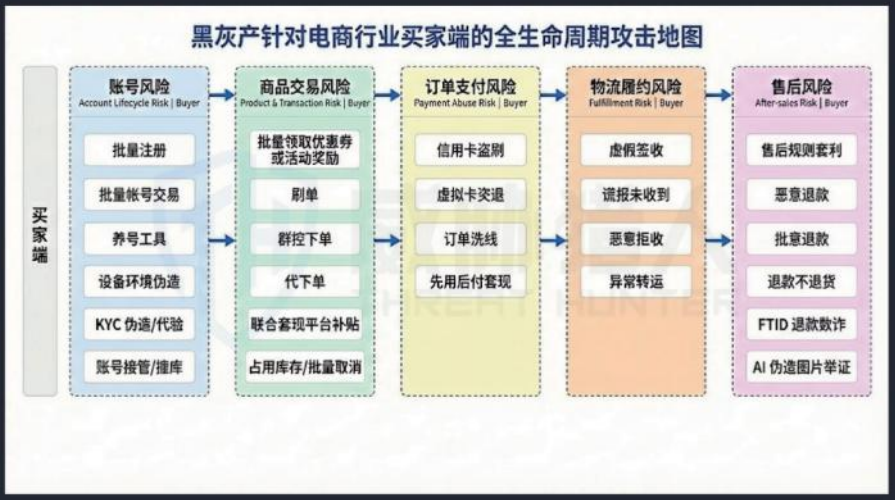
威胁猎人基于对全球电商平台风险的长期监测与分析发现，无论是卖家端还是买家端，黑灰产针对电商平台的攻击方式，均深度贴合平台业务流程。基于这一特征，本报告以电商平台的核心业务流程为主线，对分散在各业务阶段的黑灰产行为进行系统梳理，构建形成2025年黑灰产针对电商行业的全生命周期攻击地图。

2.1、黑灰产针对电商行业卖家端高频攻击行为主要集中在账号获取、违规商品供给以及交易与资金结算三大关键环节

从卖家端看，2025 年黑灰产高频攻击行为主要集中在账号获取、违规商品供给以及交易与资金结算三大关键环节，整体呈现出高度流程化、规模化与工具化的特征。

2.2、黑灰产针对电商行业买家端攻击目标在于最大化套取平台补贴与商品价值

从买家端看，黑灰产围绕账号、平台补贴、支付与售后规则，构建起一套覆盖全业务流程的生命周期套利体系，其核心目标在于最大化套取平台补贴与商品价值。



2.3、全生命周期攻击场景下，25年的黑产核心风险演化

2.3.1、利用 AI 批量伪造生成关键“证据”

2025年，随着生成式 AI、图像合成、视频换脸与文本生成能力的能力发展，黑灰产正在将申诉材料、身份材料与交易凭证等关键“证据”从以往的人工定制推向规模化生产。

威胁猎人反欺诈平台监测数据显示，自 2025 年以来，围绕 AI 人脸欺诈的黑灰产群组数正在快速增长，相关群组数量从 2025年 1 月的 116个攀升至 12 月的 361 个（仅监控数据情况）。

这类群组规模的快速扩张，意味着 利用AI 进行欺诈的相关手法，正在被大量黑灰产频繁讨论和交流。

从运作模式上看，当黑灰产供给端能够以模板、脚本与工具链的形式，对外持续提供人脸素材、KYC 视频、申诉证据等“可交付物”时，相关黑产组织会以群组形式快速复制。

在攻击路径上，黑产利用AI伪造证据的手法发展直接提升了多个关键环节的对抗效率，影响范围同时覆盖卖家端与买家端：

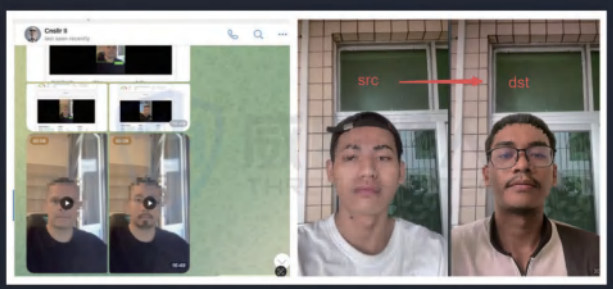
- **卖家端**：账号注册、账号申诉、商品批量上架
- **买家端**：虚假注册、恶意退款、售后申诉

2025 年，黑产利用AI作弊相关手法，主要体现在以下4个方面：

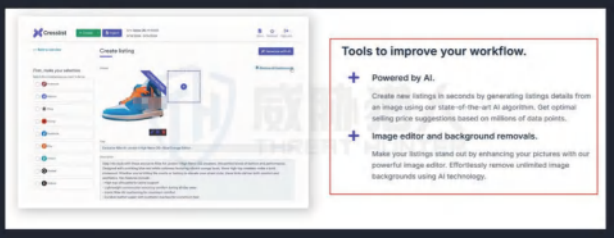
1、通过生成式 AI 批量生成身份说明、经营证明等文本材料，并结合图片加字、伪造图片等方式，快速拼装可用于申诉与审核对抗的虚假“证据”。

2、黑灰产利用图像生成与文本合成能力，自动生成虚假的物流轨迹截图、交易凭证及聊天记录，以提升在审核、申诉及售后对抗环节中的通过率。

3、黑灰产利用视频生成、换脸与语音合成等技术，批量生成用于 **KYC 认证与申诉复核** 的自拍视频和人脸验证素材，从而对抗身份校验与复核环节的风控。



4、黑灰产将图像生成能力与商品自动上架工具结合，快速生成符合平台审核规则的商品图片，并通过一键化操作完成批量上架，从而在短时间内绕过内容审核与人工抽检，放大违规商品的铺货效率。



2.3.2、物流作弊风险加剧

在 2025 年的全球电商攻击态势中，物流作弊正从传统意义上的“履约违规问题”，演化为一种跨场景、跨链条的基础攻击能力。其不再作为单一风险点独立存在，而是深度嵌入品牌仿冒货盘销售与恶意退款等高风险场景，逐步成为黑灰产规模化作恶的重要基础支撑物料。

从监测数据来看，物流作弊风险持续加剧。截至 2025 年底，相关作弊手法已覆盖至少 14 个国家和地区站点，横跨欧洲、美洲及亚太多个核心电商市场。

物流作弊之所以能够能够成为“基础物料”的根本原因在于：

物流信息在电商平台中同时承担履约证明与售后判定依据的双重角色。

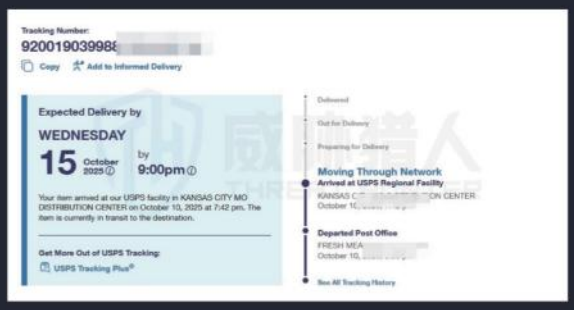
在品牌仿冒货盘倾销场景中，品牌仿冒货盘配合虚假仓能力，使仿冒商品得以在多个平台、多个账号中快速铺量，并在账号被封禁前完成集中变现；在售后阶段，黑灰产进一步通过伪造退货物流轨迹（如 FTID），利用平台对“退货已完成”状态的系统判定逻辑，在商品未实际返还的情况下触发退款流程，最终形成“货款双失”的高风险结果。

物流作弊在卖家端与买家端呈现出不同的风险表现形式，在关键业务节点带来不同的风险：

- 卖家端：商品交易风险、物流履约风险
- 买家端：恶意售后风险

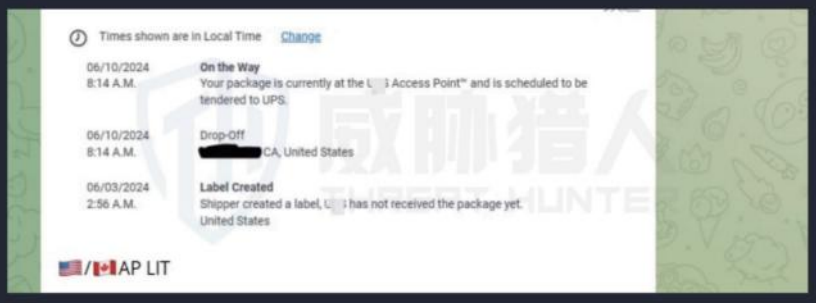
2025 年，物流作弊相关手法在效率层面呈现出明显变化，主要体现在以下3个方面：

1、通过预上网、预扫描、虚拟仓、AB 单、科技单等方式，在平台系统中提前制造“已发货 / 已揽收 / 已本地履约”的状态，使平台在风控介入时看到的是完整、合规的履约链路。



2、品牌仿冒货盘配合虚假仓，使品牌仿冒商品可以在多个平台、多个账号中快速铺量，并在账号被封禁前完成集中变现。

3、通过伪造退货物流轨迹（如 FTID），黑灰产可针对平台对“退货已完成”的系统判定逻辑，在商品未实际返还的情况下完成退款流程，形成“货款双失”的高风险结果。



2.3.3、攻击资源的真人化

随着电商平台对**虚拟化设备、指纹浏览器、异常 IP 行为**的识别能力持续提升，单纯依赖技术工具的自动化作恶模式正在面临边际收益下降以及被风控的问题。 在这一背景下，黑灰产开始系统性引入**真实人类参与的攻击资源**，推动攻击资源从“机器驱动”向“真人驱动”演化。

该类“真人众包”模式已渗透至多个关键节点：

- **卖家端：**使用真人注册卖家账号、真人代过KYC / 资质认证、真人申诉沟通帐号封禁与申诉
- **买家端：**帐号养号行为，真人代下单

2025 年，真人作弊相关风险主要体现在以下2个方面：

1. 真人使用个人手机、电脑和家庭网络进行操作使账号行为在设备指纹、IP 关联及使用环境层面高度接近真实用户，成为当前多账号治理中**最难识别的一类风险**。

2、在涉及身份校验与资质审核的关键环节，真人操作更容易被判定为正常用户行为。相比自动化工具，真人更不容易被识别为批量或异常，大幅提升了 KYC 通过率。

三、电商业务欺诈典型风险场景演变

本章所涉及的**假货风险、恶意退款、营销套利与物流作弊**，并非彼此独立存在的风险类型，而是黑灰产围绕**货源、账号、履约与售后**四个关键业务节点，在电商体系中系统性包装并组合形成的变现服务形态。

随着相关能力的不断成熟，上述风险正由以往的**单点违规行为**，演化为**跨环节联动、协同运作的系统性对抗**。

3.1、品牌仿冒风险：可规模复制的标准化货盘体系

3.1.1、2025 年品牌仿冒货盘的全球分布与规模化特征

1、仿冒货盘海外仓覆盖欧美多国

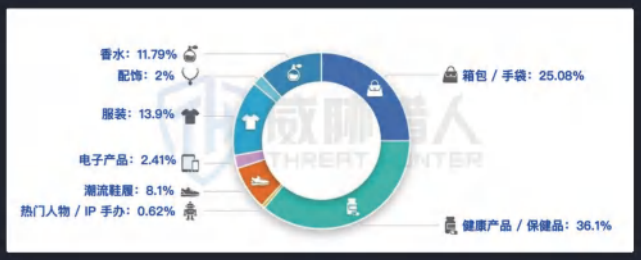
我们抽样了6个品牌仿冒货盘，接近2000款仍有库存的仿冒商品信息进行分析，从真实的冰山一角揭示当前品牌仿冒货盘带来的严峻现状。

基于这份仿冒商品数据，我们可以看到多个货盘黑产将美国市场单独作为重要的目标市场，欧洲市场也是倾销高地。因区域流通顺利，呈现出典型的欧盟国集聚，其中欧洲货盘的重点攻击市场为英国、意大利、西班牙、波兰和法国，黑产也亮出了如有欧盟境内买家，支持订单的覆盖范围。

2、仿冒品类主要集中在国际大牌的日常消费领域

仿冒货盘品类主要覆盖了鞋服箱包 、美妆个护、电子数码、保健品四大消费领域，这些品类的共性为：均是国际大牌高单价的仿冒商品、具备高客单价、高品牌溢价以及具备高复购性。

其中仿冒的保健品，是所有电商的敏感类目，直接与平台买家健康问题挂钩，也在通过各大电商中系统流入市场。同时在这份数据中，我们也看到货盘黑产紧追潮流消费热点，热爆款的IP手办的仿货也跻身其中。



3、大型的品牌侵权现场

我们不难看到每一品类都在迎合当前高消费市场潮流，以包包、潮鞋、服饰、香水、饰品、电子数码6个细分品类来看，当前的货盘主要供应的热门仿品对应的品牌top8如下：

3.1.2、货盘黑产的玩法正在全面升级

随着平台对传统仿牌、铺货行为的持续清退，货盘黑灰产并未收缩，反而通过引入自动化工具与算法能力，不断演化出更具隐蔽性与对抗性的攻击手法。

1、针对平台基因适配仿冒货盘模式

黑产比我们更懂平台的“基因”，黑灰产的攻击策略完全取决于平台商业模式、消费群体的水平和偏好。 他们不仅是在卖货，更是在针对平台的入驻门槛和假货鉴别机制、流量分发机制乃至当地消费者的偏好、观念和心理，定制差异化的攻击剧本，确保规模获利。

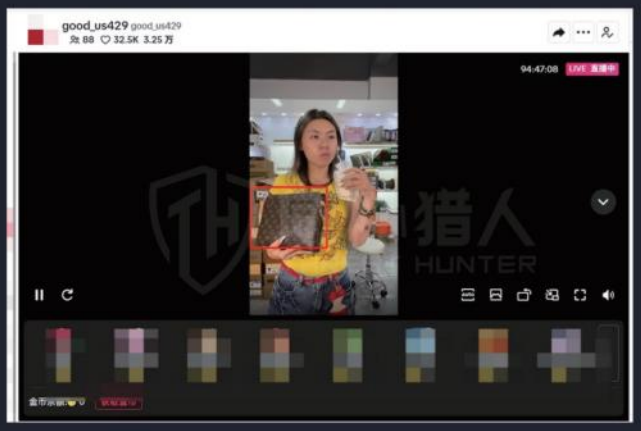
当前品牌仿冒货盘的目标电商，主要集中在c2c二手交易和b2c直播类电商，这种模式可以在两种差异的商业模式下均可规模获利的原因，除了消费群体特征在模型之内，更主要的它们在假货鉴别的机制上存在客观的难度，前者二手交易市场为低价正品批上了“天然保护色”，后者视频流生态会面临更复杂多样的假货绕过方式。

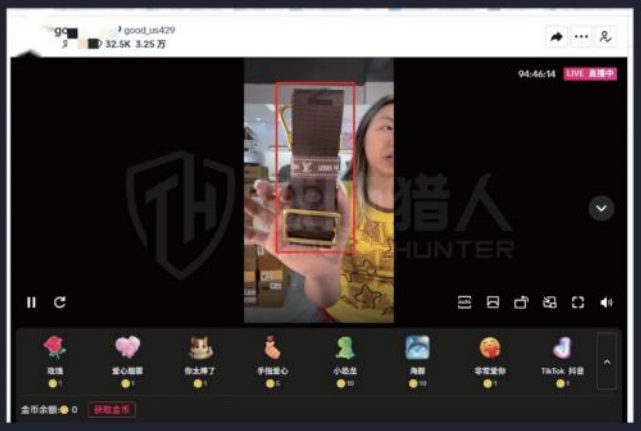
适配平台类型	平台基因	黑产攻击策略	规模化获利方式	主要治理代价
C2C 二手交易电商	• 信任驱动而非强审核 • C端卖家入驻门槛低 • 二手商品天然“非标品” • 鼓励循环经济、环保主义 • 用户存在“捡漏”、“寻宝”心理	• 将高仿包装为“闲置正品流转”合理化 • 假货特征：无原盒、无发票、轻微瑕疵 • 伪装本地个人卖家（语言/头像/定位） • 快闪铺货、违规即弃店、账号轮换 • 深度人设经营，走高价差长周期	• 多账号低成本试错快速堆量 + 短周期收割 • 单笔高利润，一单即覆盖大量成本	• 二手属性导致鉴别难 • 实物回收或强制鉴定可遏制假货风险，但成本极高，将牺牲平台扩张速度
B2C 社交直播电商	• 内容流或兴趣推荐主导 • 视频展示强于商品详情 • 达人账号权重极高年轻化 • 冲动消费市场盛行“反品牌溢价”观念	• “挂羊头卖狗肉”视频展示将高仿包装为“大牌同厂 Dupes” • 收购或盗用白名单达人老号老号为新店/仿冒链接导流 • OBS 矩阵直播 24h 循环播放	• 利用流量爆发快于审核介入，矩阵号瞬间引爆单品，在风控介入前完成收割并弃号	• 视频内容难以结构化识别 • 达人生态被反向利用监管存在明显时间差

2、社交直播引流与“暗链”闭环

在直播电商场景中，黑产逐步演化出“展示在站内、成交在站外”的分离式交易模式：

- 手法逻辑： 商家在直播间展示高仿商品，但不通过直播平台完成成交；
- 引流方式： 通过评论区机器人、语音引导或私信，将用户导流至独立站、即时通讯工具完成私下交易；
- 售后应对策略： 若被发现货不对版，商家通过“装可怜”诱导用户取消投诉，或直接利用仅退款策略快速平息争议以保全直播账号。





3、工业化店群矩阵（Store Matrix）与账号伪装

为应对平台对违规货盘的持续清退，黑灰产在中游构建起成熟的账号支撑体系：

- **高品质店铺（Elite Store）交易**：在帐号交易黑市中，具备高等级、高权重、全套法人资料、已过风控期的“高品质”是核心资源（售价高达数千元）。

- **环境隔离工具**：下游卖家普遍使用“指纹浏览器”和“矩阵上架工具”，确保数百个违规店铺在物理环境上完全隔离，避免因货盘雷同被平台封锁。

- **利用安卓真机，批量注册**：黑灰产出售**群控脚本，配合购买安卓真机，进行批量注册卖家账号**

3.1.3、“本地化”的品牌仿冒货盘提供案例：

在 2025 年度监测中，威胁猎人团队持续发现有黑灰产团伙向 某电商 卖家提供**美国本土仓品牌仿冒货盘服务**，协助违规商家在平台上架并销售高仿品牌商品，形成“货源–上架–发货”一体化的仿品供应链

1、本地仓仿冒货盘通过“供货–上架–本土履约”完成违规闭环

该类黑灰产通过以下方式完成违规交易闭环：

货源供给

1、黑产掌握多个美国本土仿冒商品仓库，主要集中在纽约及其他美国城市；

2、仿冒商品涵盖鞋履、箱包、服饰等高溢价品类，并在内部按高中低档进行分级。

商品上架操作

1、违规卖家从黑产处获取商品信息与实拍图，进行商品上架。

物流履约阶段

1、卖家将店铺发货地设置为美国本土地址（如纽约）；

2、订单成交后直接转交货盘黑产；

3、由黑产通过 **USPS** 完成本土发货，降低物流异常暴露风险。

2、黑灰产毛利率可达约 40%–73%

从黑灰产内部流通的建议售价与实际拿货成本来看，其整体毛利水平显著高于正常卖家区间。监测数据显示，相关商品的单件成本约为 50–60 美元，而对外建议售价通常在 100–200 美元之间，对应的毛利率区间可达 40%–73%。

3.2、恶意退款风险：以“退款成功率”为核心卖点的专业化欺诈产业

近年来，除个别消费者实施的恶意退款行为外，各大电商平台上逐步出现以“退款成功”为核心卖点的专业化黑灰产团伙。该类团伙通过分工协作与流程固化，形成覆盖多平台、多地区的退款欺诈服务网络。

3.2.1、2025 年恶意退款黑灰产风险：规模趋势与变现模式

1、全年恶意退款风险线索规模持续抬升，在9月达到峰值

从全年线索链变化来看，黑灰产围绕**恶意退款**的讨论热度呈现出**整体上升趋势**。 自年初起，相关线索数量逐月攀升，并在 **9 月达到全年峰值（23,099 条）**；此后虽有阶段性波动，但**连续多个月稳定维持在 20,000 条以上**。

2、恶意退款黑灰产佣金费用在退款金额的20%-30%

当下恶意退款**佣金费用在退款金额的20%-30% 区间，**该区间覆盖最多黑灰产团伙，适用于服装、鞋类、消费电子等常见品类，并且多数服务商多以“多地区多平台退款能力”作为核心卖点。

群组名称	佣金比例	覆盖站点 / 地区	服务特征与备注
黑灰产团伙1	35%	多平台	要求提供账号信息或订单信息，退款成功后抽成。
黑灰产团伙2	15% / 35%	美国、墨西哥	同一品牌下存在不同定价档位
黑灰产团伙3	30% / 35%	多平台	同时提供退款服务与“退款方法”，存在教程售卖行为
黑灰产团伙4	25%–30%	多平台	覆盖高客单商品，部分支持担保交易
黑灰产团伙5	25%–30%	印度	同时涉及账号交易与退款服务，服务混合度高
黑灰产团伙6	25%–30%	印度	针对服装、电子产品，面向印度本地市场
黑灰产团伙7	20%–25%	荷兰、德国、美国	按站点区分价格，部分设置退款金额上限
黑灰产团伙8	20%–25%	多平台	要求商品为平台自营或官方物流，降低退款失败率
黑灰产团伙9	固定 20%	多平台	要求收货后等待 2–3 天操作退款，宣称“100%成功”
黑灰产团伙10	15%	美国、墨西哥	低佣金吸引用户，部分展示未打码成功截图
黑灰产团伙11	15%	多平台	主打“稳定”“低抽成”
黑灰产团伙12	阶梯制：首单10%，后续15%	多平台	首单低价获客，强调“当天到货当天退款”
黑灰产团伙13	30%	多平台	群内同时交易信用卡、BIN、退款服务

3.2.2、新型恶意退款手法：物流欺诈与 AI 证据工业化

1、使用“危险物质泄漏”策略进行退款欺诈：

- 监测发现，部分退款案例中，黑灰产以“含电池、液体或化学物质商品发生泄漏”为由，声称存在安全风险，并引用当地危险品处理规范，诱导客服执行“仅退款不退货”流程。

2、使用虚假物流追踪（FTID）进行退款欺诈：

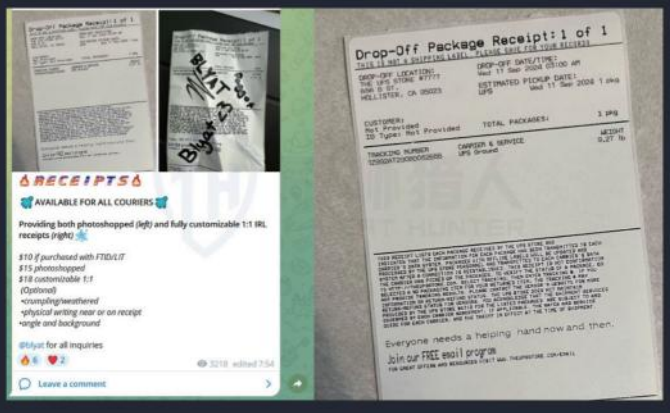
FTID，即 “Fake Tracking ID”（虚假追踪 ID）恶意退款手法，是指不法分子利用电商交易流程中的物流信息核查漏洞，在购物过程中，先订购心仪的高价值商品，收货后，通过非法渠道获取虚假的物流追踪 ID，伪装退货已送达商家的假象，进而向商家或电商平台索要退款，企图达到骗取商品和购物资金的双重目的，严重损害商家利益，扰乱电商行业的正常运营秩序。

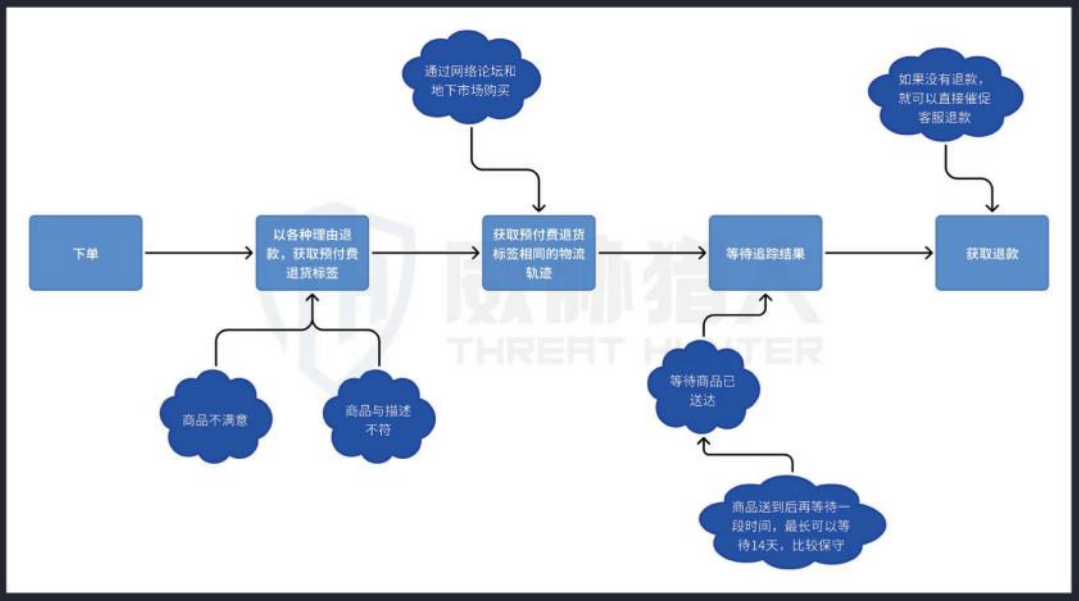
> FTID（Fake Tracking ID）是近年来较为典型的一类物流型退款欺诈手法，其核心在于构造“已完成退货”的虚假物流状态。

该类手法通常依赖于：

- 预付费退货标签机制
- 平台对物流状态的“已送达”识别盲区

一旦虚假轨迹被系统判定为“已送达”，即可能触发退款流程，对商家造成“货款双失”的风险。

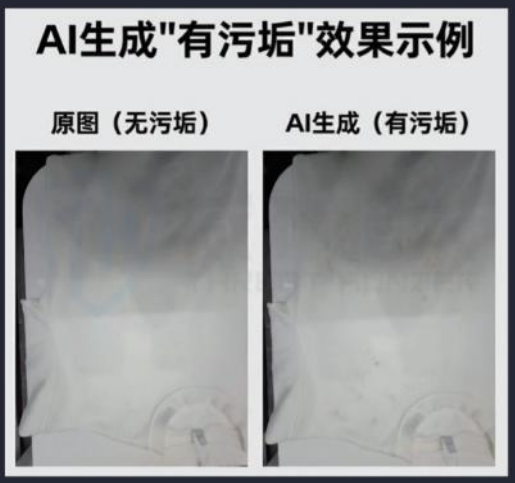




使用 AI 生成虚假证据进行退款欺诈：

随着生成式 AI 技术普及，部分恶意用户开始利用图像生成、视频合成等手段，批量生成高度逼真的商品损坏或异常使用证据。例如，他们可能使用AI将完好的商品图片或视频修改成出现裂痕、划痕、水渍等“损坏”状态，或者生成虚假的开箱视频、使用痕迹视频，以此作为向平台申请退货或退款的“证据”。

该类证据在视觉层面具有较强迷惑性，增加了人工审核与传统规则模型的识别难度，成为当前恶意退款风险的重要演化方向之一。



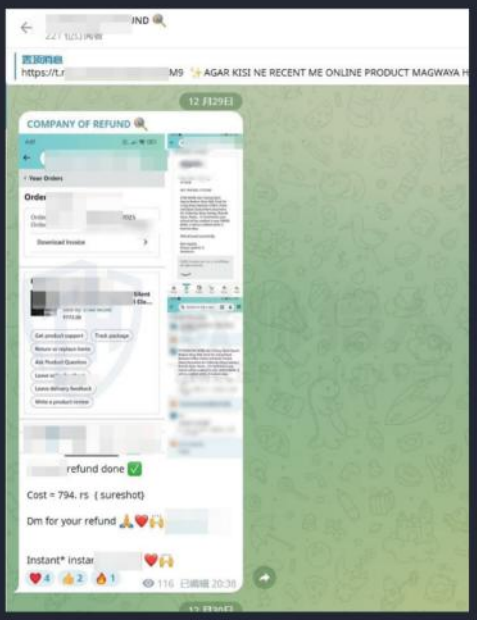
3.2.3、恶意退款典型案例：

监测发现，有黑灰产在 Telegram 渠道中**长期对外售卖某平台的退款代办服务**。该类服务以“高成功率退款”为卖点，吸引买家主动参与退款操作，并通过分成方式进行获利。

作恶模式说明：

从相关群组信息及沟通情况来看，该退款服务的核心操作模式如下：

- 买家需使用**自身真实的电商平台账户**完成商品下单，并等待商品正常送达；
- 在商品签收后，买家需将**电商平台账户登录信息**提供给黑灰产；
- 黑灰产随后登录买家账户，代为发起退款或售后申诉操作；
- 退款成功后，黑灰产按退款金额的 **35% 抽取佣金**。



该模式通过“真实账户 + 实物履约”的方式，显著降低平台对异常退款行为的识别难度。

3.3、营销活动套利：以账号与资源工程化为核心的作恶行为

黑灰产利用电商平台的营销活动机制（如新人礼、拉新奖励、满减券、优惠券裂变等），批量获取优惠券或积分资源，并以较低成本为第三方用户代下单，从中收取服务费用或通过价差实现套利，形成持续性的资金损耗风险。

3.3.1、营销套利的两种基础手法：虚拟化矩阵与真人众包：

监测显示，目前在电商平台营销活动套利场景中，主要存在两类手法模式：**虚拟化矩阵模式**与**真人众包模式**。

虚拟化矩阵工具持续升级：

虚拟化矩阵是黑灰产在电商营销套利场景中长期存在且持续演进的基础能力，其本质并非新技术出现，而是既有虚拟化手段的工程化与规模化升级。

当前在电商平台中观察到的虚拟化矩阵能力，主要可归纳为三类的技术手法：

1）指纹浏览器 + 代理 IP

2）模拟器母盘批量克隆

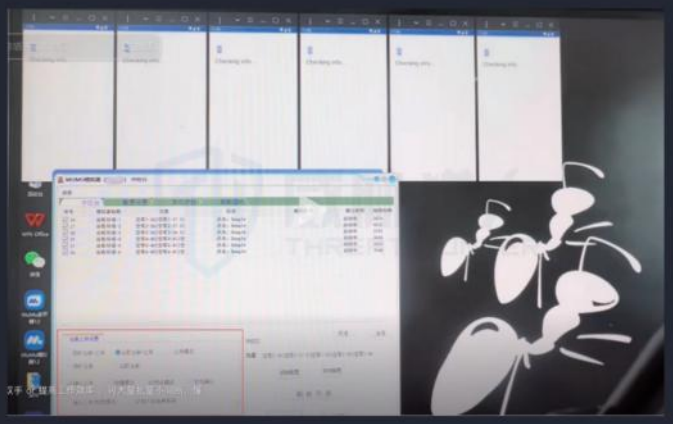
3）跨境云手机规模化部署

值得关注的是，上述工具的开发与商业化生态多源在功能完备性、规模化调度能力及自动化程度上已高度成熟，使相关虚拟化能力能够被低门槛地复制并应用于全球其他电商平台场景。

以下以模拟器母盘为例，对其作弊手法进行说明：

模拟器母盘是一种通过在计算机上运行虚拟设备环境（如模拟安卓或iOS设备）来实现多个账号独立运行的技术。**黑灰产利用这一技术创建虚拟环境，通过克隆母盘生成多个独立的模拟器实例，并对每个实例进行微调，以便批量注册多个账号并绕过平台的风控机制。**

该手法的核心思路是通过设置一个标准的母盘环境，包含设备指纹、IP地址、操作系统等信息，再批量克隆多个实例，然后进一步对每个克隆的模拟器进行微调，使得每个账号看起来像是在独立的设备上注册，从而避免平台的风控检测。



从风险特征看，该类行为往往表现为：**账号创建规模异常、环境高度相似但存在刻意差异、行为节奏具备自动化特征**，是电商平台营销套利与账号滥用场景中的常见基础能力之一。

真人众包成为对抗强风控环境下的方案

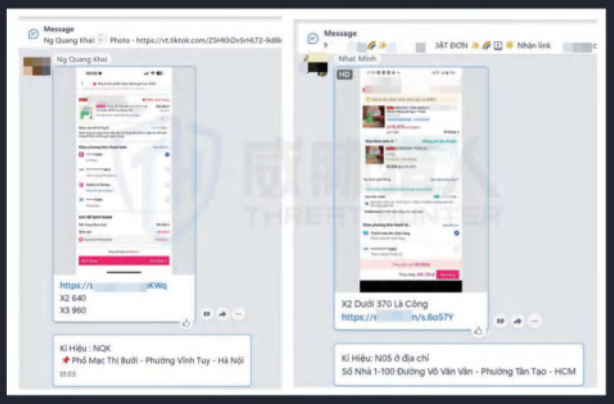
在电商平台持续强化 IP 与设备环境风控的背景下，除自动化工具刷单外，黑灰产在营销套利场景中也开始引入“真人众包”模式，以规避设备指纹和环境识别风险。

目前监测发现，该模式主要出现在私域社群渠道中，包括 Telegram、Zalo 等即时通讯平台。例如，在部分越南 Zalo 群组内，存在以领券、代下单为目的的真人用户招募行为。

黑灰产通过向真实用户支付报酬，引导其使用**本人真实设备、家庭网络环境**完成优惠券领取或指定订单操作，再由黑灰产进行订单回收或集中结算，从而规避平台对虚拟化环境的识别。

结合现有样本与区域分布情况，初步判断该模式的出现与以下因素相关：

- 部分平台对虚拟化操作行为的识别与拦截能力相对较强，压缩了虚拟化方案的实际投入产出空间；
- 部分地区真实用户人力成本水平较低，使真人参与模式在成本结构与成功率方面具备相对优势；
- 在上述因素叠加影响下，相关营销活动套利在特定区域内呈现出向真人众包模式集中的趋势。



3.3.2、黑五期间的营销套利案例：

在黑五期间的持续监测中发现，有黑灰产在社交平台公开发布并售卖某电商平台美区**10 美元无门槛优惠券**，并宣称该类优惠券可“长期供应”“数量充足”。

进一步跟进显示，该类优惠券**并非来源于正常用户的自然消费行为**，而是通过以下方式获取并变现：

1	2	3
黑灰产通过批量拉新注册账号，触发平台新用户营销机制获取无门槛优惠券；	在优惠券生成后，以账号整体交付的方式提供账号及登录凭据出售给下游使用者；	由购买者直接登录对应账号完成下单，规避优惠券跨账号使用的常规风控识别。

在交易与使用过程中，黑灰产明确向下游强调仅需“做好 IP 隔离”即可完成操作，要求使用独立 IP 环境以规避平台风控。这一表述反映出相关团伙已具备对平台基础风控逻辑的认知，并将 IP 与环境对抗作为其默认操作前提。

与此同时，其所宣称的“无限供应”并非源于单一优惠券异常，而是建立在成熟的批量账号注册能力之上：拉新流程高度自动化、账号批量注册获取，从而支撑该类套利行为的持续与规模化运作。

3.4、物流作弊风险：黑灰产跨环节协同的基础设施

过去，物流作弊更多体现为个别卖家为规避平台规则而采取的**单点违规行为**；而在 2025 年的全球电商风险图谱中，物流作弊并非独立风险场景，而是贯穿假货销售、营销套利与恶意退款的通用支撑能力。

3.4.1 两大核心变化：履约信息被伪造和风险被持续放大

1、物流作弊从“真实发货”转向“伪造履约信息”

物流作弊的核心变化，是**在平台风控介入之前，提前完成“系统侧履约闭环”**。当前主流电商平台的卖家履约判定体系中：商品是否发货，是否本地仓库进行发货，是否按时发货，高度依赖**物流信息节点反馈上报的信息，**黑产正是基于这一机制，使用非法技术**伪造合规信息，**具体表现为：

1. 利用虚拟仓、预上网、预扫描制造“本地已揽收”的合规信息；
2. 通过AB 单、信息嫁接伪造完整物流轨迹；

在平台风控介入前，提前完成“系统侧履约闭环”，平台看到的是“合规履约”，实际发生的是“跨境倾销 + 风险延迟暴露”。

2、物流作弊的“风险放大器效应”：货盘倾销与恶意退款的联动演化

在当前电商生态中，物流作弊已不再是孤立存在的履约违规问题，而是逐步演化为**同时放大前端货盘风险与后端售后风险的关键枢纽节点**，通过操纵物流信息，**为黑灰产风险行为规模化提供前提条件**。

1）对品牌假冒货盘风险的放大效应：支撑货源的规模化倾销

在虚拟仓、预上网、AB 单等手法的支撑下，违规卖家可以在未建立真实本地履约能力的情况下，完成以下伪装：

- 将品牌仿冒商品伪装为“本地现货”；
- 绕过平台对本地发货、时效履约的前置校验；

在这一模式下，**物流作弊成为品牌假冒货盘实现“工业化复制”和快速铺量的基础设施**，违规卖家能更快速地完成短期变现。

2）对恶意退款风险的放大效应：履约造假向售后套利的延伸

物流作弊的风险并不会在“发货完成”后结束，在**售后环节同样可以得到释放**。

虚假物流追踪（FTID）退款欺诈介绍中提到在该类场景下，其核心不在于真实退货，而在于构造一个“退货已完成”的虚假物流状态。黑灰产通常先完成高价值商品下单与收货，随后通过非法渠道获取或伪造与预付费退货标签匹配的虚假物流追踪 ID，使系统侧显示退货包裹已“送达”至商家或指定地址。一旦该虚假轨迹命中平台对“已送达”状态的自动识别逻辑，退款流程即可能被触发，而实际商品并未返还，最终造成商家“货款双失”。

3.4.2、AB 单的利用典型案例

威胁猎人发现有黑产**出售海外知名物流公司的真实面单单号信息**，可以用于**AB单**中的A面单。

黑产通过特殊手段将已有轨迹的面单收集到私人网站中，违规卖家可通过网站查询相应的面单进行购买，并上传到电商平台中，来**伪造发货时间和物流轨迹，绕过平台本土发货和发货时间规则的限制**。

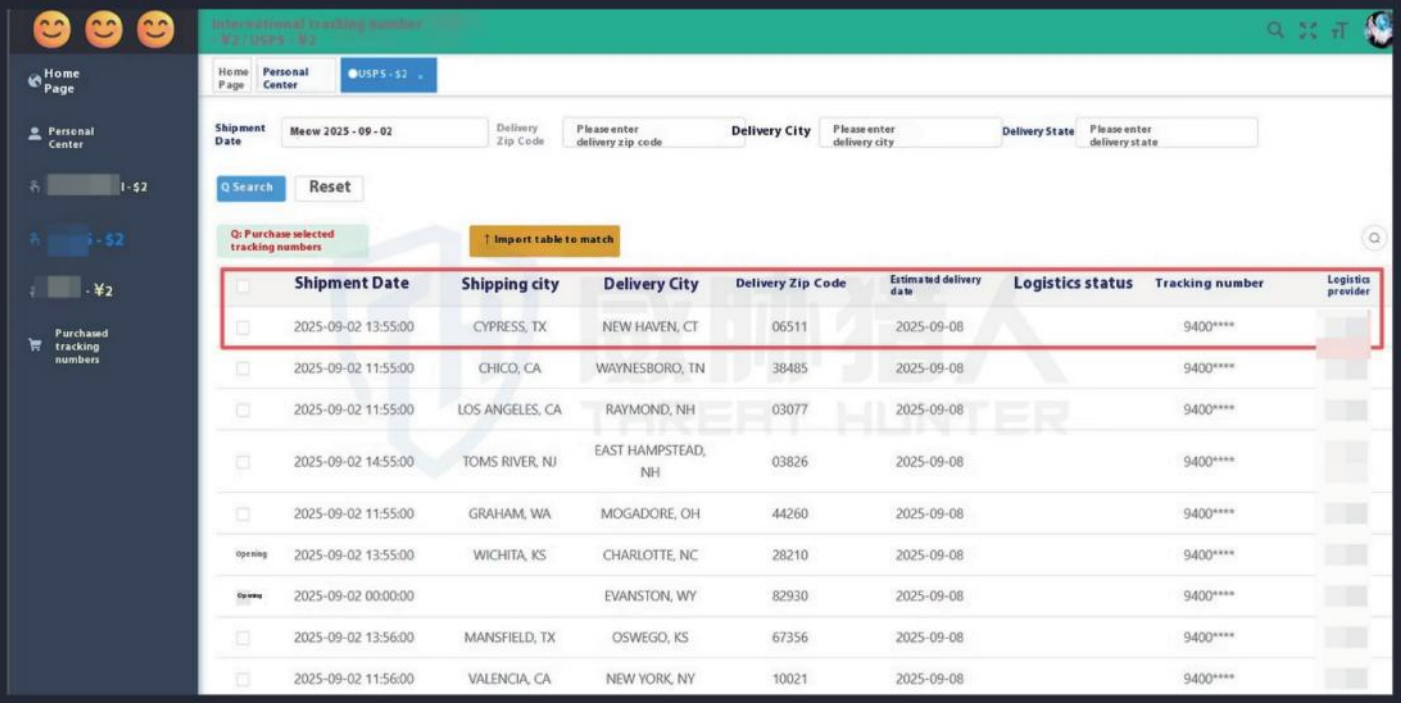
查询黑产私人网站发现，涉及到多个**站点国家均有本土单号出售**，例如：英国、法国、德国、美国等；澳大利亚地区单号也在提供范围。

AB单会用到了两种单号：

- A单（虚假单号）：卖家使用一个**虚假的、与实际发货不符的物流单号**（A单）上传至电商平台，以满足平台发货时效要求，**制造已发货的假象**。
- B单（真实包裹）：卖家通过其他物流渠道，**使用真实的物流单号**（B单）发送实际商品给买家。**B单通常不上传至平台，仅用于实际发货和买家收货**。

黑产操作方式：

1	2	3
面单选择与购买： 违规卖家出订单后，根据买家收货地址从黑产的私人网站查找与收货地址相同的本土发货A面单，购买相应面单。	**A面单上传平台：** 将已购买面单单号上传到发货的电商平台中。	**卖家发货自主发货：** 违规卖家使用另一个B面单直接发送商品包裹到买家收货地址中，完成交易闭环。



总结：

2025 年，黑灰产不再只是围绕单一规则漏洞或局部业务场景展开作恶，而是以平台业务流程为攻击蓝本，构建起覆盖账号、货源、履约与售后的**全生命周期、可复制的作恶方式。**

在这一过程中，物流作弊、虚假证据生成、真人化资源等，已不再是孤立存在的风险作弊手段，而是逐步演化为**跨场景复用的基础能力**。这些能力被嵌入品牌仿冒、恶意退款、营销套利等多个高风险场景之中，使呈现出**联动放大**的态势。

面对这一趋势，单一的“防守策略”已无法奏效，平台必须构建多层面的情报驱动防御体系，将“看见风险”升级为“压缩黑产 ROI 的系统工程”：多层面的情报驱动防御体系

战略层面

建立以跨区域流动性与攻击迁移能力为核心的风险预警机制，提前识别黑灰产资源在不同市场间的转移与重组；

战术层面

需要从封堵单一手法，转向识别可复用的攻击能力与行为模式，重点打击其规模化与自动化基础；

技术层面

则应通过多模态信息交叉校验、业务逻辑反验证与成本放大机制，持续压缩黑灰产的投入产出比（ROI），迫使其攻击路径不断失效。

展望未来，电商安全将不再是单一技术问题，而是一场围绕业务理解深度、深入贴近业务的长期博弈。威胁猎人将持续关注相关欺诈动态，为企业提供最新的情报支持和防范建议。

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