威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

黑产大数据

2024上半年度海外电商平台风险研究报告

THREATHUNTER

目录

前言

近年来，海外新兴电商平台不断涌现并迅速成长。Shopee、Lazada、Tokopedia 等东南亚平台在东南亚市场发展势头强劲，已占据主导地位；Mercado Libre 在拉丁美洲市场表现出色； Etsy 在手工艺品、复古商品等细分领域具有较强竞争力；中资跨境电商平台 SHEIN、Temu、AliExpress、TikTok Shop 被业界称为跨境电商平台“四小龙”，为全球电商市场的发展注入新的活力。

与此同时，海外电商平台面临的安全挑战亦日趋严峻。**恶意刷单、优惠滥用、恶意退款等黑灰产活动频发。**这些攻击行为不仅扰乱了市场秩序，还给海外电商平台和企业带来了直接的经济损失，影响了正常运营和长期发展。

威胁猎人基于黑灰产在海外电商场景的威胁情报分析，正式发布**《2024 上半年度海外电商平台风险研究报告》**。本报告统计数据周期为 2024 年 1 月至 7 月，针对海外电商当前行业面临的 **8** 大类风险场景，威胁猎人情报研究团队通过深入地数据分析，提供全面的风险洞察，助力海外平台及企业有效识别并防范潜在威胁，实现业务持续稳定发展。

相关名词定义：

1. 偷区：指在运输过程中，商家将货物的实际发货地址更改为费用较低的地址，以减少运费；

2. 偷重：指在运输过程中，商家故意低报重量来减少物流费用；

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

4. 私域群聊：指微信、qq、WhatsApp，zalo 等群聊渠道；

5. 社交媒体：指小红书、微博、Facebook、twitter 等社交软件；

6. 发卡网站：指一种专门用于自动化销售虚拟商品或服务的在线平台。发卡平台现已成为互联网黑灰产的主要交易通道和协作平台，发卡网站不能被网页检索，需要具体的发卡商品链接才能链接到商品页；

7. 成品账号、成品号：指已经绑定了个人或企业资料信息的账号，这些账号购买后无需额外注册或填写信息，可直接使用；

8. 黄牛代下：指黑灰产雇佣真人远程下单，来批量薅取活动限购优惠商品的作恶行为；

9. 接码号：指黑灰产或羊毛用户通过接码平台，利用接码平台黑卡手机号批量注册平台账号或授权登录平台，薅取平台或小程序活动奖品；

10. CK 号：CK 号是一种上号方式，该数据号包含平台账号登录信息，通过独立的 COOKIE 账号信息，可实现免密登录，每种 CK 号，都会对应一种上号器。CK 号可以无视 IP 频繁登录，登录设备无记录，可有效减少部分影响账号权重的因素，通常被黑灰产用于批量注册、授权微信小程序，薅取平台活动奖品；

11. 平台代入驻：指想要入驻平台的商家通过中介办理入驻手续；

12. EIN 证书：EIN 是 Employer Identification Number（雇主识别号）的缩写，是美国国税局（IRS）为企业或其他组织分配的唯一识别号码。EIN 证书是一个正式文件，证明某个组织或企业已经获得了 EIN，并且该号码已经注册并生效。该证书通常包括企业名称、EIN 和注册日期等信息；

13. VAT 照片：VAT 是 Value Added Tax（增值税）的缩写，是一种广泛使用的消费税，许多国家和地区对销售商品和服务收取此税。VAT 照片通常指企业或个人获得的增值税登记证明的照片或扫描件；

14. 真人众包：指一群兼职人群（宝妈、学生）通过众包平台、众包群领取悬赏任务，协助黑灰产（众包任务发布者）完成任务，领取做单费用，而黑灰产则顺利完成任务薅取平台奖励，任务类型包含：拉新、注册、助力、下载、点赞等刷量风险，还可发布实名、申请等高危风险众包；

15. 自养号刷单：指商家使用指纹浏览器购买海外服务器、IP 搭建刷单环境，实现批量注册目标平台账号、养号、浏览模拟以及下单的行为；

16. 真人刷单：指黑灰产通过雇佣真实用户伪装成普通消费者的方式在电商平台上进行虚假交易的行为；

17. 指纹浏览器：指一种特殊的浏览器，访问网站时可以通过设置语言、操作系统、显示分辨率和硬件配置等信息，来模拟和伪造用户的浏览器指纹；

18. 物流作弊：指电商卖家使用虚假发货单或科技快递单发货的行为，以实现偷区、偷重或逃税，降低销售成本；

19. 二次单号：指物流单号被泄露或被物流公司售卖再次使用；

20. 跑水账号：指拖欠运费或使用盗刷信用卡来支付运费的物流账号；

21. 跑水面单：指使用跑水账号生成的物流面单；

22. 科技面单：指黑灰产破解面单生成规则后自己生产的快递面单，这类面单可以被部分单号扫描仪正常识别并可以在官网上查询对应的物流单号与物流轨迹；

23. 认证绕过：指黑灰产在电商平台身份认证过程中，利用某些技术手段或采用不合规的方法，逃避认证的行为；

24. 店铺账号保证金：卖家在平台注册时，需要缴纳的一定金额，以确保店铺能够正常运营，如果账号出现违规行为，保证金可能会被封禁；

25. 货盘：指企业将产品批量运输并存储在境外仓库，即海外仓，以便快速配送和销售到当地或周边市场。

01

海外电商平台风险场景态势

一、海外电商平台风险场景态势

以下为威胁猎人针对海外电商的情报分析，统计数据周期为 2024 年 1 月至 7 月：

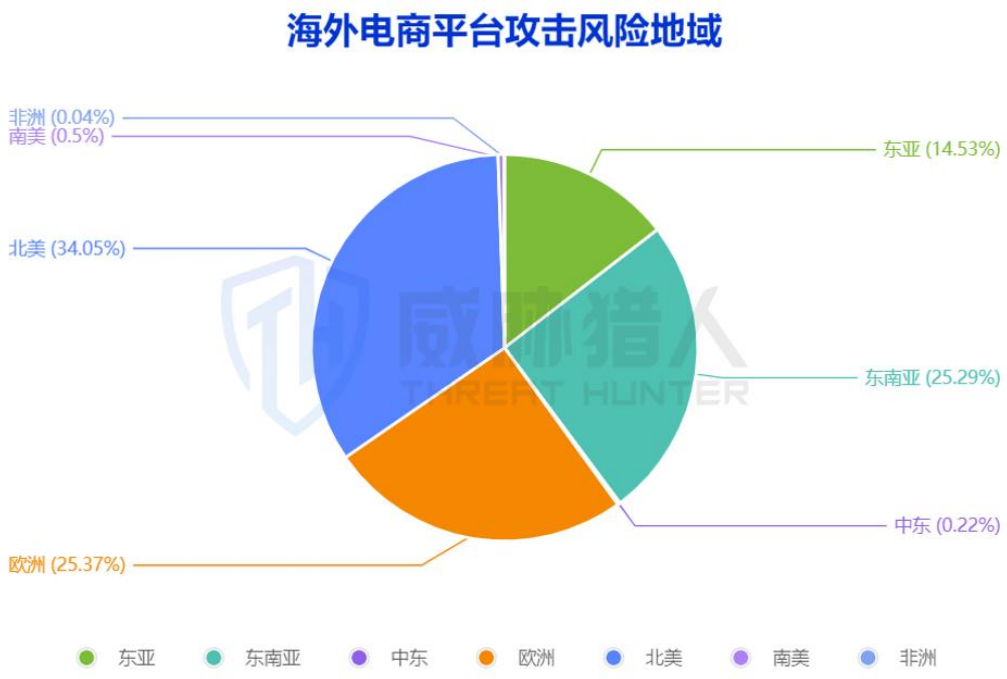
1.1、捕获到攻击海外电商平台的风险线索总数超 201 万条

威胁猎人捕获到的攻击海外电商平台的风险线索总量超过 201 万条，共有超过 72 万个黑灰产账号参与，这些黑灰产账号归属地包括：中国、越南、泰国、西班牙、印尼、美国等。

1.2、海外电商平台攻击风险地域，北美、欧洲、东南亚排名前三

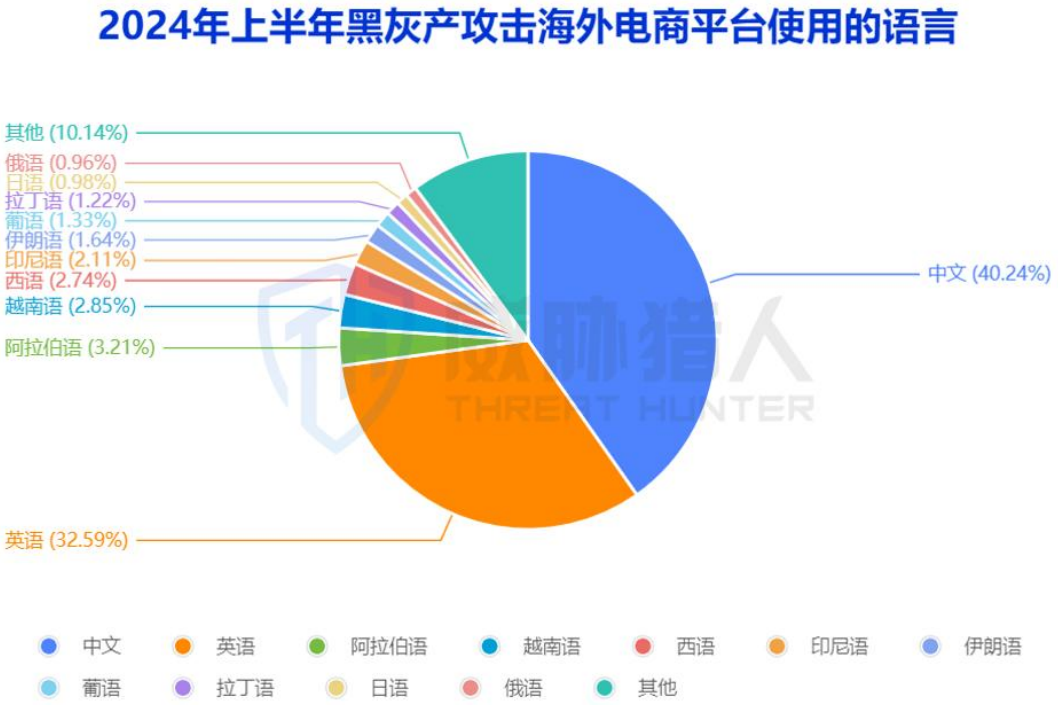
在全球各个地区的海外电商平台中，**北美的电商平台受到的攻击最多，占比 34.05%，其次是欧洲地区和东南亚地区，分别占比 25.37%和 25.29%。**北美地区被攻击占比高的原因主要由于北美地区有许多全球性的海外电商公司，这些公司业务范围广泛，规模庞大，使用人群多，因此成为黑灰产主要攻击目标。

注：中国区域电商平台统计数据不包含本土电商，如：淘宝、京东、拼多多等。



1.3、中文和英文成黑灰产攻击海外电商平台主要使用的语言

截至 2024 年 7 月底，威胁猎人针对平台监控渠道中攻击海外电商平台的情报统计分析发现，在黑灰产活动中，黑灰产使用中文、英文占比最高，分别占 40.24%、32.59%。



注：数据来源于 Telegram、Facebook、twitter、zalo、reddit 等海外渠道，以及微信、qq、微博等国内渠道。

1.4、海外电商平台主要面临 8 大风险场景，账号风险、刷单、物流作弊排前三

威胁猎人针对 2024 年截止 7 月底捕获到的攻击情报统计分析发现，海外电商平台主要面临 8 大风险，分别是：账号风险、刷单风险、物流作弊风险、商品信息爬取风险、恶意退款风险、认证绕过风险、内外勾结风险、货盘风险。

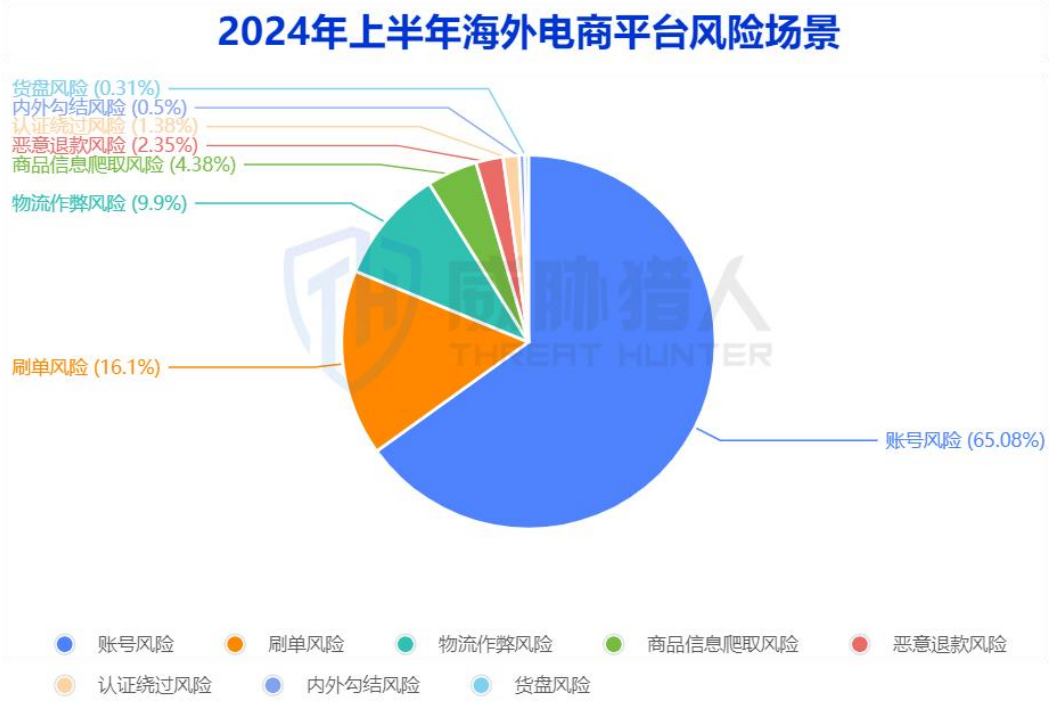
其中，**最常见的 3 大风险分别是：账号风险占比 65.08%、刷单风险占比 16.1%、物流作弊风险占比 9.9%。**

账号风险占比最高的原因，主要有三点：

（1）账号在海外注册比较方便，仅需要邮箱就可以成功注册买家账号，而且还存在匿名邮箱可以使用，黑灰产极易获得；

（2）海外电商卖家账号的产业链非常健全，从注册需要使用的虚假物料信息到成品账号都有大量黑灰产业在进行销售；

（3）账号是黑灰产后续作恶的基本物料，没有账号将不能领取优惠券，也不能进行刷单作恶，因此黑灰产会对账号注册进行大量研究。

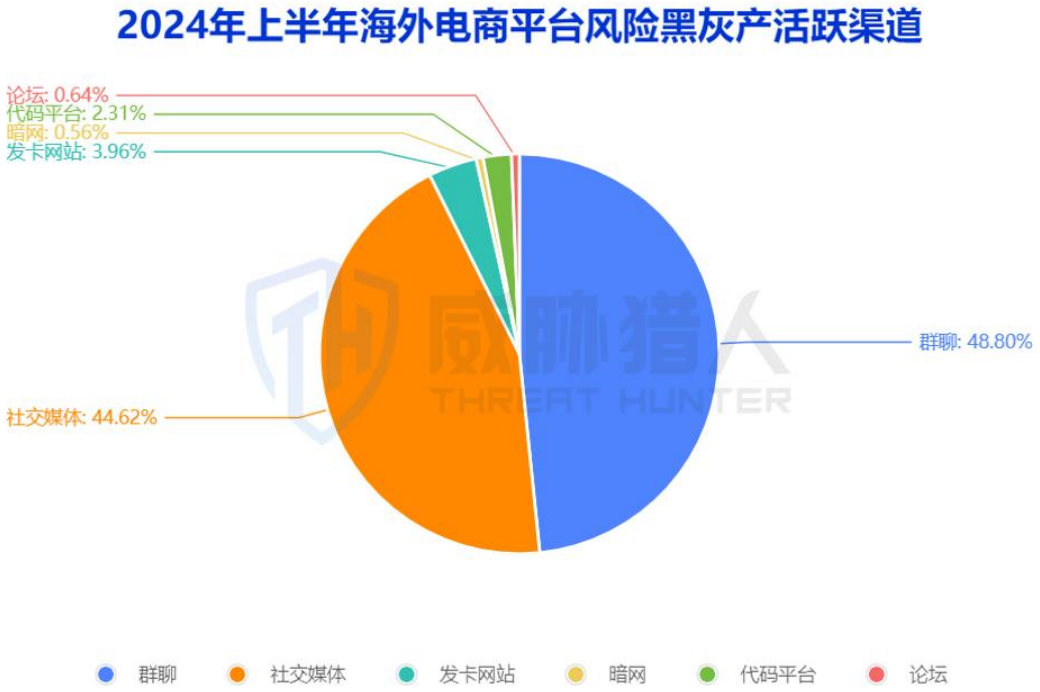


1.5、风险线索来源中，私域群聊中的线索最多，其次是社交媒体

全球各地的黑灰产作恶行为主要通过私域群聊渠道和社交媒体平台进行传播和牟利。**海外电商平台的风险线索来源中，私域群聊占比 48.80%，其次是社交媒体，占比 44.62%。**

不同国家和地区在使用的平台上有所差异。例如，国内沟通的私域群聊渠道有 Telegram、

微信、QQ 等，越南则普遍使用 Zalo，印尼更常用 WhatsApp。东南亚地区的社交媒体以 Facebook 为主，美洲和欧洲则更倾向于使用 Twitter，黑灰产也通过这些平台进行传播和非法活动。



针对发卡网站渠道分析发现，国外与国内出售的黑灰产商品大类基本相同，不同的是出售商品细节根据各国特点会有所不同，例如：国外个人资料的出售通常涉及护照和驾照，而国内则主要使用身份证。在国外，注册多用邮箱，出售的各种邮箱也比较常见。目前威胁猎人共监控到 195 个海外发卡网站，所提供的风险线索占总体 3.96%。

发卡网站：指一种专门用于自动化销售虚拟商品或服务的在线平台。发卡网站不能被网页检索，需要具体的发卡商品链接才能链接到商品页，目前已成为互联网黑灰产的主要交易通道和协作平台。

1.6、针对国内和海外电商平台，黑灰产攻击的风险场景有差异

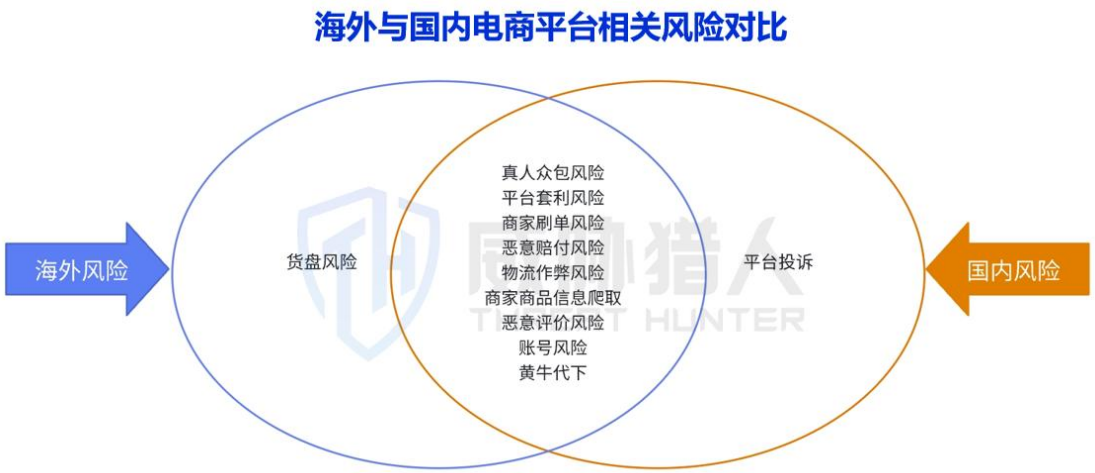
国内电商平台和海外电商平台面临的风险有许多重合之处，但在细分场景上却有差异。两者

均面临商家刷单、黄牛代下、账号等风险，但在操作方式和具体细节上却有不同。例如：

（1）刷单场景：国内的商家刷单风险在海外电商平台上同样普遍。然而，国内平台对店铺刷单作弊行为进行了长期的风险控制，导致刷单方式变得多种多样，比如通过直播间进行低价秒杀，利用优惠平台如一分钱购，以及通过小程序进行免费试用刷单等。相比之下，海外电商平台的刷单方式仍主要依赖真人刷单和自养号刷单。

（2）黄牛代下：目前在国内新兴的黄牛代下在海外也存在，并且海外也存在直接利用各平台之间的差价，进行低买高卖行为。比如：黑灰产在 A 平台采集更低价的商品信息，在 B 平台注册电商账号，并以高价进行售卖。如有用户在 B 平台下单，黑灰产会返回 A 平台下单，以此赚取差价。而国内普遍作法是将低价商品先大量购买到仓库保存，再进行出售。

（3）账号风险：无论国内或是国外电商平台都存在账号风险。国内主要集中在买家端的账号风险，而海外则主要集中在卖家端的账号风险。国内很多营销活动都需要买家账号助力，黑灰产为了能够完成活动任务，会需要大量账号，因此国内会产生出很多接码号、ck 号等。而海外注册账号难度比较低，大多数仅需邮箱就可以注册成功，注册难度比较低，黑灰产出售买家账号较少。



02

海外电商平台
具体风险场景分析

二、海外电商平台具体风险场景分析

威胁猎人针对海外电商平台进行调查发现，海外电商平台主要经受的风险分别是：账号风险、刷单风险、物流作弊风险、商品信息爬取风险、恶意退款风险、认证绕过风险、内外勾结风险、货盘风险。

风险定义：

账号风险：指涉及账户的安全威胁和潜在风险的各种情境。这些场景包括但不限于以下几种情况：账号注册风险、账号接管风险、代入驻风险、成品号售卖风险、账号共享和租借风险；

刷单风险：指由平台卖家付费委托刷单黑灰产，通过刷单工具或真人刷手向指定的平台卖家购买商品、填写虚假好评来提升店铺销量、信用度和评分、获取平台流量的欺诈做法；

物流作弊风险：指电商卖家使用虚假发货单或科技快递单发货的行为，这样可以实现偷区、偷重或逃税，从而降低销售成本。然而，物流作弊一旦被物流公司查到，货物可能会被扣押，卖家还需补交运费，这将严重延误商品的交付时间，降低用户对平台的信心；

商品信息爬取风险：指电商平台或网站可能面临未经授权的爬虫程序（爬虫）非法获取平台上商品信息的风险；

恶意退款风险：指用户通过不正当手段申请退款，从而获取不应得的利益；

认证绕过风险：指黑灰产在电商平台身份认证过程中，利用某些技术手段或采用不合规的方法，逃避认证的行为；

内外勾结风险：指黑灰产与平台的内部人员秘密勾结合作，达成非合规入驻平台，解封账号等目的；

货盘风险：指黑灰产在海外仓的低质货盘，容易给平台带来质量风险和平台履约率问题。

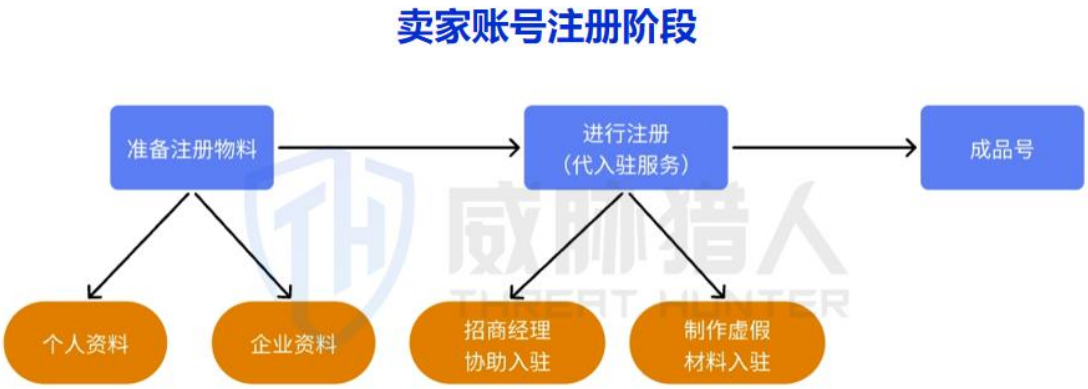
下面将围绕这 8 大风险场景进行分析：

2.1、账号风险场景分析

账号风险场景：指涉及账户的安全威胁和潜在风险的各种情境。这些场景包括但不限于以下几种情况：**账号注册风险、账号接管风险、代入驻风险、成品号售卖风险、账号共享和租借风险；**

在电商平台中主要有买家和卖家两种用户角色，因此，电商平台的账号风险也被分为两大类：买家账号风险和卖家账号风险。**以下将对将卖家账号风险做重点分析，**包括卖家账号注册、平台代入驻，以及售卖卖家成品号等方面。这些风险可能导致欺诈行为增加、侵权风险上升，严重降低用户信任，最终对平台的声誉和业务发展产生负面影响。

卖家账号注册需要提前准备注册材料，并按照一系列步骤进行注册入驻。注册成功的账号称为成品号。即共有三个阶段，分别是**准备注册材料，注册阶段，成品号阶段。**



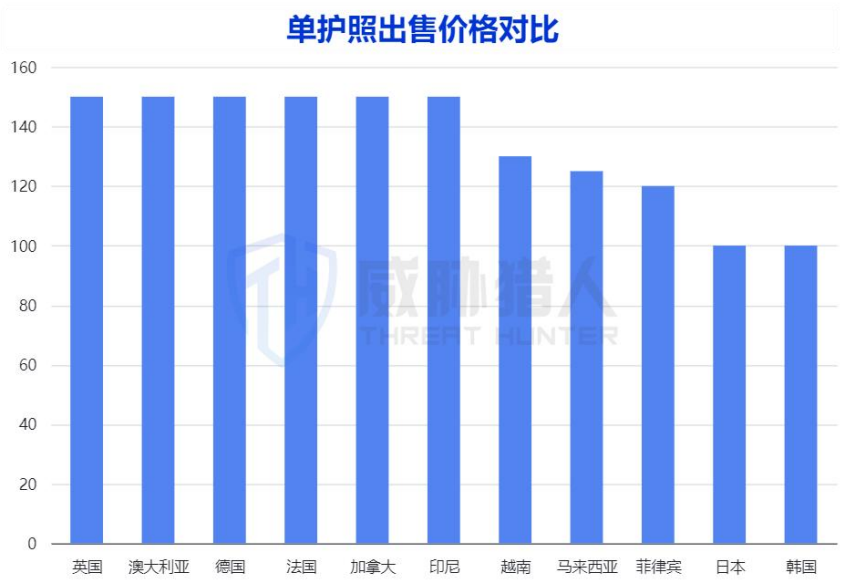
2.1.1、准备注册材料阶段，黑灰产会使用虚假信息注册账号

黑灰产通常会通过私域渠道进行推广，在发卡网站发布和出售基础物料信息。根据注册材料的要求，黑产售卖的基础物料主要有两种类型：个人资料和企业资料信息售卖。

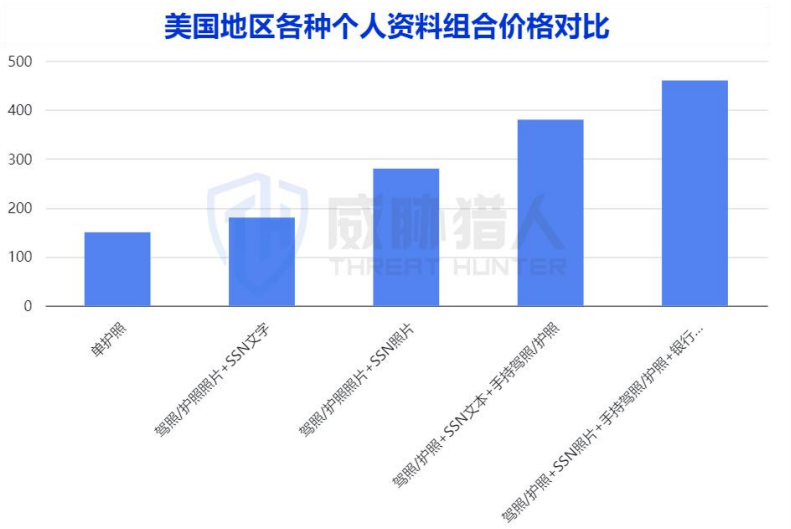
（1）个人资料信息售卖

海外电商卖家账号注册可以使用驾照或者护照进行注册，根据不同平台要求还会增加手持照片或者银行流水等补充材料。

a. 单护照的出售价格，购买美洲国家和欧洲国家的护照价格最高，出售价为 150 元。东南亚国家中，购买印尼的护照同样为 150 元，购买越南的护照需要 130 元，购买马来西亚的护照 125 元，购买菲律宾的护照 120 元，东亚国家中，购买日本和韩国的护照仅需要 100 元。



b. 美国是出售个人资料组合类型最多的国家之一。价格随着资料种类增多也相对提高。



(2) 企业资料信息售卖

由于海外电商平台通常要求企业提供相关资料才能入驻，因此，出售企业资料信息情况频发。

威胁猎人发现，黑灰产出售的企业资料在各国普遍存在五种类型的组合：

① 企业营业执照 + ein 证书/vat 照片 + 法人护照

② 企业营业执照 + ein 证书/vat 照片 + 法人护照 + 6 月内银行账单

③ 企业营业执照 + ein 证书/vat 照片 + 法人护照 + 法人手持护照

④ 企业营业执照 + ein 证书/vat 照片 + 法人护照 + 法人手持护照 + 6 月内银行账单

⑤ 企业营业执照 + ein 证书/vat 照片 + 法人护照 + 法人手持护照 + 法人 SSN 照 + 6 月内银行账单

具体价格如下：

类型	均价
企业营业执照+ein证书/vat照片+法人护照	400
企业营业执照+ein证书/vat照片+法人护照+6月内银行账单	570
企业营业执照+ein证书/vat照片+法人护照+法人手持护照	700
企业营业执照+ein证书/vat照片+法人护照+法人手持护照+6月内银行账单	805
企业营业执照+ein证书/vat照片+法人护照+法人手持护照+法人SSN照+6月内银行账单	957.5

2.1.2、在注册阶段，黑灰产会提供商家代入驻服务

商家代入驻服务主要指没有相应资质的卖家通过招商经理购买邀请码，或者利用黑灰产的不正当手段申请入驻，从而绕过电商平台的入驻要求。

商家代入驻目前主要有两种方式：1.使用招商经理的邀请码，进行入驻；2.黑灰产提供虚假的入驻资料进行入驻平台。

(1) 使用招商经理的邀请码，进行入驻

为了吸引优质商家入驻，电商平台往往会给招商经理一批邀请码，有邀请码的商家在入驻时，平台会给予一定的优惠或者特权。比如，商家入驻速度比较快，容易得到平台的流量倾斜等。

一些招商经理为了牟利，选择和黑产进行合作，黑产负责找想要入驻平台的商家，招商经理主要负责提供入驻平台的邀请码，商家入驻后，黑产和招商经理再进行分配利益。因此，通过招商经理邀请码入驻平台的方式存在内外勾结的风险。

（2）黑灰产提供虚假入驻资料，协助卖家入驻平台

黑灰产代入驻方式主要出现在电商的跨境店铺账号中，即中国国内发货，海外销售模式的店铺。黑灰产代入驻方式针对不了解电商平台的用户，以及一些想要快速入驻平台的用户，提供入驻服务。

a. 代入驻的价格，根据用户提供的材料而有所不同。

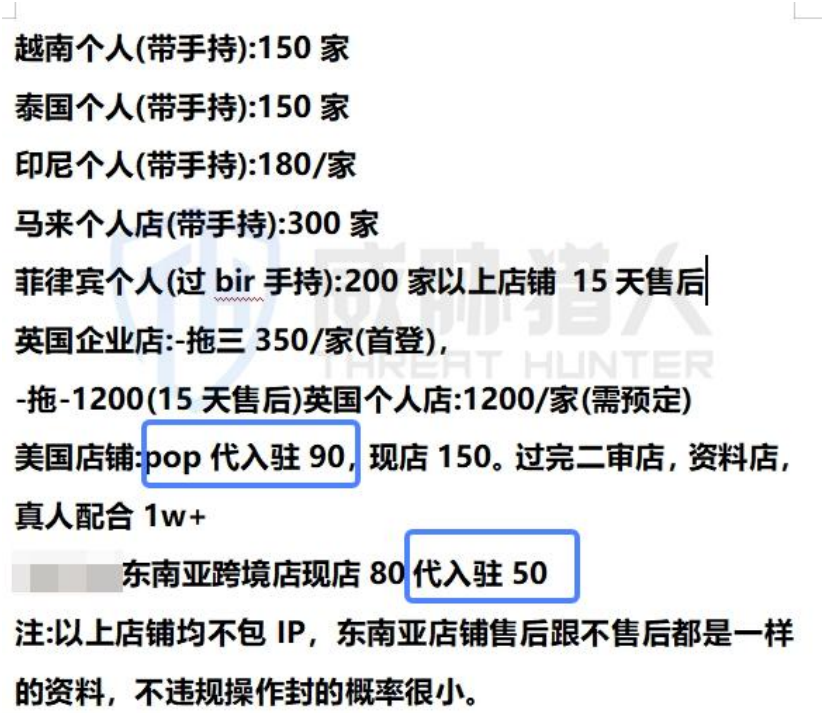
以某电商平台为例，如果用户只提供个人身份信息，黑产将利用这些信息注册营业执照，并准备银行流水和海外仓储证明等文件。因此，相对于那些提供完整材料的用户来说，只提供部分材料的代入驻的价格将高出不少。

b. 代入驻的价格，根据类型和区域不同，差异较大，在 50 元-13000 元之间。如：

- 美国普通跨境店代入驻的费用只需 100-200 元，入驻这种类型的店铺需要的注册材料只是纯文本的信息，比如身份证信息、营业执照信息、手持证件照即可。
- 代入驻收费较高的，比如美国跨境水晶类目店铺，代入驻费用高达 13000 元。这种类型的店铺入驻需要的注册材料比较复杂，除了身份证信息、营业执照信息、手持证件照外，还需要店铺报白、品牌资质、商品信息等材料。
- 此外，东南亚区域代入驻的价格普遍低于美国区域。东南亚区域代入驻价格为 50 元，

美国区域代入驻价格 90 元。

以下为一位黑灰产的报价单，显示了出售店铺账号价格的具体情况：



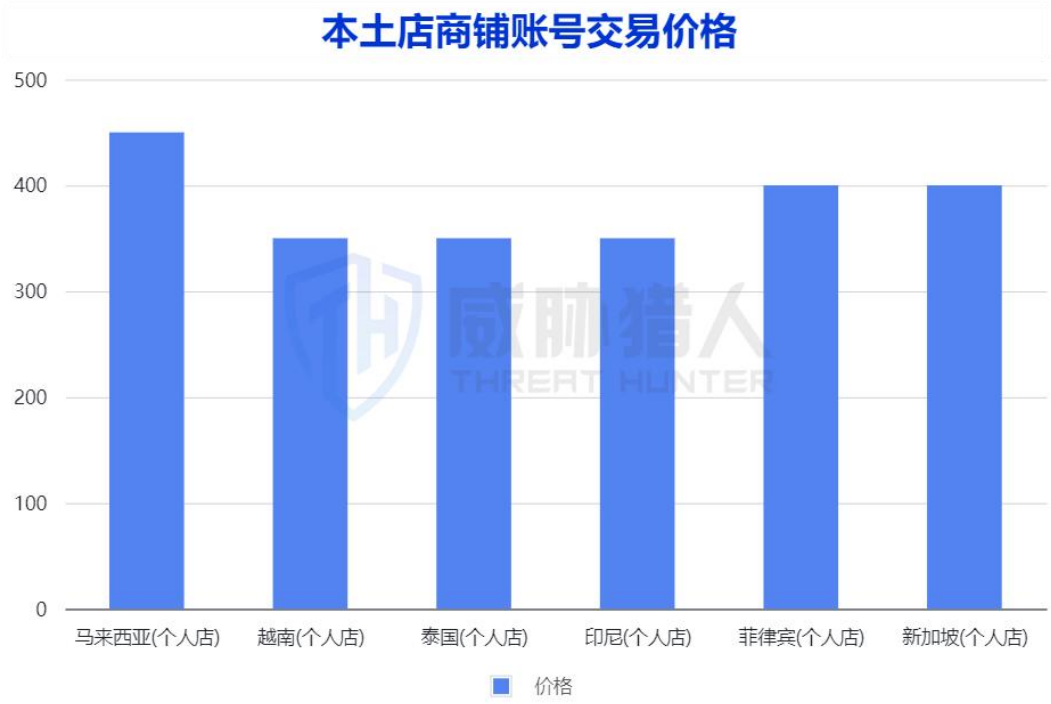
2.1.3、卖家账号交易风险

卖家账号交易风险是指黑灰产通过批量注册和众包等手段获得了通过实名认证的账号，并将其直接出售给想要入驻平台的用户，从而达到绕过入驻门槛的目的。

（1）账号交易根据每个平台的账号类型，有各种类型的店铺出售

如：某商家成品号交易的账号类型主要有：跨境店账号、本土店账号、品牌店账号，其中品牌店价格最高，需 3000 元。这主要是因为品牌店的资质不容易获取，入驻流程繁琐，审核严格，导致价格比较高。其他的本土店和跨境店的价格在 300-450 元之间。同时，不同的国家之间的本土店铺价格也不一致。

（2）本土店商铺账号交易价格表，如下图所示。



2.2、店铺刷单风险分析

店铺刷单一般指平台卖家付费委托刷单黑灰产，通过刷单工具、真人刷手向指定的平台卖家购买商品、填写虚假好评来提升店铺销量、信用度和评分，获取平台流量的欺诈做法。

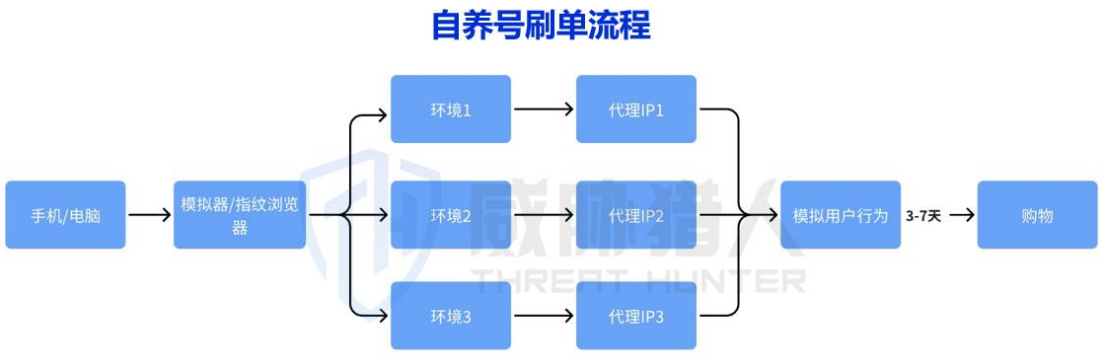
店铺刷单不仅误导消费者的购物决策，还容易引发店铺不公平竞争，严重影响平台的正常运营。海外电商平台对刷单作弊行为长期进行风控，刷单群体防风控意识随之增强，以往常见的机器刷单消失殆尽，目前主要提供的刷单服务类型有两种：自养号刷单和真人刷单。

(1) 自养号刷单：通常指商家利用指纹浏览器购买海外服务器、IP 搭建刷单环境，实现批量注册目标平台账号、养号、浏览模拟以及下单的行为。

(2) 真人刷单：指黑灰产通过雇佣真实用户伪装正常消费者的方式在电商平台上进行虚假交易的行为。这些“刷手”通常会按照黑灰产的要求，使用真实身份信息、支付方式和地址，在电商平台上完成购买商品的流程。

2.2.1、自养号刷单

自养号刷单在国内的使用相对较少，但在海外电商的操作中却十分常见。这类行为通常以线上线下教学的形式传授技术，黑灰产提供一系列教程和工具，帮助用户搭建自建服务器和刷单环境。通过这些资源，用户可以完成账号注册、养号、下单等一系列操作。因此，自养号刷单目前已经形成了一套完整的刷单流程。



(1) 自养号技术孵化分析

威胁猎人发现，自养号的产业链比较完善，有测评技术孵化公司专门出售教程技术。从整个自养号产业链来看，刷单的利润由汇率差价+礼品卡差价+刷单佣金组成。具体流程如下。

① 测评技术孵化公司提供：海外手机号、全套身份信息、礼品卡、跑水单号、IP、防关联浏览器；

② 黑灰产使用自养号刷单的收益由三部分组成，即 总利益 = 汇率差价 + 礼品卡差价 +

刷单佣金。

(2) 自养号刷单典型工具分析

黑灰产为了实现多账户统一管理，并且隔离环境，稳定的 IP 线路，普遍会选择“指纹浏览器”作为多开店铺的环境基础，指纹浏览器可以保障每个浏览器实例在一个隔离的环境中运行 ，也就是说每个账号都在一个独立的浏览器中运行，避免账号之间被关联和封号风险。

威胁猎人抽取 9 款指纹浏览器，对它们的平台登录方式、IP 维度使用情况、浏览器设置、环境的使用方式进行分析发现：

a. 登录平台的方式：分析发现，指纹浏览器支持自动登录的范围已覆盖 100 余家电商平台、支付平台、邮箱。其他不支持自动登录的平台，也可以在新建浏览器后，自行手动登录。

b. 使用的 IP 维度：通过分析 9 款指纹浏览器发现，共支持 58 个动态 IP 代理平台和 12 个云服务器厂商，其中指纹浏览器支持最多的云服务器平台是亚马逊云，共有 5 个指纹浏览器支持使用，其次是阿里云和腾讯云，有四个指纹浏览器支持使用。

c. 可选择配置的浏览器设置：

- 浏览器内核版本（可选择具体的版本号）
- 操作系统（可选择：windows，mac OS， linux，Android， IOS）
- UA 设置（可设置版本号、User-Agent）
- WebRTC 设置（可设置隐藏真实 IP）

- 地理位置（可设置跟随代理 IP 的地理位置）
- 窗口尺寸、分辨率、字体
- 端口扫码保护
- 媒体设备指纹设置：视频输入、音频输出、音频输入
- 硬件设备设置（设备名称、MAC 地址、CPU 核心、设备内存）

d. 环境使用方式：有两种使用方式：

- 直接打开浏览器，新建环境进行可视化页面使用；
- 用 api 接口的方式使用环境。

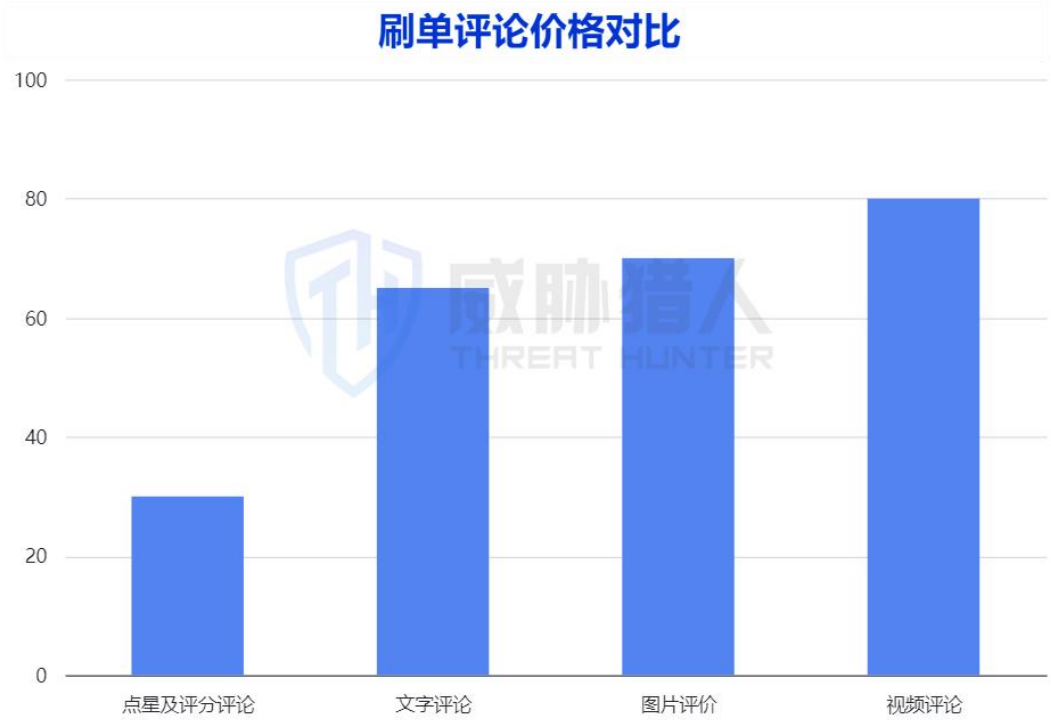
2.2.2、真人刷单

（1）刷单手法

黑灰产刷单手法如下图所示：

（2）刷单价格

威胁猎人调查发现，价格的主要影响因素是评论的内容类型和区域，目前共有四种评论内容：点星及评分评论、文章评论、图片评论、视频评论。以某一区域价格为例，视频评论的价格最高需要 80 元。点星及评分评论的价格最低只需要 30 元。价格对比如下表所示。



2.3、物流作弊风险分析

物流作弊指电商卖家使用虚假发货单或科技快递单发货，以实现偷区、偷重或逃税，降低销售成本。物流作弊一旦被物流公司查到，货物可能会被扣押，卖家还需补交运费，不仅严重延误商品的交付时间，还会降低用户对平台的信心。此外，卖家还可能利用虚假单号刷单，以获得平台的物流补贴和价差福利。

目前市场上主要的作弊物流单号有三种类型：二次单号、跑水单号、科技单号。

（1）二次单号，指物流单号被泄露或被物流公司售卖再次使用。

a. 出售渠道：黑灰产通过单号售卖网站进行出售或通过私域渠道进行对接。

b. 使用条件：可通过发货时间、收货地址、发货地址，邮政编码，甚至收货时间进行匹配对应的单号。

c. 更新数量：以美国物流单号为例，在单个出售单号网站上，每天大约会更新超过 4000

个单号。

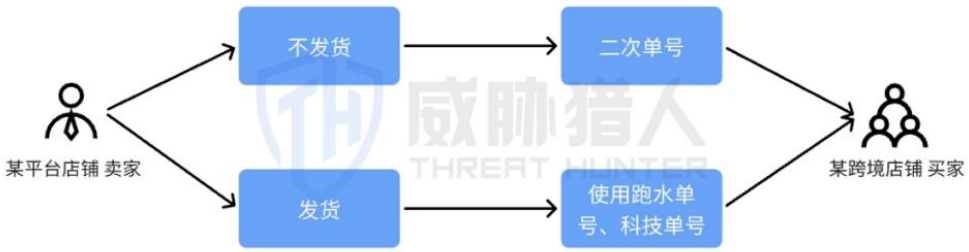
（2）科技面单，指黑灰产破解面单生成规则后自己生产的快递面单，这类面单可以被部分单号扫描仪正常识别并可在官网上查询对应的物流单号与物流轨迹。

a. 现状：尽管经过美国邮政多次升级和打击，市面上流通的这种面单数量已经减少，但仍有一些黑灰产声称还有可用的面单号码。

b. 使用条件：通过实际地址进行打印单号，进行实际发货。

（3）跑水单号，指使用跑水账号打单的面单。面单本身是正规单号，但是由于关联的打单账号拖欠运费或是使用盗刷信用卡来支付运费，导致该账号关联的所有单据和仓库面临货运风险，从而造成损失，并且有一定概率受到处罚。

a. 使用条件：根据实际地址打印单号，进行实际发货。



2.3.1、物流单号价格

在以上三种作弊物流单号类型中，科技单号的售价最低，仅需 0.6 元就可以购买，这主要是因为科技单号是通过破解单号规则获取，单次成本比较低。其次是二次单号，平均 2.56 元/单，二次单号通过发货时间、收货地址、发货地址，邮政编码等信息匹配单号。最高为跑水单号，平均 10 元/单，跑水单号需要有真实收货地址进行发货，价格还会根据商品的规格大小、重量产生波动。

2.4、商品信息爬取风险分析

商品信息爬取风险指未经授权的爬虫程序在电商平台或网站非法获取平台上的商品信息的风险。该行为可能侵犯版权或知识产权，也可能导致平台或商家敏感数据泄露，亦可通过对特定商品进行浏览器刷量的操作，扰乱正常的市场秩序。

上游黑灰产主要通过社交平台和二手交易网站发布与赚钱相关的帖子，诱导用户使用挂机工具进行电商平台商品数浏览并采集数据。用户采集到一定数量的数据后，便会进行统一结算。例如在某电商平台上，采集 1000 条数据可以获得 7 元的佣金。

相关工具出售情况示例：

2.5、恶意退款风险分析

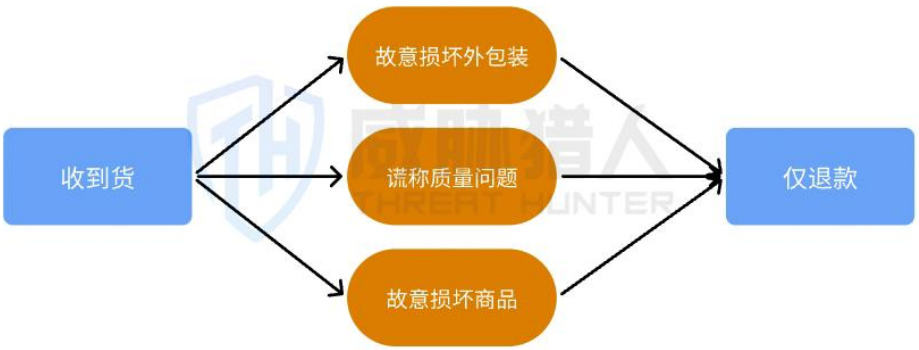
恶意退款指用户通过不正当手段申请退款，从而获取不应得的利益。这种行为会对电商平台和商家造成经济损失和其他负面影响。

常见的恶意退款行为包括：

（1）虚假声明商品未收到：用户声称未收到商品，实际却已经收到，以此要求退款；

（2）谎称质量问题：用户收到商品后，谎称商品有质量问题或与描述不符，要求退款或部分退款，同时保留商品；

（3）故意损坏商品：用户收到商品后故意损坏，再以商品有瑕疵为由要求退款。



黑灰产会通过群聊和教程的方式传播恶意退款方法，如：在黑灰产网站上出售退款教程。

2.6、认证绕过风险分析

认证指确认用户的身份，以确定其是否有权访问和使用特定资源。在电商平台上，认证主要用于确认卖家是否具备开店的资格，保证店铺正常运营。然而，黑灰产为实现批量开店的目标，往往会尝试绕过身份认证。

认证绕过指黑灰产在电商平台身份认证过程中，利用某些技术手段或采用不合规的方法，逃避认证的行为。

2.6.1、认证绕过的方法和技术

（1）真人绕过

黑产在利用真人众包进行账号注册时，会与众包人员签订合同或协议，要求他们在遇到认证环节时协助完成认证流程，以实现绕过认证的目的。

（2）图片合成绕过

图片合成绕过是指黑产利用技术手段将照片合成一段视频，当平台要求进行认证时，直接将合成的视频上传到平台，从而绕过真实认证的要求。

真人绕过和图片合成绕过手段主要应用在账号二审阶段，在这阶段需要认证的是卖家账号的人脸信息。

（3）摄像头绕过

目前发现的摄像头绕过共有两种类型，分别是：1.虚拟摄像头绕过；2.摄像头劫持绕过。

a. 虚拟摄像头绕过

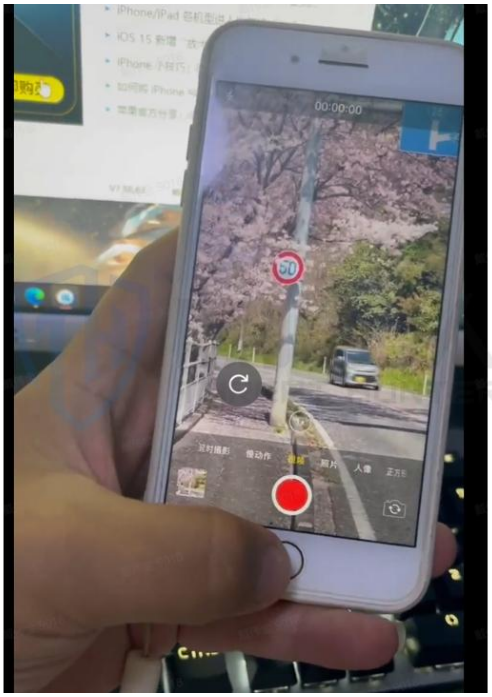
虚拟摄像头绕过指黑产使用虚拟摄像头软件来替代电脑自带的摄像头。通过这种方式，可以将录制好的视频作为实时视频流传输，达到绕过认证的效果。

案例：此案例通过硬改 XCMS 工具基于修改系统驱动，使得虚拟摄像头在系统中被识别为真实摄像头。通过这种方式，软件和平台在调用摄像头时，会误以为连接的是真实摄像头，从而接受其输入。

b. 摄像头劫持绕过

摄像头劫持指黑产通过获取手机的 ROOT 权限，安装特定的软件或插件，提前录制好视频后将其自动加载到这些软件或插件中。当平台进行认证时，手机上的软件或插件会使用录制的视频进行认证，从而绕过风控措施。摄像头绕过作恶的应用场景为电商直播和引流场景。

案例：此案例通过某 app 结合苹果 6s 版本以上的手机操作实现，如下图所示，将相机实时拍摄的信息更换成提前录制好的视频信息。



2.7、内外勾结风险分析

内外勾结指黑灰产与平台内部人员秘密勾结，通过不正当的行为，达成非合规入驻平台、解封账号等目的。

在电商场景下，内部勾结通常出现在以下三个场景：招商邀请码入驻平台、店铺账号保证金强提、店铺账号解封。

（1）招商邀请码入驻平台

招商经理将平台发放的邀请码，高价出售给想要入驻平台的用户，或者勾结黑产直接出售邀请码以获取利益。通常情况下，招商邀请码的价格较高，威胁猎人最近捕获的案例显示，某个电商平台邀请码的售价高达 80,000 元人民币。

（2）店铺账号保证金强提

店铺账号保证金指卖家在平台注册时需要缴纳的一定金额，以确保店铺能够正常运营，如果账号出现违规行为，保证金可能会被封禁，电商平台一般禁止提取保证金。然而，一些黑产

通过和内部人员勾结，能够强行提取这一保证金，通常收取的费用为保证金的 30%左右。

（3）店铺账号解封

店铺账号被封是指卖家因为操作不当或违规而触发平台风控规则，被封禁账号。然而，一些黑灰产通过和平台内部员工勾结，协助店铺解封账号。值得一说的是，这种店铺账号的解封并不绝对有效，当涉及虚假运输被封禁时，通常无法解除封锁。

另一种情况是卖家使用完平台提供的申诉机会(一般情况下,平台会给予用户两次申诉机会)仍不能解封，此时，不法分子也可能通过内部人员勾结，有偿协助卖家解封账号。

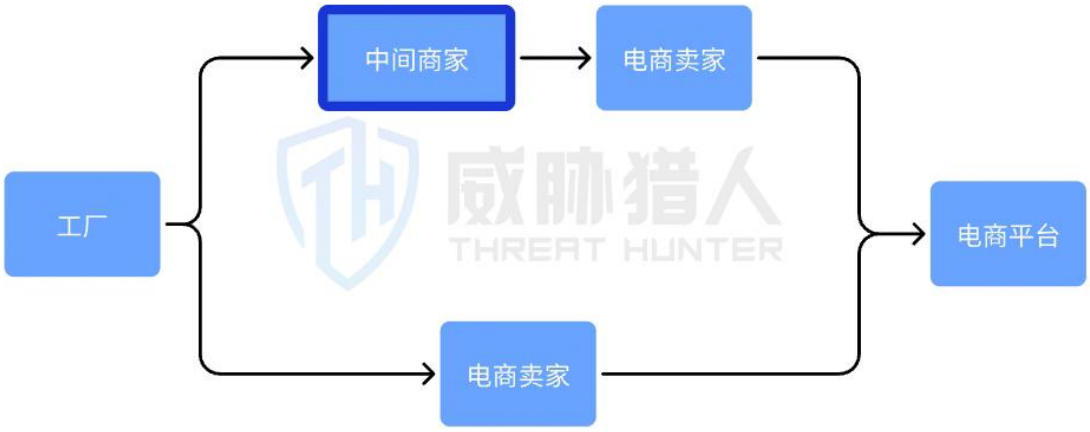
2.8、货盘风险分析

货盘指企业将商品批量运输并存储在境外仓库（即海外仓），以便快速配送和销售到当地或周边市场。然而，一些个人卖家担心货物运到海外后销售不佳，因此，他们会直接购买海外仓货盘，类似于国内的无货源模式。这样虽然可以降低卖家资金风险，但也容易导致商品质量问题和履约率下降的问题：

（1）低质量风险：货盘的货源主要来自工厂直接发出的低质量产品或滞销产品。这类货盘通常没有门槛，属于大众化货盘，往往是尾货、清仓货，或者因各种原因被下架的产品。这些产品存在质量隐患，容易引起消费者投诉。

（2）履约率下降：由于货盘由第三方管理，平台卖家无法直接控制货物的发货和售后，可能导致卖家履约率下降。

目前已发现有美国本土货盘、东南亚区货盘，涉及的商品类目包含有日用家居、数码 3C、五金用品、宠物用品等全品类。



三、结语

通过上述风险分析不难发现，海外电商正面临着日益复杂多变的风险环境，对平台而言，黑灰产攻击通常涉及网络攻击和营销欺诈，可能导致资金受损、消费者权益受侵犯。对企业而言，可能出现销售受阻、账户冻结、品牌被封等经营财务风险。

海外电商平台和企业需要时刻保持对黑灰产的警惕，不断提升技术能力和风险管理水平，在专业安全情报厂商的支持下，结合具体业务场景建立更加完善的安全防护和营销风控体系，从而能更全面地应对来自网络黑灰产的威胁，实现海外业务健康可持续发展。

威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

关注“威胁猎人”

深圳永安在线科技有限公司（品牌名：威胁猎人）

官方服务热线：400-809-3699

官方合作邮箱：marketing@threathunter.cn

官网地址：www.threathunter.cn