THREAT HUNTER RESEARCH

2025 Global E-commerce Fraud Risk Report

A global e-commerce study covering seller and buyer account abuse, promotion fraud, payments and criminal supply chains.

Original publication: 2026-02-02
Research team: Threat Hunter Research Team
Source report: 28 pages

Original report text

This text version is reconstructed based on the 28-page original PDF, retaining the report narrative, chapters and research scope; the cover, repeated table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

Preface

In the past year, Threat Hunter based on continuous monitoring of the global e-commerce cybercrime ecosystem intelligence system found that in 2025, cybercriminal groups are shifting from the low-level malicious activity mode of "single point violation and rule bypass" to a "full life cycle, modular, service-oriented" attack method that carries out continuous attacks around the platform business system.

In terms of overall scale, the number of cybercrime-related risk clues monitored in the global e-commerce field in 2025 reached 15 million, a year-on-year increase of 226%; a total of 1.6 million cybercrime ecosystem-related accounts have been captured, a year-on-year increase of 55%, and the risk scale has significantly expanded.

From the perspective of core evolutionary trends, e-commerce cybercrime ecosystem showed three structurally significant changes in 2025:

AI-driven “evidence industrialization”:

With the popularization of generative AI, key materials such as identity materials, complaint evidence, and logistics vouchers are shifting from manual customization to templated, scripted, and large-scale generation. This change has significantly improved the pass rate of cybercrime ecosystem in KYC review, appeal confrontation and after-sales links.

The risk of logistics fraud intensifies:

The risk of logistics fraud is not limited to a single fulfillment violation point used by sellers to avoid shipping costs, but has evolved into basic materials that simultaneously support counterfeit dumping and malicious refunds;

Realization of attack resources:

As the platform continues to strengthen its device and environment recognition capabilities, cybercrime ecosystem systematically introduces real humans to participate in malicious activity deeds, reducing fraud controls hit rates through real devices and real network environments, and improving the success rate of key links.

Based on the above findings, Threat Hunter released the "2025 Global E-commerce Fraud Risk Research Report". Relying on massive intelligence data and typical cases covering multiple regions and multiple platforms, it systematically presents the current development trend of cybercrime ecosystem in e-commerce from the macro-situation, full life cycle attack paths, key capability evolution and typical risk scenarios. It aims to provide e-commerce platforms and related industries with practical intelligence insights and fraud controls decision-making references.

1. Overall risk landscape of global e-commerce platforms in 2025

1.1. The scale of e-commerce cybercrime ecosystem risk clues jumped to 15 million, a year-on-year increase of 226%

In 2025, the Threat Hunter anti-fraud intelligence platform captured a total of 15 million pieces of e-commerce cybercrime ecosystem risk intelligence, a year-on-year increase of 226%, and captured 1.6 million related malicious accounts used by cybercriminal groups, a year-on-year increase of 55%.

4 In 2025, Threat Hunter will continue to strengthen the monitoring of cybercrime ecosystem activity outside China and the construction of localized intelligence sources, focusing on covering underground communities, trading channels and key active nodes in different countries and regions, gradually forming cross-regional, multi-language intelligence collection and analysis capabilities, and providing customers with core intelligence support that is more regionally oriented and can be researched and judged.

2024 vs 2025 E-commerce cybercrime ecosystem monitoring data comparison number (unit: 10,000)

2024 2025 2000+226% 1500-1500 Pulse Hunter 1000-ERT+55% Significant increase in the number of 500-1 information (10,000 pieces)

number of cybercrime-related entities (10,000)

1.2. Global e-commerce platform attack risks are highly concentrated in Europe, China and the United States.

The three major regions of Europe, China and the United States together contribute more than 70% of the world's e-commerce risk clues, forming the current core concentration area of global e-commerce risks. The above-mentioned areas are also the most important e-commerce economies in the world. Risk distribution and business volume are highly overlapped, which is in line with the basic law of "threat actors follow the money".

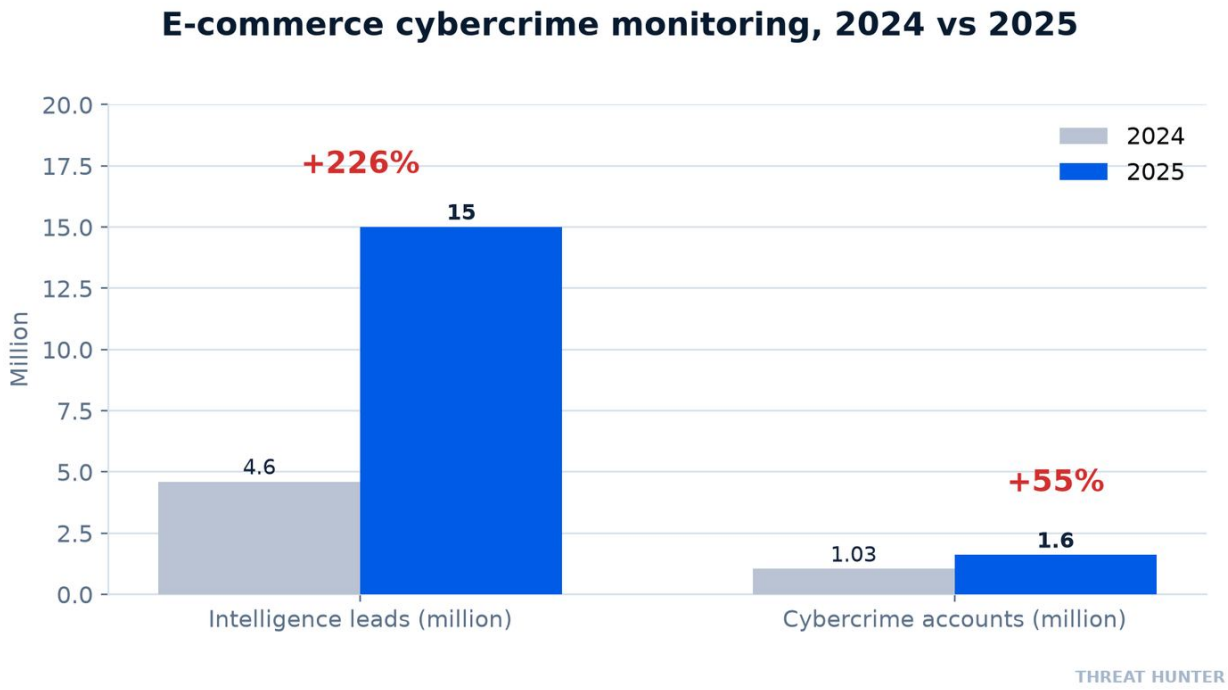
Global e-commerce cybercrime ecosystem monitoring regional distribution heat map (2025)

Europe: 26% United States: 22% China: 24% Middle East: 89 Southeast Asia: 6% Latin America: 13%

1.3. The cybercrime ecosystem operating model uses global channels to attract traffic and localized channels to close transactions.

In various key areas, cybercrime ecosystem generally adopts a two-tier operation model of "global channel traffic + local channel transaction": that is, threat actors first diffuse customers and traffic on global social platforms, and then transfer to local instant messaging tools, local forums and regional trading platforms to complete private domain undertaking, transaction matching and delivery closed loop.

In view of this cross-platform and cross-regional operational link, Threat Hunter simultaneously promoted the expansion of localized intelligence sources this year and strengthened its continuous acquisition and monitoring capabilities of key channels and active nodes in different regional ecosystems.



Observed e-commerce cybercrime intelligence leads grew 226% in 2025, and the number of associated entities grew 55%.

Source: Threat Hunter original report, page 2. Redrawn in English from the original figure.

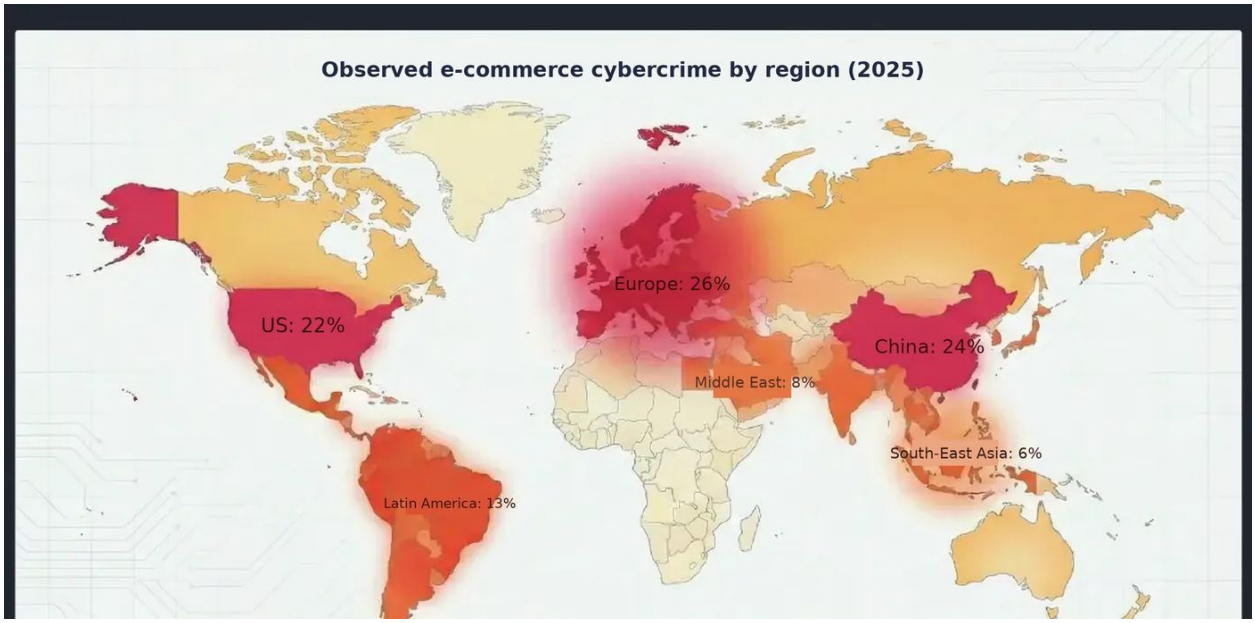
Localized intelligence source channel coverage structure (2025)

1.4 Buyer and seller account prices vary materially by platform and control threshold

Whether it is a seller account or a buyer account, there are obvious differences in pricing in the underground market, which is mainly affected by the region where the platform is located, the merchant hierarchy and the operating authority of the account. In essence, account prices reflect threat actors' reverse assessment of platform account access costs and fraud controls intensity: the more sensitive the regional attributes, account tier, and operating permissions, the higher the platform's fraud-control threshold, and the higher the pricing of the corresponding account in the underground market.

Seller accounts can exceed 10,000 yuan in underground markets, while buyer accounts range from below 1 yuan to around 1,000 yuan depending on platform, region, account tier and available permissions.

1.5 Global e-commerce fraud shows clear cross-regional patterns



Observed e-commerce cybercrime activity is concentrated in Europe, China, the US, Latin America, the Middle East and South-East Asia.

Source: Threat Hunter original report, page 3. Original figure with Chinese text replaced by English.

Global the cybercrime ecosystem activities show significant cross-regional and networked characteristics.

Relevant criminal gangs are no longer limited to a single country or region, but make full use of the borderless nature of the Internet to complete information collection and technology research and development in country A, and then carry out attacks and realize funds in country B, forming a chain of threat actors with clear division of labor and coordinated operation, and continue to target key global markets.

Global cybercriminal groups attack radiation situation map

For example: Threat Hunter monitoring found that in the cybercrime ecosystem group Back Fight Jcwmeon S qoi &roocp oobooboogGf Brapefryp:apo?

Some Burmese threat actors claimed that "through this method, can anyone have SKTBA every day? Let's get points stably. Just follow the steps to complete the adjustment. It is Burmese people who accuse daily activities of fraud. 0M5: 8.15-8.31%." Combined with the pictures it released, it can be seen that the App interface in question is in Japanese environment, indicating that the relevant cybercrime groups is participating in the activities and points tasks of Japanese apps across regions to achieve incentive arbitrage.

Similar patterns also appear in other regions, such as Vietnam's cybercriminal groups' cross-regional participation in activities in South Korea.

In addition, it was also discovered that cybercrime ecosystem in China collects coupons in batches for activities in the United States, claiming to produce 100,000 units per month.

The US coupons can be consumed as follows: You got $2, with a monthly output of about 100,000 u. Hecaive daity check n p.sh quoted the exchange rate~!

Localized intelligence-source coverage by region, 2025

Region	Localized intelligence sources
South-East Asia	Zalo; local Facebook groups; local WhatsApp groups; private Telegram groups; local marketplace (Carousell); local forums
Latin America	Local WhatsApp groups; private Telegram groups; local forums; local marketplace (OLX)
North America	Reddit; private Telegram groups; local WhatsApp groups; Facebook Marketplace; local forums
Europe	Private Telegram groups; local forums
Middle East	Local WhatsApp groups; private Telegram groups; local marketplaces (Haraj, OpenSooq)
Russian-speaking region	VK; private Telegram groups

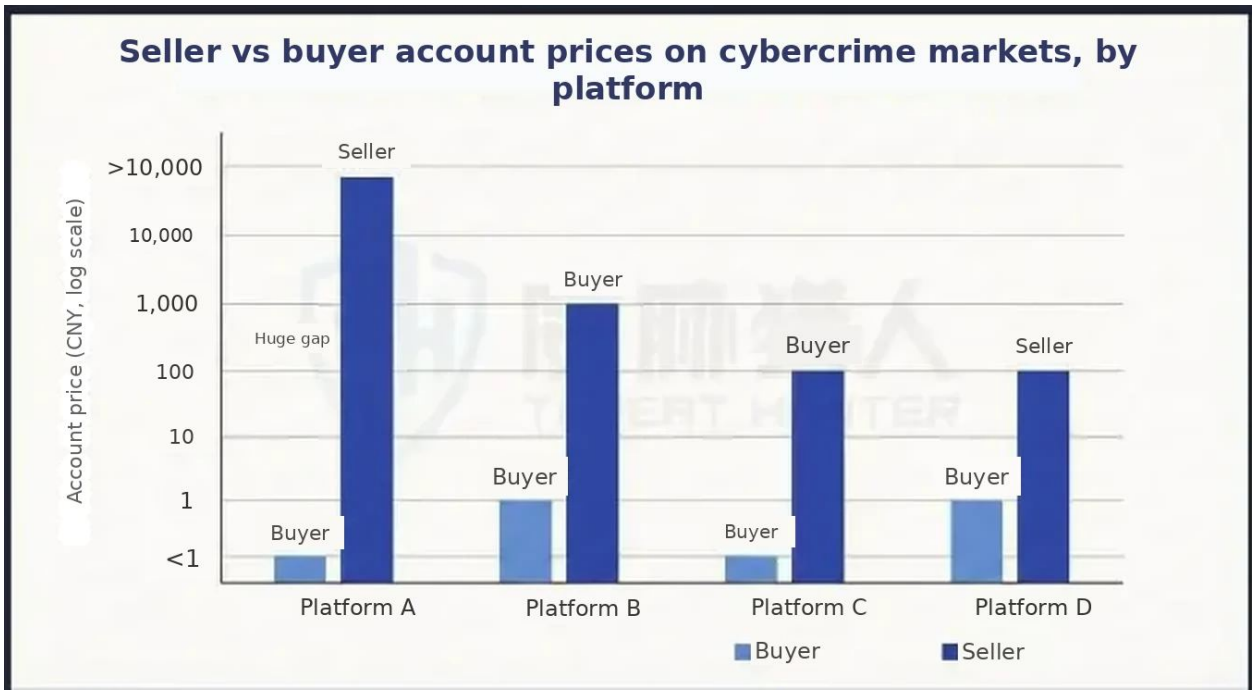
Each region relies on a different mix of localized intelligence sources, from messaging-app groups to local marketplaces and forums.

Source: Threat Hunter original report, page 4. Table re-typeset in English from the original.

US coupons. Is there any one with a high exchange rate?! PM me! Bring your own exchange rate quote. Communicate effectively!

2. Attack links of threat actors on global e-commerce platforms in 2025

Based on long-term monitoring and analysis of global e-commerce platform risks, Threat Hunter found that cybercriminal groups' attack methods against e-commerce platforms, whether on the seller's side or on the buyer's side, are deeply aligned with the platform's business processes. Based on this feature, this report takes the core business processes of the e-commerce platform as the main line, systematically sorts out the cybercrime ecosystem behaviors scattered in various business stages, and constructs a full life cycle attack map of cybercrime ecosystem against the e-commerce industry in 2025.



Seller-account prices are consistently higher than buyer-account prices, reflecting differences in access thresholds and operating permissions.

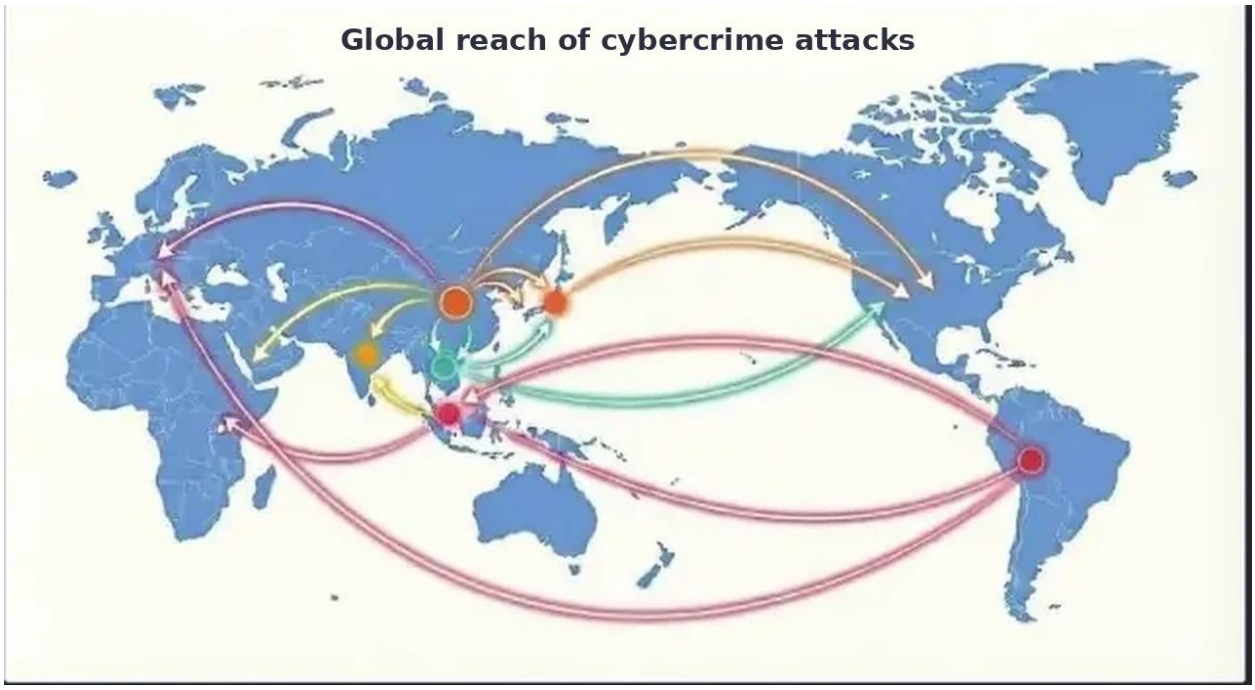
Source: Threat Hunter original report, page 4. Original figure with Chinese text replaced by English.

2.1. cybercriminal groups' high-frequency attacks on sellers in the e-commerce industry mainly focus on the three key links of account acquisition, illegal product supply, and transaction and fund settlement.

From the seller's perspective, cybercrime ecosystem high-frequency attacks in 2025 are mainly concentrated in the three key links of account acquisition, illegal product supply, and transaction and fund settlement. The overall characteristics are highly process-oriented, large-scale, and instrumental.

cybercriminal groups targets the full life cycle attack on sellers in the e-commerce industry. Map account risk Account Lifecycle commodity transaction risk order payment risk logistics fulfillment risk payment Abuse Bypassing the code/environment to fight against counterfeit and inferior product pallets, fake transactions, traffic manipulation AB orders, controlling evaluation, third-party collection and payment, store number sales, concealed counterfeit sales (replacement/passing off as good)

Benchmark Channel Technology Order Malicious Complaints about Competitive Products Virtual Currency Settlement - HkKYC Material Kit Automatically Listed/Follow-Sell Virtual Warehouse Dispute/Complaint Confrontation Deposit Forced Withdrawal AI Video Pass Inspection human participant Represents!



Cybercrime groups spread intelligence gathering, technical preparation, attack execution and monetisation across many countries.

Source: Threat Hunter original report, page 4. Original figure with Chinese text replaced by English.

Customized complaint materials for traffic manipulation orders/group control and diverting traffic

2.2. cybercriminal attacks buyers in the e-commerce industry with the goal of maximizing platform subsidies and product value.

From the buyer's perspective, cybercriminal groups have built a life cycle arbitrage system covering the entire business process around account numbers, platform subsidies, payment and after-sales rules. Its core goal is to maximize platform subsidies and product value.



Public evidence of cross-regional participation, supported by localized accounts, languages and operating environments.

Source: Threat Hunter original report, page 5. Original image retained.

cybercrime ecosystem Full life cycle attack map for buyers in the e-commerce industry Account Llccucie KiSKBUe account risk oaud a ransecon kisk Cuwen commodity transaction risk Favmene aouse Nsk tUwe order payment risk logistics fulfillment risk -ulnlmnencs. tueAfter-sales Risk | Buyer after-sales risk Batch registration Batch receipt of coupons or event rewards Credit card theft False collection After-sales rules Arbitrage Batch account transactions Swiping orders Virtual card capital refund False reporting Not received Malicious refund Account maintenance tool Group control order order line washing Malicious rejection Approval Refund Equipment environment Forgery Order first use, pay later Cash out Abnormal transfer refund No return KYC Forgery/Authorization Joint Luanxian platform subsidy FTID Refund Fraudulent account takeover/Jieku inventory occupation/batch cancellation AI Forgery picture evidence

2.3. 25 years of core risk evolution of threat actors under the full life cycle attack scenario

2.3.1. Use AI to generate key “evidence” through batch forgery

In 2025, with the development of generative AI, image synthesis, video face-changing and text generation capabilities, cybercriminal groups are moving key "evidence" such as complaint materials, identity materials and transaction vouchers from previous manual customization to large-scale production.



A sample showing bulk acquisition of US promotional coupons and discussion of downstream redemption channels.

Source: Threat Hunter original report, page 5. Original image retained.

Threat Hunter anti-fraud platform monitoring data shows that since Threat Hunter detected the number of cybercriminal groups related to AI face fraud in 2025, the number of cybercriminal groups surrounding AI face fraud has been growing rapidly, with the number of related groups rising from 116 in January 2025 to 361 in December (monitoring data only).

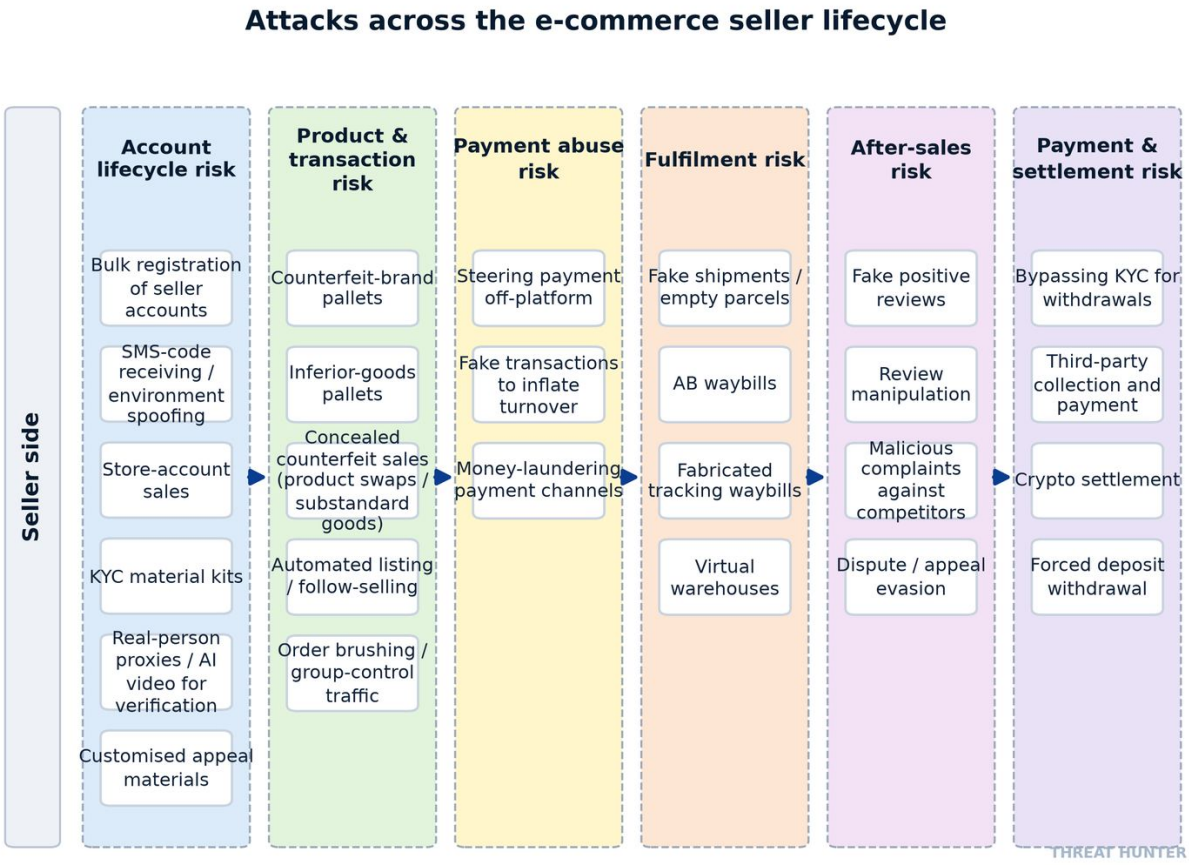
The rapid expansion of the size of this type of group means that related methods of using AI to commit fraud are being frequently discussed and exchanged by a large number of cybercrime operators.

meaning. .

From the perspective of the operating model, when the cybercrime ecosystem supplier can continuously provide "deliverables" such as face materials, KYC videos, and complaint evidence in the form of templates, scripts, and tool chains, the relevant threat actor organizations will quickly replicate in the form of groups.

On the attack path, the development of threat actors' methods of using AI to forge evidence directly improves the efficiency of confrontation in multiple key links, and the scope of influence covers both the seller and the buyer:

- Seller side: account registration, account appeal, product batch listing
- Buyer side: false registration, malicious refund, after-sales appeal In 2025, threat actors will use AI fraud techniques, which are mainly reflected in the following four aspects:



Seller-side risk spans the account, product, payment, fulfilment, after-sales and settlement lifecycle.

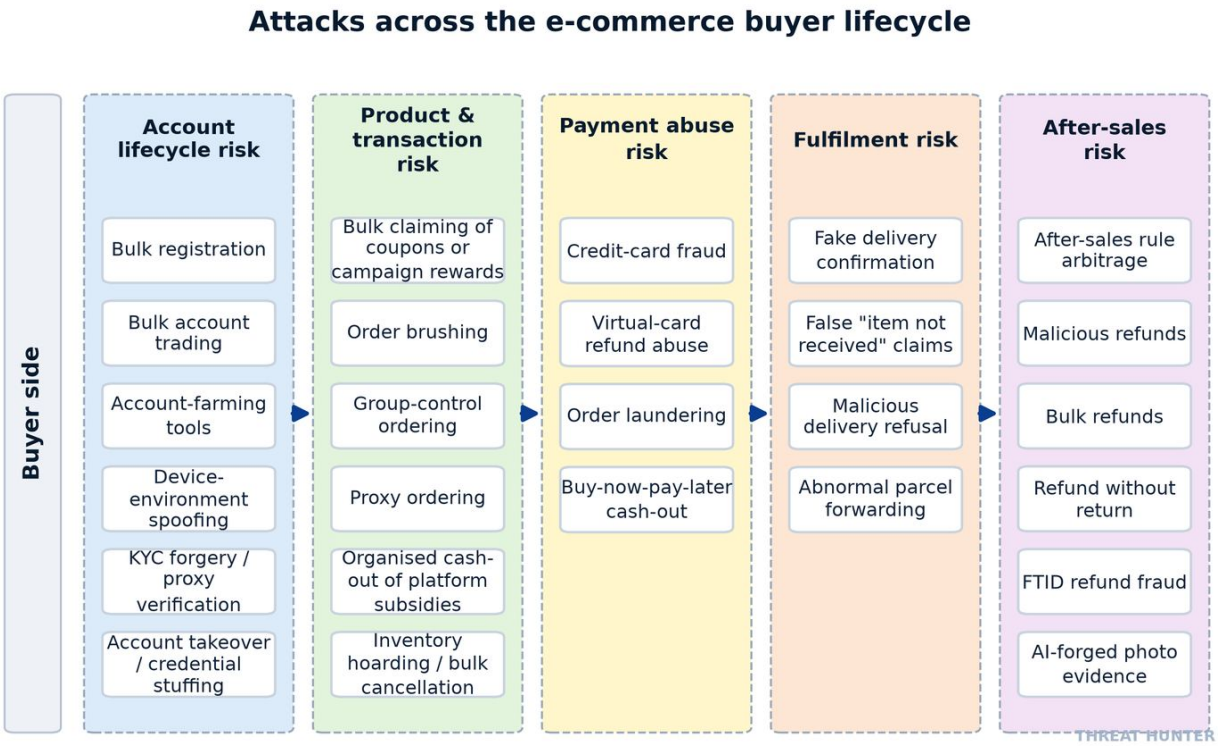
Source: Threat Hunter original report, page 6. Redrawn in English from the original figure.

1. Batch generation of identities through generative AI

2. cybercriminal groups use image generation and text synthesis

Text materials such as certificates and business certificates, combined with diagram capabilities, can automatically generate false logistics track snippets, add text, forge pictures, etc., and quickly assemble diagrams, transaction vouchers and chat records to improve the passing rate of false "certificate audits, appeals and after-sales confrontation" that can be used for appeals and audit confrontations.

The original AI-generated refund notification was successful at 05:41 pm. The actual refund for "use now, pay later" orders was 0 yuan.



Buyer-side risk runs from bulk accounts and subsidy arbitrage to payment abuse, false delivery claims and malicious refunds.

Source: Threat Hunter original report, page 6. Redrawn in English from the original figure.

Threat HunterMENER View details More news Undercooked/raw fishy smell

3. cybercriminal groups use video generation, face changing and language

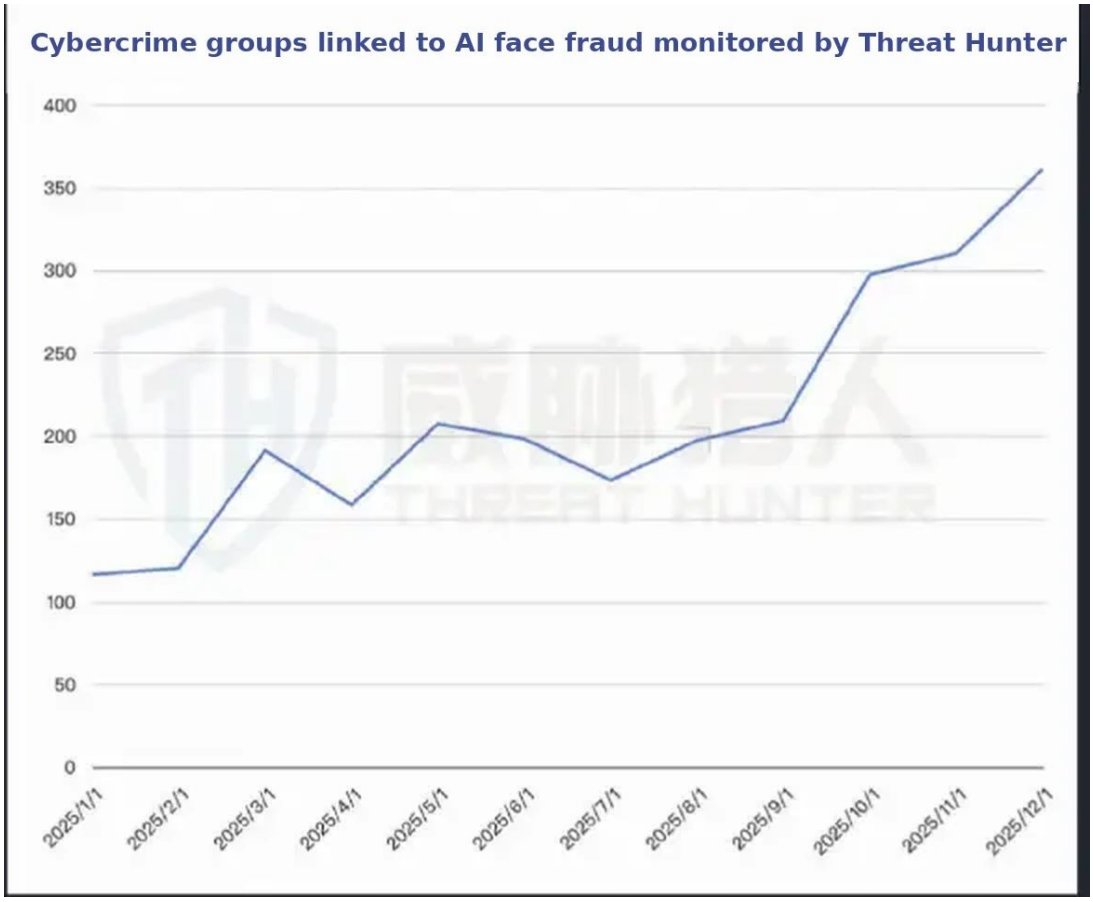
4. cybercrime ecosystem combines image generation capabilities with product automation

Audio synthesis and other technologies are combined with batch generation of KYC tools for online listing to quickly generate selfie videos and face verification materials that comply with platform certification and appeal review, thereby resisting product pictures of identity verification and review rules, and passing one-click fraud controls.

The operation is completed and put on shelves in batches, thereby bypassing content review and manual sampling inspections in a short period of time, and amplifying the distribution efficiency of illegal products.

Tools to improve your workflow.

2.3.2. The risk of logistics fraud intensifies



Cybercrime groups linked to AI face fraud monitored by Threat Hunter rose from 116 to 361 during 2025.

Source: Threat Hunter original report, page 7. Original figure with Chinese text replaced by English.

In the global e-commerce attack situation in 2025, logistics fraud is evolving from a "contract performance violation problem" in the traditional sense to a cross-scenario and cross-chain basic attack capability. It no longer exists independently as a single risk point, but is deeply embedded in high-risk scenarios such as brand counterfeit pallet sales and malicious refunds, and has gradually become an important basic supporting material for cybercriminal groups' large-scale malicious activity.

Judging from monitoring data, the risk of logistics fraud continues to intensify. As of the end of 2025, relevant fraud techniques have covered sites in at least 14 countries and regions, spanning many core e-commerce markets in Europe, America and Asia-Pacific.

The fundamental reason why logistics fraud can become a "basic material" is:

Logistics information plays the dual role of proof of contract performance and basis for after-sales judgment in the e-commerce platform.

In the dumping scenario of brand counterfeit pallets, the counterfeit brand pallets cooperate with the fake warehouse capabilities to enable counterfeit goods to be quickly distributed on multiple platforms and multiple accounts, and to realize centralized monetization before the account is banned; in the after-sales stage, cybercrime ecosystem further forges the return logistics track (such as FTID) and uses the platform's system judgment logic for the "return completed" status to

trigger the refund process when the goods are not actually returned, ultimately resulting in a high-risk result of "lost payment for both goods."

Logistics fraud presents different risk manifestations on the seller's side and the buyer's side, bringing different risks at key business nodes:

- Seller’s side: commodity transaction risk, logistics performance risk



Generative AI is used to produce identity documents, logistics evidence, KYC videos and product images at scale.

Source: Threat Hunter original report, page 7. Original figure with Chinese text replaced by English.

- Buyer’s side: malicious after-sales risk

In 2025, logistics fraud-related techniques showed significant changes in efficiency, mainly reflected in the following three aspects:

1. Through pre-internet, pre-scanning, virtual warehouse, AB order, technology order, etc., create "already-made goods" in advance in the platform system

"Delivered/Received/Local Performance" status enables the platform to see a complete and compliant fulfillment link when fraud controls intervenes.

920019039988uracking Numben0 copyAdd to Informed DeliverExpected Delivery byWEDNESDAY15~9:00pm1uspS Trackna Plus

2. Brand counterfeit pallets and fake warehouses enable brand counterfeit goods to be quickly distributed on multiple platforms and multiple accounts.

amount, and complete the centralized realization before the account is banned.

1. Front-end destination-market warehouse

2. Virtual destination-market warehouse

One box of salt, one imitation pallet, physical warehouse in the destination market, local delivery, fast buyer, China direct mail shielding tube, tracking destination port, local trajectory shows that the boss uses physical screens to blur the source of goods, disguised as the core: physical disguise. The core of real inventory in the destination market, cross-border tracking routes, and manufacturing goods that have been shipped domestically is address camouflage. No physical inventory, blocking "local sellers" from carrying out large-scale shipments and circumvents direct mail restrictions

3. Pre-scan fraud

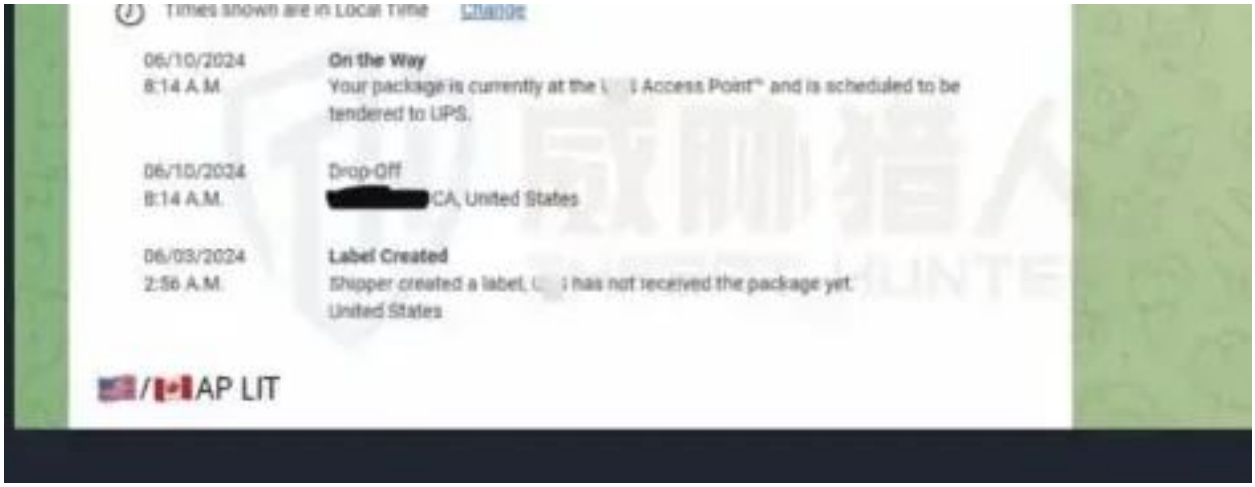
4. AB waybill fraud

,Lingyi Canfa goods have not moved black market scanner platform system: B waybill has been collected (true)

The core of the actual delivery of goods: timeliness fraud. Before the goods are moved, the counterfeit goods are evaluated (perfect trace and receipt), and the core of B waybill is posted:

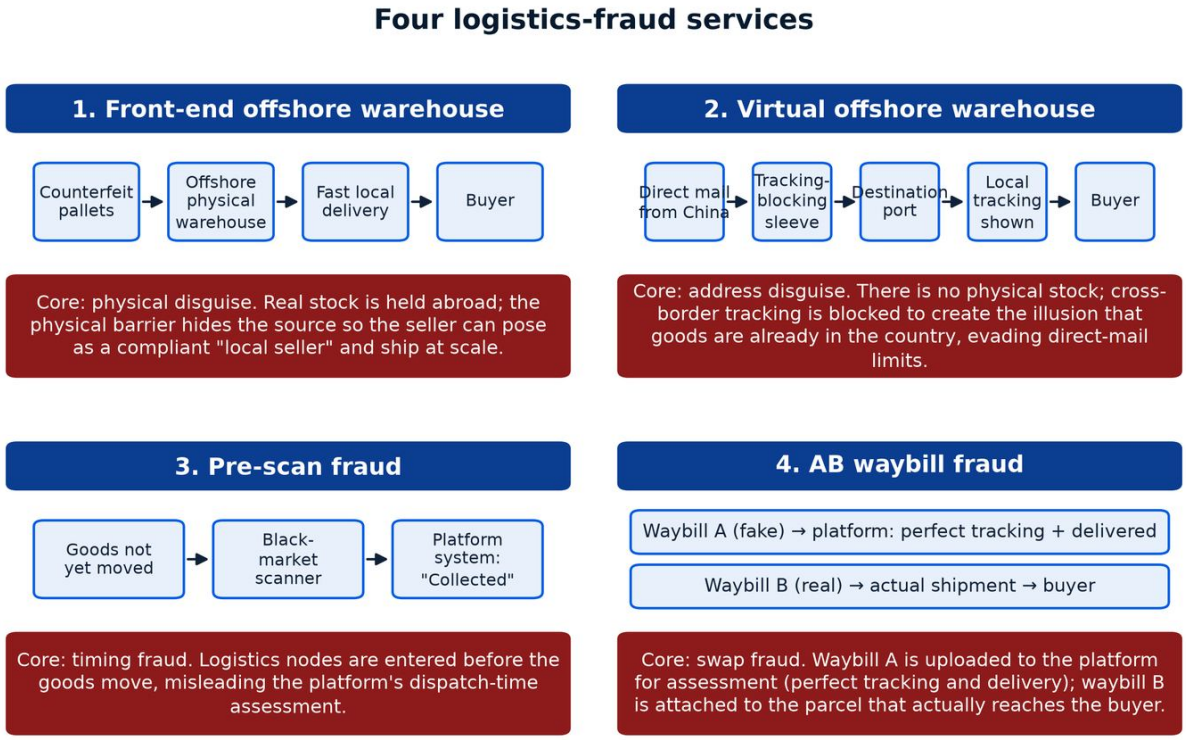
Subcontract fraud A waybill is uploaded to the platform and entered using flow nodes to deceive the platform into delivering timely assessments. Attached packages are used for actual delivery to buyers. Summary: These four services assist illegal sellers to disguise the logistics fulfillment process, circumvent platform fraud controls and obtain false compliance identities.

3. By forging the return logistics track (such as FTID), cybercriminal groups can target the platform’s system judgment logic of “return completed”.



Fake refund tracking exploits the platform's reliance on logistics checkpoints to trigger refunds without the goods being returned.

Source: Threat Hunter original report, page 9. Original image retained.



Summary: these four services help non-compliant sellers disguise fulfilment, evade platform risk controls and obtain a false compliant identity.

THREAT HUNTER

Virtual offshore warehouses, pre-scanning and AB waybills separate compliance in the platform system from real logistics.

Source: Threat Hunter original report, page 9. Redrawn in English from the original figure.



Pre-entry and pre-scanning create logistics checkpoints visible to the platform before the goods physically move.

Source: Threat Hunter original report, page 9. Original image retained.

Editing, completing the refund process without actually returning the goods, resulting in a high-risk result of "losing both money for the goods".

8:14A.M.

06/10/2024.

Your package is currently at the L ; Access Point" and is scheduled to beOn theWaytendered to a parcel carrier,8:14A.M.

JCA, United States2:56 A.M.

06/03/2024Shipper created a label, L ihas not recelved the package yet.

United States ILNTE country/bar IAP LIT

2.3.3. Real-life attack resources

As e-commerce platforms continue to improve their ability to identify virtualized devices, fingerprint browsers, and abnormal IP behaviors, automated malicious activity models that rely solely on technical tools are facing problems of declining marginal returns and fraud controls. In this context, cybercriminal groups began to systematically introduce attack resources involving real humans, promoting the evolution of attack resources from "machine-driven" to "human-driven".

This type of “human-in-the-loop crowdsourcing” model has penetrated into many key nodes:

- Seller side: Use human participants to register seller accounts, human participants perform KYC/qualification certification on their behalf, and human participants complain and communicate account bans and appeals
- Buyer side: Account maintenance behavior, human participants place orders on their behalf. In 2025, the risks related to human-operated fraud are mainly reflected in the following two aspects:

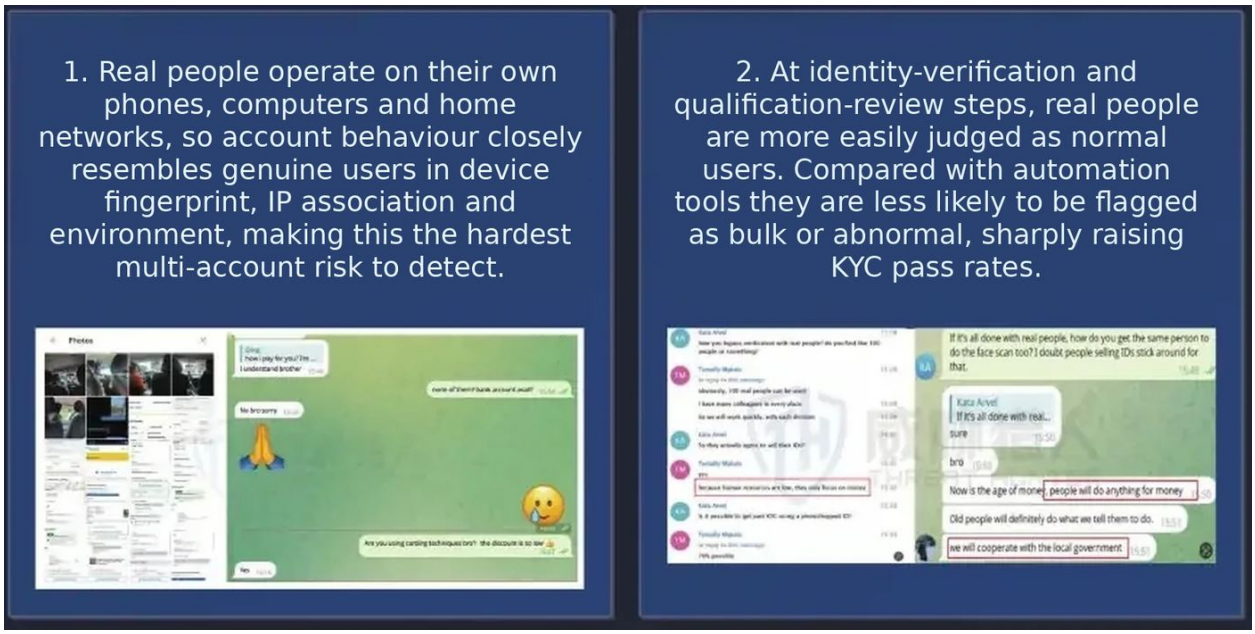
human participants using personal cell phones, computers and home networks

2. Key issues involving identity verification and qualification review

The network operation makes the account behavior in the device control link, and the human-operated operation is more likely to be judged as normal, which is highly connected to the user behavior at the level of pattern, IP association and usage environment. Compared with automated tools, human participants are closer to real users, making it difficult to identify batches or abnormalities in current multi-account management, greatly increasing the risk that is most difficult to identify.

Increased KYC pass rate.

ith human participants? do vou find lie 100If it's all done with human participants, how do you get the same person todo the face scan too? l doubt people selling IDs stick around for15:49hve mny colleaoues in every placKata Arvel|sureIf its all done with real..



Real-person proxies use genuine devices, home networks and identities to lower the chance that bulk attacks are detected.

Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

15:50bro 15:50Now is the age of money, people will do anything for money

3. Evolution of typical risk scenarios of e-commerce business fraud

The risks of counterfeit goods, malicious refunds, marketing arbitrage and logistics fraud covered in this chapter are not risk types that exist independently of each other, but are a form of monetization services that are systematically packaged and combined in the e-commerce system by cybercrime ecosystem around the four key business nodes of supply, account number, fulfillment and after-sales.

As relevant capabilities continue to mature, the above-mentioned risks are evolving from single-point violations in the past to systemic confrontations that are linked and operated collaboratively across links.

3.1. Risk of brand counterfeiting: standardized pallet system that can be replicated on a large scale

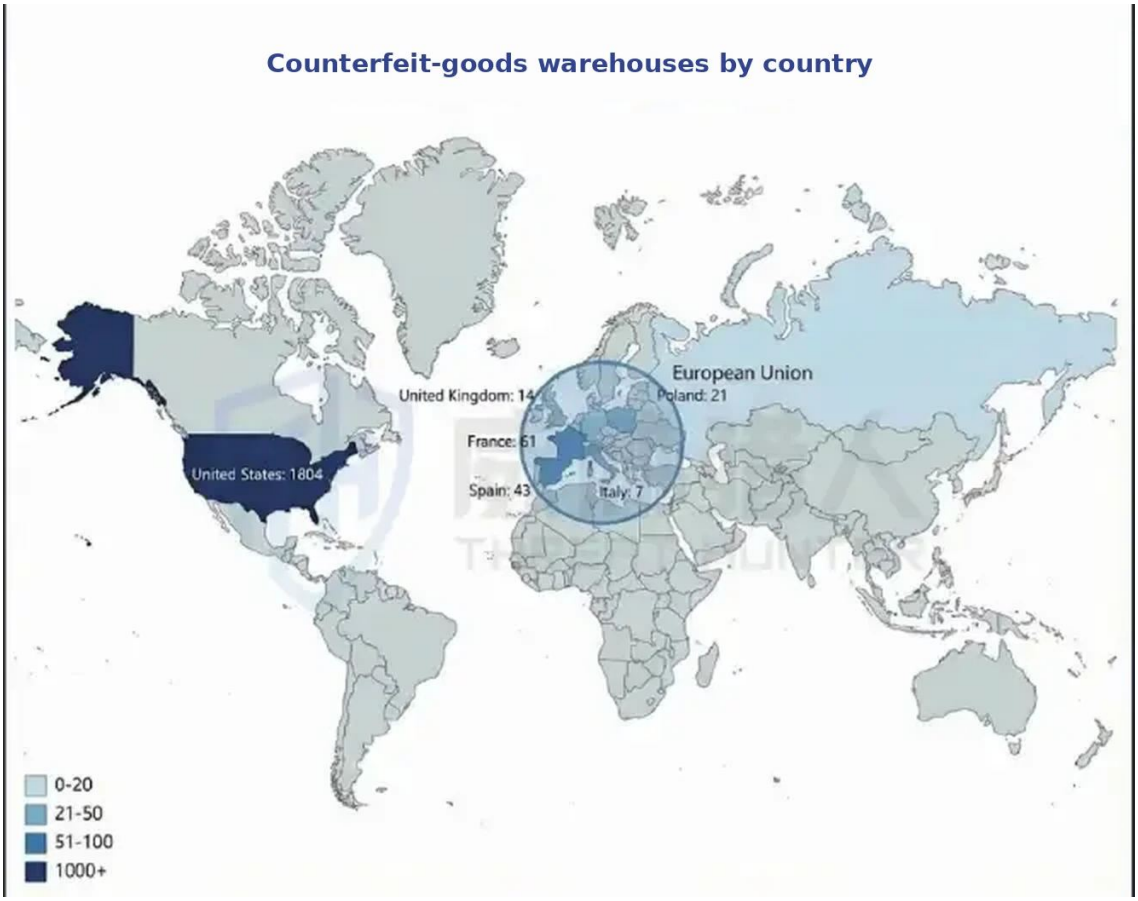
3.1.1. Global distribution and scale characteristics of brand counterfeit pallets in 2025

1. Counterfeit pallets are stocked in warehouses across many European and American countries.

We sampled 6 brand counterfeit pallets and analyzed the information of nearly 2,000 counterfeit goods that are still in stock, revealing the current serious situation caused by brand counterfeit pallets from the tip of the real iceberg.

Based on this counterfeit goods data, we can see that many counterfeit goods are distributed on pallets in destination-market warehouses. threat actors regard the US market as an important target market alone, and the European market is also a highland for dumping. Due to the smooth regional circulation, showing a typical agglomeration of EU countries, the key attack markets for European pallets in the European Union are the United Kingdom, Italy, Spain, Poland and France. threat actors also revealed the coverage of support orders if there are buyers in the EU.

0-2021-50



Sampled counterfeit-goods warehouses outside China were mainly in the US and several European countries.

Source: Threat Hunter original report, page 11. Original figure with Chinese text replaced by English.

2. Counterfeit products are mainly concentrated in the daily consumption areas of international big brands.

The counterfeit pallet category mainly covers the four major consumer fields of shoes, clothing and bags, beauty and personal care, electronics and digital products, and health care products. The common features of these categories are: they are all high-unit-price counterfeit products of international brands, with high customer unit prices, high brand premiums, and high repurchase potential.

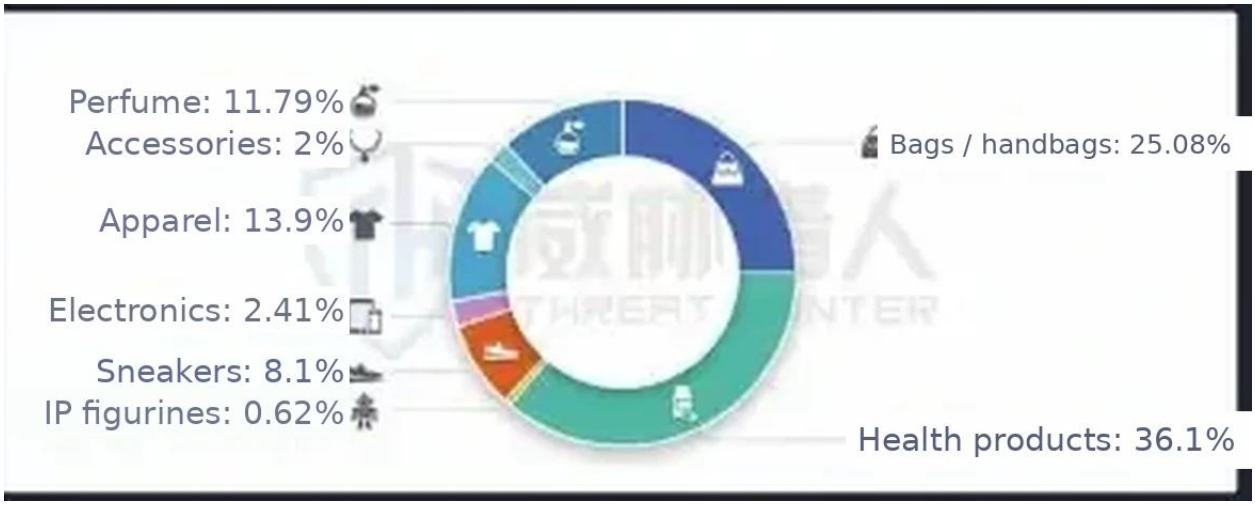
Among them, the counterfeit health products are all sensitive perfumes of all e-commerce companies: 11.79%. 2 items, which are directly linked to the health problems of platform buyers. They are also passed through accessories: 2%, color luggage/handbags: 25.08%, clothing: 13.9%, and flow into the market through the systems of major e-commerce companies. At the same time, in this data, we also see that threat actors are closely following the trend of consumption. Trendy

shoes: 8.1%, popular figures/IP figures: 0.62%, health products/health products: 36.19 points, and imitations of popular IP figures are also among them.

3. Large-scale brand infringement sites

It is not difficult to see that each category is catering to the current high-consumption L FAKE large-scale brand infringement scenario. Ranking of counterfeit brands by category UINFRINGEMENT market trend, based on the 6 subcategories of bags, trendy shoes, clothing, perfumes, accessories and bags, Top 8 trendy shoes, Top 8 clothing, Top 4w"Seit Laven products, electronics and digital products, the current goods mPaFAEThhorth Face2 plate mainly supplies popular counterfeit brands such as perfume Top 8 8 Accessories Top7 electronic products Top3 below:

var" Chel & Apes

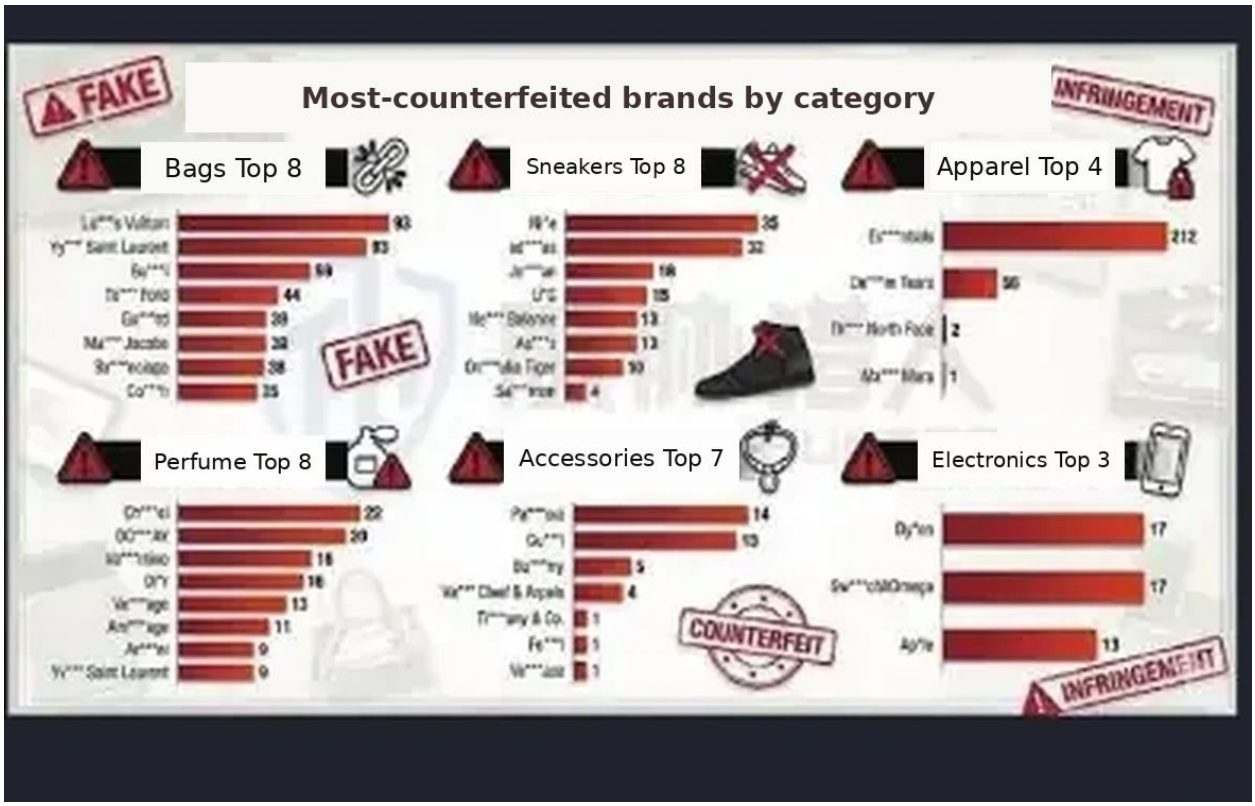


Sampled counterfeit pallets are dominated by high-value consumer goods such as health products, bags, apparel and perfume.

Source: Threat Hunter original report, page 12. Original figure with Chinese text replaced by English.

3.1.2. The gameplay of pallet threat actors is being fully upgraded.

As the platform continues to eliminate traditional brand counterfeiting and product distribution behaviors, cybercriminal groups have not shrunk. Instead, it has continuously evolved more covert and confrontational attack methods through the introduction of automated tools and algorithm capabilities.



Product categories and most-counterfeited brands in large-scale infringement, by category; brand names are masked in the original.

Source: Threat Hunter original report, page 12. Original figure with Chinese text replaced by English.

1. Adapt the counterfeit pallet model to the platform genes

threat actors understand the "genes" of the platform better than we do, and cybercriminal groups' attack strategies completely depend on the platform's business model and the level and preferences of the consumer group. They are not only selling goods, but also customizing differentiated attack scripts based on the platform's entry threshold, counterfeit identification mechanism, traffic distribution mechanism and even the preferences, concepts and psychology of local consumers to ensure large-scale profits.

The current target e-commerce companies for brand counterfeit pallets are mainly C2C second-hand transactions and B2C live-streaming e-commerce. The reason why this model can make large-scale profits under two different business models is that in addition to the characteristics of consumer groups within the model, the more important reason is that they have objective difficulties in the mechanism of identifying fakes. The former second-hand trading market has a "natural protective color" for low-price genuine products, while the latter's video streaming ecosystem will face more complex and diverse ways to bypass fakes.

Adapted platform type platform genes threat actors attack strategy large-scale profit method main governance cost

- Trust-driven rather than forceful review

Counterfeit strategies by platform type

Platform type	Platform traits	Attack strategy	How profit is scaled	Main governance cost
C2C second-hand marketplace	• Driven by trust rather than strict review • Low entry bar for individual sellers • Second-hand goods are naturally non-standard • Circular economy and sustainability are encouraged • Users hunt for bargains and "treasure"	• Pass replicas off as genuine items being resold • Fake traits: no box, no receipt, light wear • Pose as local individual sellers (nickname, avatar, location) • Hit-and-run listings: abandon stores on violation, rotate accounts • Deep persona building for high-margin, long-cycle sales	• Many low-cost accounts test quickly and pile up listings, then harvest in short cycles • High margin per sale: one order covers much of the cost	• Second-hand nature makes authentication hard • Physical collection or mandatory authentication curbs fakes but is very costly and slows platform growth
B2C social / live-stream commerce	• Content feeds and interest-based recommendations dominate • Videos outweigh product details • Influencer accounts carry very high weight; young audience • Impulse market where "anti-brand-premium" attitudes prevail	• Bait-and-switch videos present replicas as "same-factory dupes" • Buy or steal whitelisted influencer accounts to drive traffic to new stores or counterfeit links • Matrix live streams looping 24/7 via open-source streaming software	• Traffic bursts outpace review: matrix accounts spike a single product, harvest before risk controls act, then abandon the accounts	• Video content is hard to recognise in a structured way • The influencer ecosystem is turned against the platform; enforcement lags noticeably

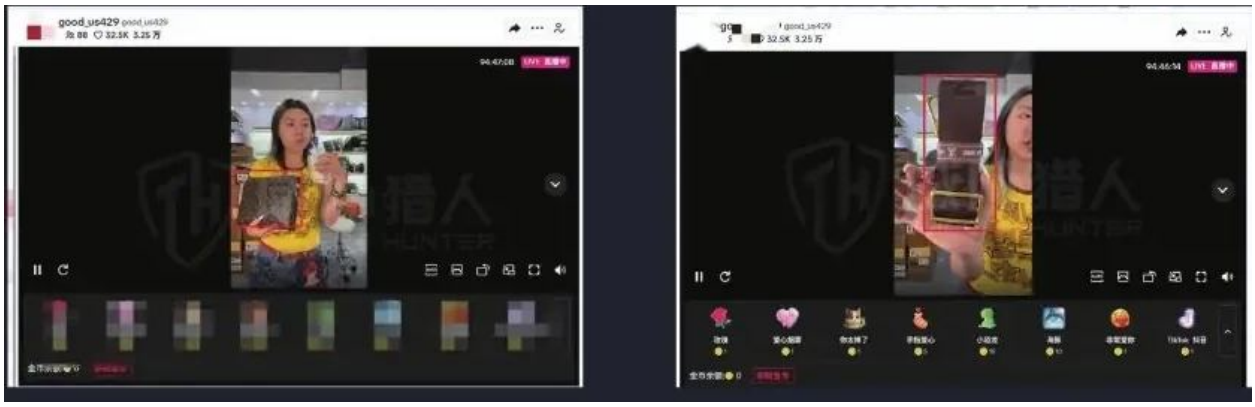
Cybercriminals choose different counterfeit and traffic-diversion strategies according to the mechanics of second-hand and live-stream commerce platforms.

Source: Threat Hunter original report, page 12. Table re-typeset in English from the original.

- Rationalize the packaging of high imitations as "idle genuine products"
- Low threshold for C-end sellers to enter
- Counterfeit characteristics: no original box, no invoice, slight design defects
- Multiple accounts, low-cost trial potential, rapid accumulation + short cycle
- Second-hand attributes make identification difficult C2C second-hand transaction e-commerce
- Second-hand goods are naturally "non-standard"
- Pretend to be a local individual seller (language/avatar/positioning)

Harvest period

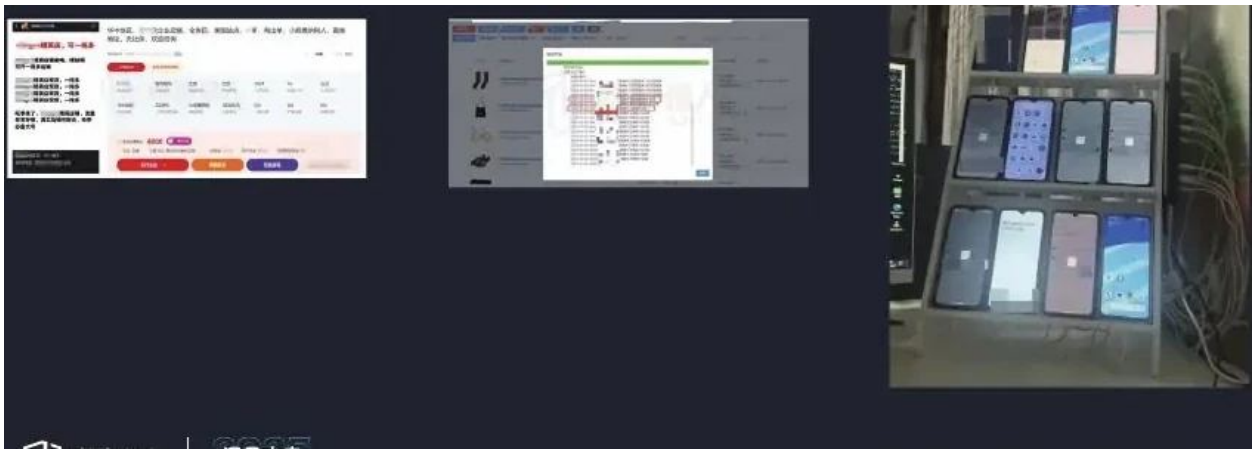
- Physical recycling or mandatory identification can curb the trend of counterfeit goods and encourage circular economy, environmentalist pop-up sales, illegal abandonment stores, and account rotation
- Single high profit, one order can cover a large amount of cost insurance, but the cost is extremely high and will sacrifice platform expansion. Users have a "leak detection" and "treasure hunt" mentality
- Deep people are not operating. High spread, long-term speed THRNTER• Dominated by content flow or interest recommendation• "Selling dog meat at the head of a sheep's head" visual display packaging high imitation as "the same company of big brands" Dupes*B2C social live e-commerce• Video display is stronger than product sentiment• The use of traffic burst is faster than review intervention, matrix• Video content is difficult to identify in a structured way• Master account weight is extremely high and young• Acquisition or misappropriation of the old accounts of whitelisted masters to attract green items for new stores/accounts, completed before fraud-control intervention



Live streams display counterfeit goods and steer buyers to independent sites or messaging channels to complete the deal.

Source: Threat Hunter original report, page 13. Original image retained.

- The master ecology is reversely exploited and supervision is obvious
- The concept of "anti-brand and price increase" prevails in the impulse consumption market
- 0B5 short-term live broadcast 24h loop filming counterfeit chains to divert traffic into harvesting and abandoning the account time lag



Trading of high-weight stores, environment isolation and live-stream matrices together support large-scale counterfeit pallets.

Source: Threat Hunter original report, page 14. Original image retained.

2. Social live streaming traffic and “hidden link” closed loop

In the live e-commerce scenario, threat actors have gradually evolved a separate transaction model of "display on the site and transaction outside the site":

- Technological logic:

Merchants display high imitation products in the live broadcast room, but do not complete transactions through the live broadcast platform;

- Drainage methods:

Guide users to independent sites and instant messaging tools to complete private transactions through comment area robots, voice guidance or private messages;

- After-sales response strategy: If the product is found to be incorrect, the merchant will induce users to cancel the complaint by "acting pitiful", or directly use the refund-only strategy to quickly quell the dispute to preserve the live broadcast account.

good_us429 good_us42028 88 0 32.5K 32,500•□2

32.5K 32,5000003 US4

94:47:08Hunter~Yinren UNTER"CHaijunjinshimeal:20

3. Industrialized store matrix (Store Matrix) and account disguise

In response to the platform’s continued removal of illegal pallets, cybercriminal groups have built a mature account support system in the midstream:

- High-quality stores (Elite• Environmental isolation tools: downstream sales• Use real Android devices. Register in batches for Store) transactions: "Fingerprint browsing book: cybercriminal" is commonly used in account owners In the underground trading black market, group control tools are equipped with "high-end devices" and "matrix listing tools", which ensure that hundreds of illegal stores are on-machine with the purchase of true-grade Android, high weight, and a full set of legal entities. "Completely isolated in a high physical environment to register seller information in batches and have passed the fraud-control review period, account quality" is the core resource (to avoid being sold by the platform for thousands of yuan due to the same pallet).

Blockade.

3.1.3. "Localized" brand counterfeit pallets provide cases:



A sample pallet list records cost, suggested price and margin, with margins of about 40% to 73% on some items.

Source: Threat Hunter original report, page 15. Original image retained.

During the 2025 annual monitoring, the Threat Hunter team continued to discover that cybercriminal groups provided counterfeit pallet services of American local warehouse brands to an e-commerce seller, assisting illegal merchants to list and sell high-imitation brand goods on the platform, forming an integrated counterfeit supply chain of "source of goods, goods on shelves, shipment".

1. Counterfeit pallets in local warehouses complete the illegal closed loop through "supply-on-shelf-local fulfillment"

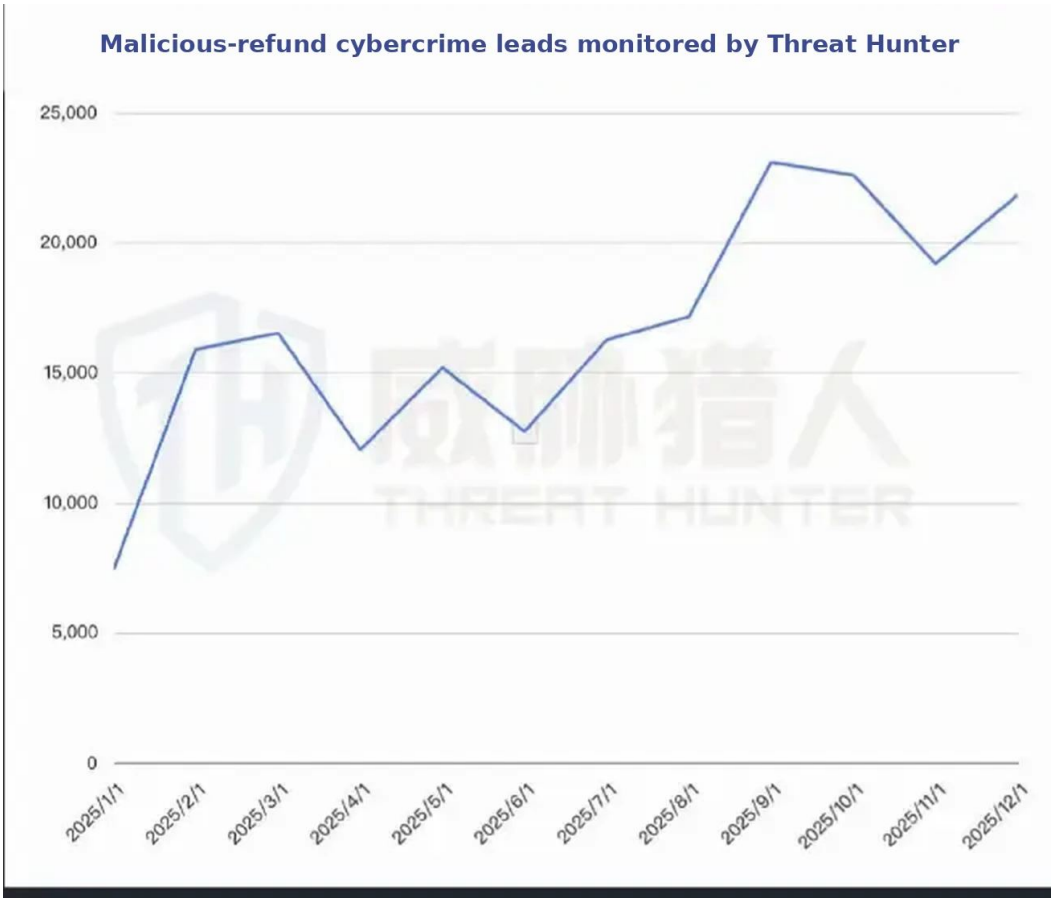
This type of cybercrime ecosystem completes the closed loop of illegal transactions in the following ways:

Supply of goods, goods on shelves, operation, logistics and fulfillment stage

1. threat actors master multiple American

1. Illegal sellers obtain funds from threat actors

1. The seller sets the shipping location of the store



Leads linked to malicious refunds rose overall, peaking at 23,099 in September.

Source: Threat Hunter original report, page 16. Original figure with Chinese text replaced by English.

The counterfeit goods warehouse mainly obtains product information and real photos, and sets them as local addresses in the United States (for example, focusing on New York and other United States to put goods on shelves.

New York);

city;

2. Transfer directly after the order is completed

2. Counterfeit goods include shoes

delivery tray threat actors;

Shoes, bags, clothing, etc.

3. By threat actors via the national postal service

price categories, and internally complete local shipments according to high-end, and reduce goods to medium-low and low-end grading.



Some refund fraud claims battery or liquid leakage as a safety hazard to push customer service into a refund-only process.

Source: Threat Hunter original report, page 17. Original image retained.

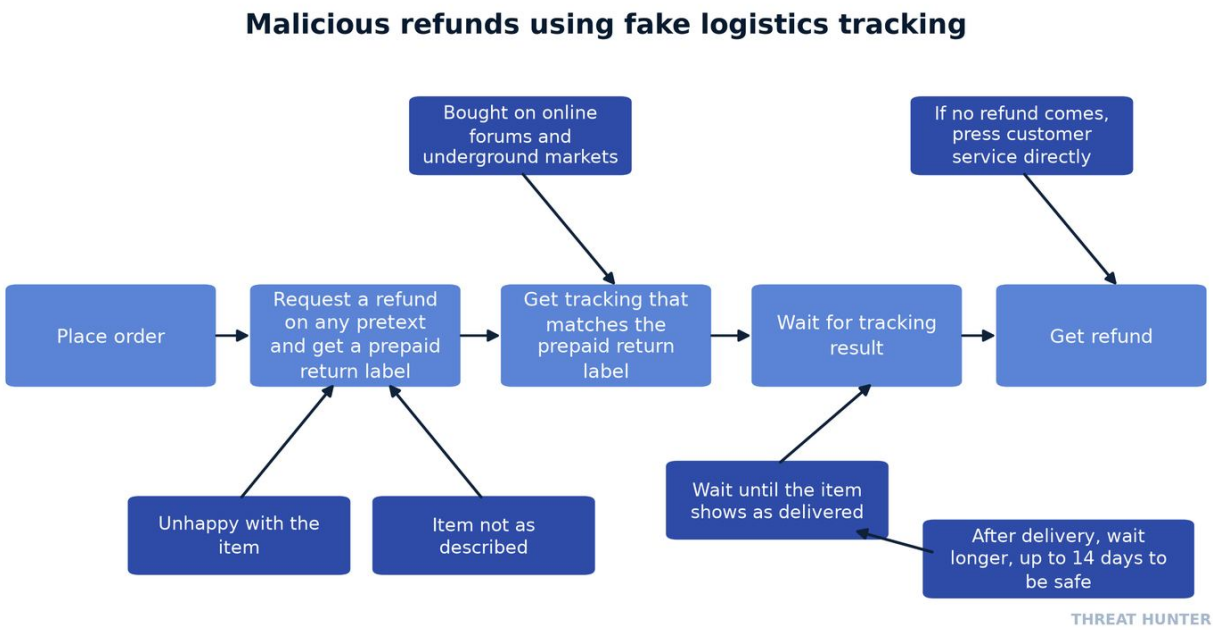
Flow anomaly exposure risk.

We can also provide products in China) For example, when customers need to purchase products on the same day, they can take the above photo album and private domain chat order operation guidance: mainly promote our pallets to attract traffic. It can promote transactions at low prices. (TK and FB live broadcasts require a sample address to directly The materials you can see in the photo album after dumping them to customers are those that are in stock that day. We will hide the materials that are not in stock that day and have a recommended price of 100-200 US dollars. Our local warehouse can keep at least 100-150 styles in stock every day.

Real shot material album address: https://xieyang123123.x.yupoo.com/Report SKU old SKU new sku style Chinese picture style

No. 12.1 Inventory includes last-mile RMB price (woven bag packaging) size

53. C ~

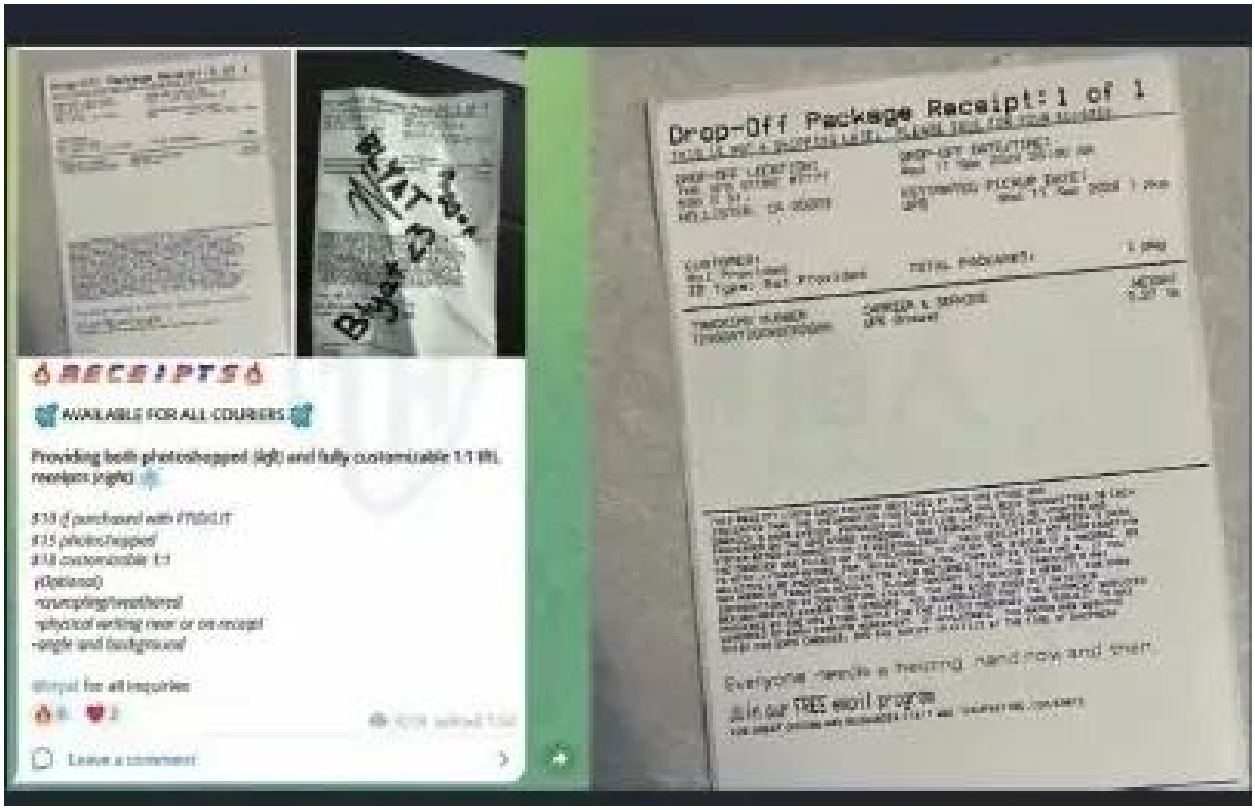


Fake-tracking fraud creates the appearance of a completed return by forging return labels and logistics status.

Source: Threat Hunter original report, page 17. Redrawn in English from the original figure.

LOSNBSJTSA-014 Mahjong three-piece set, three-piece black belt 24×13.5×4 month bucket $3CLXSNBSJTSA-015 three-piece Xiangmi ribbon 24×13.5×4 original light 53-C24×13.5×4cm A-017$3-CA-01824× 13.5×4cm$3-C

4.019 Sanqianxin Pink Street



By forging return labels and tracking, the FTID method makes the system wrongly record the goods as returned.

Source: Threat Hunter original report, page 17. Original image retained.

24×13.5×4 U.S. warehouse bag [luxury-brand bags and other U.S. warehouse sneaker and boot series precautions U.S. warehouse high luxury stocking plan U.S. high luxury clothing white boots reported SKU 52%

2. cybercriminal groups' gross profit margin can reach about 40%-73%

Judging from the recommended selling price and actual purchase cost of cybercriminal groups' internal circulation, its overall gross profit level is significantly higher than the normal seller range. Monitoring data shows that the unit cost of related products is about US$50-60, while the external recommended selling price is usually between US$100-200, and the corresponding gross profit margin range can reach 40%-73%.

3.2. Malicious refund risk: a professional fraud industry with "refund success rate" as its core selling point

In recent years, in addition to malicious refund behaviors carried out by individual consumers, professional cybercriminal groups with "successful refunds" as their core selling point have gradually appeared on major e-commerce platforms. This type of gang has formed a refund fraud service network covering multiple platforms and multiple regions through division of labor, collaboration and solidification of processes.

3.2.1. cybercrime ecosystem risk of malicious refunds in 2025: scale trend and monetization model

1. The scale of malicious chargeback risk clues continued to rise throughout the year, reaching a peak in September.

Judging from the clue chain changes throughout the year, the number of cybercrime-related clues related to malicious refunds monitored by cybercrime undergroundThreat Hunter showed an overall upward trend of 25,000. Discussions around malicious refunds showed an overall upward trend. Since the beginning of the year, the number of related clues has increased month by month, reaching the peak for the year (23,099) in September; although there have been periodic fluctuations since then, it has remained stable above 20,000 for several consecutive months.

5,0002025/10/

2. The cybercrime ecosystem commission fee for malicious refunds is 20%-30% of the refund amount.

The current malicious refund commission fee in the refund group name commission ratio covers the 20%-30% range of the site/region service characteristics and the remark amount. This range covers 135% of the cybercriminal group. Many platforms require account information or order information, and a commission will be drawn after the refund is successful.

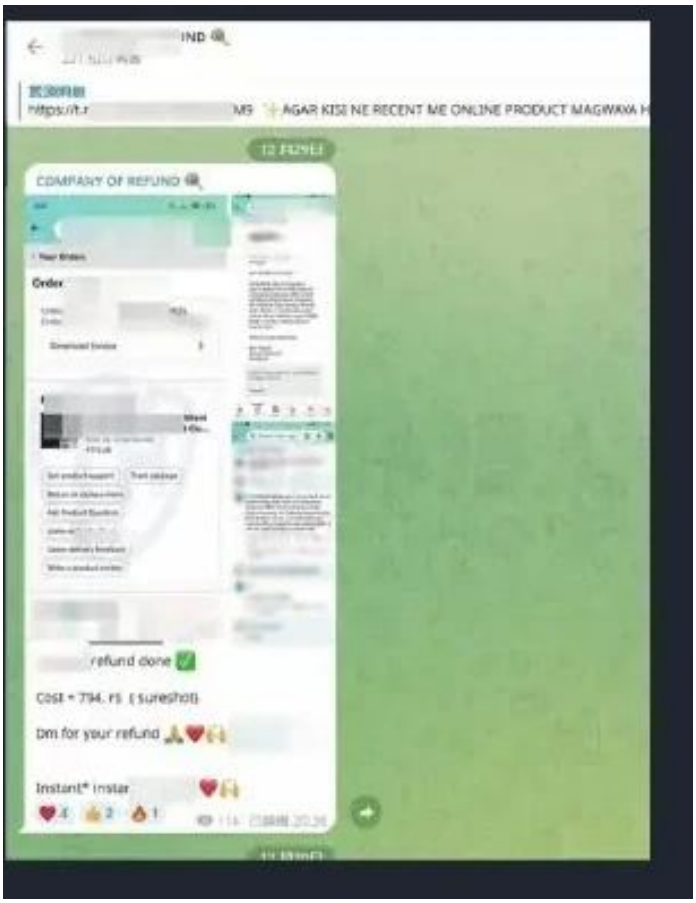
cybercriminal group 215% / 35% There are different pricing brackets under the same crystal brand. Most cybercriminal groups are suitable for serving cybercriminal group 330% / 35%. Many platforms provide refund services and "refund methods" at the same time, and there are tutorials for selling common products such as clothing, shoes, consumer electronics, etc. cybercriminal group 425%-30%. Multiple platforms cover high-order products, and some support guaranteed transactions cybercriminal The underground gang 525%-30% India is involved in both account transactions and refund services. The services are highly mixed, and most service providers use "multi-regional cybercriminal group 625%-30% India targeting clothing, electronic products, and multi-platform refund capabilities for the Indian local market" as their core selling point.

cybercriminal group 7 cybercriminal group 820%-25% Many platforms require products to be self-operated or official logistics by the platform, reducing refund failures cybercriminal group 9 Fixed 20% of platforms require waiting 2-3 days after receiving the goods for refund, claiming "100% success" cybercriminal group 10 low commission Meng Jun 5 factories, all branches have not been coded successfully. cybercriminal group 15% multi-platform focuses on "stable" and "low commission" cybercriminal group 12 ladder system: first order 10%, subsequent 15% multi-platform first order low price, emphasizing "same day arrival, same day refund" cybercriminal group 1330% multi-platform group trades credit cards, BINs, and refund services at the same time

3.2.2. New malicious refund techniques: logistics fraud and AI evidence industrialization

1. Chargeback fraud using the “hazardous material spill” tactic:

- Monitoring found that in some refund cases, cybercrime ecosystem hagua online 6 was refunded as "products containing batteries, liquids or chemical substances" in Chinese, txt



A public sample claims a high success rate for refund services and asks buyers for real account and order details.

Source: Threat Hunter original report, page 19. Original image retained.

2.9 KB

On the grounds of "leakage", it claimed that there was a safety risk, and quoted local dangerous goods handling regulations to induce customer service to send that email to implement the "refund only but not return" process.

Ha 13:24 File (F Wenzi Chinese, tt. Notepad

4. Leakage of hazardous substances

If your item package has batteries, please tell me the battery drained when you opened the package, you will be charged later if you ask them for a refund, they will charge a refund, so it's best to call back and keep it under $500 at the time of delivery. If you want a triple dip project it's very easy to get it done. What I want to do is to return foreign history instead of returning the gains, and then use another method. It’s not as hard to be homesick as people think when you are born with twin kings. But please note that it is the most challenging but reasonable!

2. Use fake logistics tracking (FTID) for refund fraud:

FTID, or "Fake Tracking ID" malicious refund technique, refers to criminals taking advantage of logistics information verification loopholes in the e-commerce transaction process. During the shopping process, they first order their favorite high-value goods, and after receiving the goods, obtain false logistics tracking IDs through illegal channels, pretend that the returns have been

delivered to the merchant, and then ask for a refund from the merchant or e-commerce platform. They attempt to achieve the dual purpose of defrauding goods and shopping funds, seriously harming the interests of merchants and disrupting the normal operating order of the e-commerce industry.

FTID (Fake Tracking ID) is a relatively typical logistics refund fraud technique in recent years. Its core is to construct a false logistics status of "return completed".

This type of approach usually relies on:

of1SPSTk,cA0602%• Prepaid return label mechanism ofa ProvidesTOTAL PACKAGES• The platform’s blind spot for “delivered” identification of logistics status CAVALABLE FOR ALL COURERSO: otoshopped (eft) and fully customizable 1:1 IRL Once the false track is judged as “delivered” by the system, $18 customizoble 1:!

That is to say, the refund process may be triggered, causing the risk of "both loss of payment" to the merchant.

If you purchase through online forums and underground markets, you can directly urge customer service to refund money if there is no refund, obtain prepaid refunds for various reasons, obtain prepaid return return labels, have the same logistics track, wait for tracking results, get refunds, wait for the product to be unsatisfied, the product does not match the description, and then wait for a period of time after the product is delivered. The maximum waiting time is 14 days. It is more conservative to use AI to generate false evidence for refund fraud:

With the popularization of generative AI technology, some malicious users have begun to use image generation, video synthesis and other means to batch generate highly realistic evidence of product damage or abnormal use. For example, they may use AI to modify intact product images or videos into a "damaged" state with cracks, scratches, water stains, etc., or generate false unboxing videos or usage traces videos as "evidence" to apply for returns or refunds to the platform.

This type of evidence is highly confusing at the visual level. Adding the "dirt" effect generated by AI illustrates the difficulty of identification between manual review and traditional rule models, resulting in the original image (without dirt).

AI generation (with dirt)

It is one of the important evolving directions of current malicious chargeback risks.

3.2.3. Typical cases of malicious refunds:

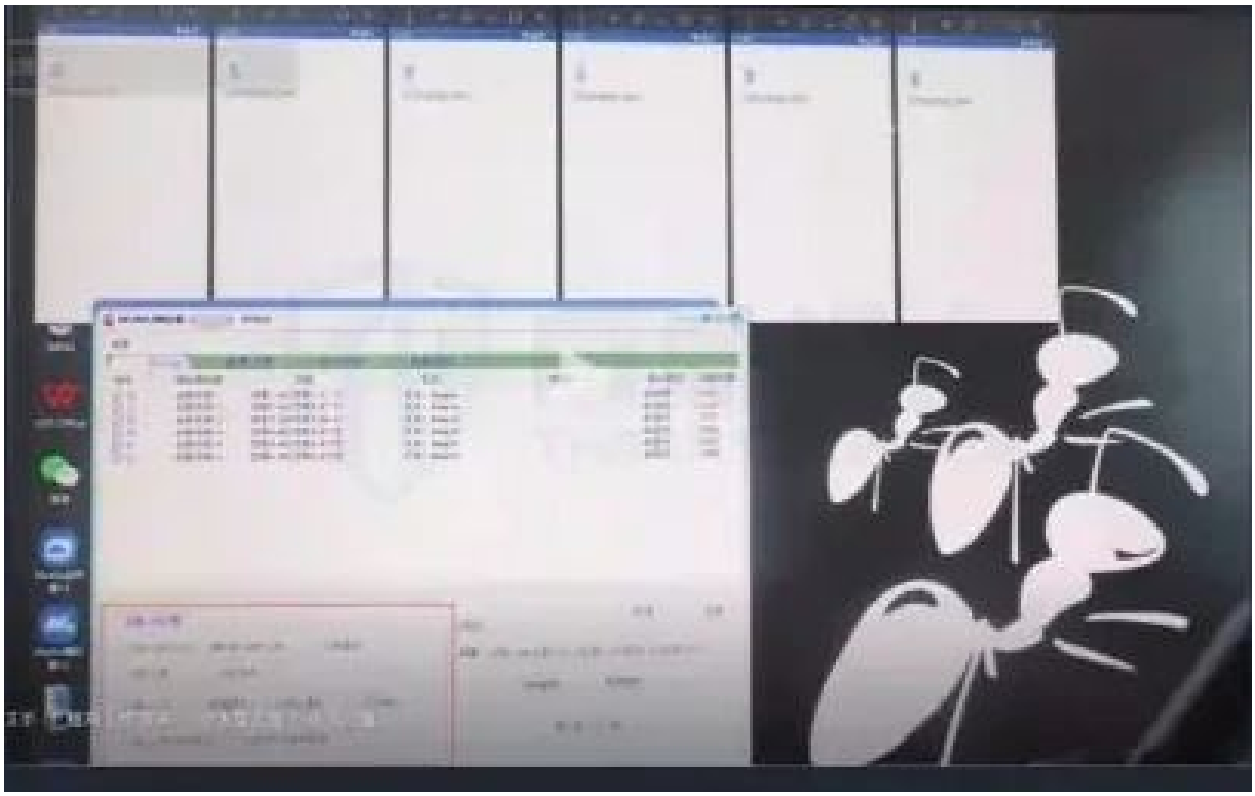
Monitoring found that cybercriminal groups have been selling refund agency services for a certain platform on encrypted messaging app channels for a long time. This type of service uses the selling point of "high success rate for refunds" to attract buyers to actively participate in refund operations and make profits through sharing.

malicious activity mode description:

Judging from the relevant group information and communication situation, the core operation mode of the refund service is as follows:

- Buyers need to use their real e-commerce platform account to complete the product IND@ order and wait for the product to be delivered normally;

MS AGAK NISL NE KCCENI ME ONLINE PKODUCI MAGYVAIATCOMPANY OF REFUND @• After signing for the goods, the buyer needs to provide the e-commerce platform account login information to cybercrime ecosystem;



Emulator base images are cloned in bulk, and device fingerprints and networks are fine-tuned to create seemingly separate accounts.

Source: Threat Hunter original report, page 21. Original image retained.

- cybercrime ecosystem then logs in to the buyer's account and initiates a refund or after-sales appeal on his behalf;
- After a successful refund, cybercrime ecosystem charges a commission of 35% of the refund amount.

Cost = 794.rs {sureshot)

Dm ior your refund This model significantly reduces the platform's difficulty in identifying abnormal refund behavior through the method of "real account + physical fulfillment".

3.3. Marketing activity arbitrage: cybercrime ecosystem, an malicious behavior centered on account and resource engineering, uses the marketing activity mechanism of the e-commerce platform (such as newbie gifts, new recruit rewards, full discount coupons, coupon fission



Private communities pay real people small sums to use their own devices and home networks to claim coupons and place orders.

Source: Threat Hunter original report, page 21. Original image retained.

etc.), obtain coupons or point resources in batches, and place orders for third-party users at a lower cost, collect service fees from them or realize arbitrage through price differences, forming a continuous risk of capital loss.

3.3.1. Two basic methods of marketing arbitrage: virtualization matrix and human-in-the-loop crowdsourcing:

Monitoring shows that currently there are two main types of techniques and models in the arbitrage scenario of marketing activities on e-commerce platforms: the virtualization matrix model and the human-in-the-loop crowdsourcing model.

The virtualization matrix tool continues to be upgraded:

The virtualization matrix is a long-standing and continuously evolving basic capability of cybercrime ecosystem in e-commerce marketing arbitrage scenarios. Its essence is not the emergence of new technologies, but the engineering and large-scale upgrade of existing virtualization methods.

The virtualization matrix capabilities currently observed in e-commerce platforms can be mainly summarized into three categories of technical techniques:

1) Fingerprint browser + proxy IP 2) Emulator master disk batch cloning 3) Cross-border cloud mobile phone large-scale deployment It is worth noting that the development and commercialization ecological multi-source of the above tools are highly mature in terms of functional completeness, large-scale scheduling capabilities and degree of automation, allowing related virtualization capabilities to be copied with a low threshold and applied to other e-commerce platform scenarios around the world.

The following uses the emulator master disk as an example to explain its fraud techniques:

Emulator master is a technology that enables multiple accounts to run independently by running a virtual device environment (such as simulating an Android or iOS device) on a computer. cybercriminal groups use this technology to create a virtual environment, generate multiple independent simulator instances by cloning the master disk, and fine-tune each instance to register multiple accounts in batches and bypass the platform's fraud-control mechanism.

The core idea of this method is to set up a standard master disk environment, including device fingerprints, IP addresses, operating systems and other information, then clone multiple instances in batches, and then further fine-tune each cloned emulator to make each account look like it is registered on an independent device, thus avoiding platform fraud-control detection.

From the perspective of risk characteristics, this type of behavior often manifests itself as: abnormal scale of account creation, highly similar environments but with deliberate differences, and automated behavior rhythms. It is one of the common basic capabilities in e-commerce platform marketing arbitrage and account abuse scenarios.

human-in-the-loop crowdsourcing has become a solution to combat strong fraud controls environments. In the context of e-commerce platforms continuing to strengthen IP and equipment environment fraud controls, in addition to automated tools to manipulate orders, cybercriminal groups have also begun to introduce "human-in-the-loop crowdsourcing" models in marketing arbitrage scenarios to avoid device fingerprinting and environmental identification risks.

Current monitoring finds that this model mainly appears in private community channels, including instant messaging platforms such as encrypted and local messaging apps. For example, in some Vietnamese messaging-app groups, there is recruitment of real users for the purpose of collecting coupons and placing orders on their behalf.

By paying rewards to real users, cybercrime ecosystem guides them to use their real devices and home network environments to complete coupon collection or designated order operations, and then cybercrime ecosystem performs order recovery or centralized settlement, thereby circumventing the platform's recognition of the virtualized environment.

Combining the existing samples and regional distribution, it is preliminarily determined that the emergence of DAT DON + G day # Nhan link is related to the following factors:

- Some platforms have relatively strong ability to identify and intercept virtualization operation behaviors, which reduces the actual input-output space of virtualization solutions;

https:

X2 Dudi 370 La congn/S.505/• The labor cost level of real users in some areas is lower than * PhG Mac Thi Budl - Phuong Vinh Tuy- HaNoiKiHifu: Nos a dia chaSo wha 1-00 .uana vo van van-huanaan Tao•C, which gives the human-operated participation model a comparative advantage in terms of cost structure and success rate;

- Under the combined influence of the above factors, related marketing activities 300-volume plan smartphone arbitrage has presented itself to the real public in specific areas https://u.

mTNFIILINTER package mode concentration trend.

6415-300=6115 Quote 6260

3.3.2. Marketing arbitrage cases during Black Friday:

During the continuous monitoring during Black Friday, it was discovered that cybercrime ecosystem publicly posted and sold US$10 no-threshold coupons for an e-commerce platform on social platforms, and claimed that such coupons could be supplied in "long-term supply and in sufficient quantity."

Further follow-up showed that this type of coupons does not come from the natural consumption behavior of normal users, but is obtained and realized through the following methods:

] cybercrime ecosystem draws new customers in batches and after the coupons are generated, the buyer directly logs in to the corresponding account and triggers the overall delivery of new accounts on the platform to provide the account to complete the order, circumventing the user marketing mechanism to obtain threshold-free accounts and login credentials and sell them to conventional coupons that can be used across accounts;

downstream users;

fraud controls identification.

During the transaction and use process, cybercrime ecosystem clearly emphasized to the downstream that only "IP isolation" is required to complete the operation, requiring the use of an independent IP environment to avoid platform fraud controls. This statement reflects that the relevant groups already have an understanding of the basic fraud controls logic of the platform, and regard the confrontation between IP and the environment as their default operating premise.

At the same time, the "unlimited supply" it claims does not stem from a single coupon anomaly, but is based on mature batch account registration capabilities: the new acquisition process is highly automated, and the account registration and acquisition are in batches, thus supporting the continuous and large-scale operation of this type of arbitrage behavior.

3.4. Logistics fraud risk: cybercrime ecosystem cross-link collaboration infrastructure

In the past, logistics fraud was more reflected in single-point violations taken by individual sellers to circumvent platform rules; in the global e-commerce risk map of 2025, logistics fraud is not an independent risk scenario, but a general support capability that runs through fake sales, marketing arbitrage and malicious refunds.

3.4.1 Two core changes: falsification of contract performance information and continued amplification of risks

1. Logistics fraud shifts from “real delivery” to “falsified performance information”

The core change in logistics fraud is to complete the "system-side contract fulfillment closed loop" in advance before platform fraud controls intervenes. In the current seller performance judgment system of mainstream e-commerce platforms: whether the goods are shipped, whether the goods are shipped from the local warehouse, and whether the goods are shipped on time, they are highly dependent on the information reported by the logistics information nodes. It is based on this mechanism that threat actors use illegal techniques to forge compliance information. The specific performance is as follows:

Use virtual warehouses, pre-online access, and pre-scanning to create “locally collected” compliance information;

2. Forge a complete logistics track through AB orders and information grafting;

Before the platform's fraud controls intervenes, the "system-side contract performance closed loop" is completed in advance. What the platform sees is "compliance performance", but what actually occurs is "cross-border dumping + delayed risk exposure".

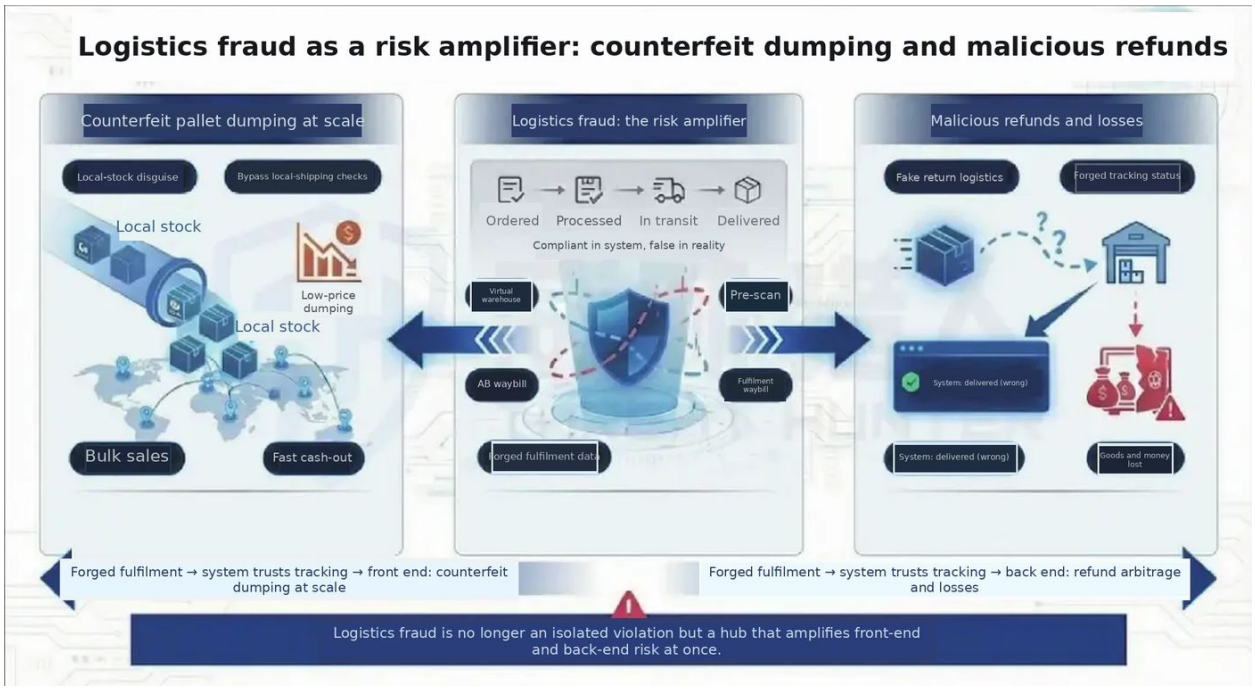
Logistics fraud: from real delivery to forged fulfillment information system side fulfillment path (forged)

Pre-Internet □-Virtual warehouse pre-Internet* Pre-scan AB order logistics information grafting system side performance closed-loop completion system sees that the compliance performance time is completed in advance (Compliance Confirmed)

Information falsification 1. System misjudgment 1. Delayed risk return T3 What actually occurs is the misalignment point of risk external benefits, system side performance closed loop completion point Feng The actual performance occurrence point flows across the border to the real performance/risk path (delayed)

Low-cost sales risk, lag risk, delayed withdrawal, and boom

2. The "Risk Amplifier Effect" of Logistics fraud: The Linked Evolution of Pallet Dumping and Malicious Chargebacks



Logistics fraud links front-end counterfeit dumping with back-end refund arbitrage, separating system-side compliance from real fulfilment.

Source: Threat Hunter original report, page 25. Original figure with Chinese text replaced by English.

In the current e-commerce ecosystem, logistics fraud is no longer an isolated performance violation problem, but has gradually evolved into a key hub node that simultaneously amplifies front-end pallet risks and back-end after-sales risks. By manipulating logistics information, it provides prerequisites for the scale of cybercrime ecosystem risk behaviors.

1) The amplification effect on the risk of brand counterfeit pallets: With the support of large-scale dumping of goods sources, such as virtual warehouses, pre-online access, and AB orders, illegal sellers can complete the following disguises without establishing real local performance capabilities:

- Disguise branded counterfeit goods as “local off-the-shelf”;
- Bypassing the platform’s pre-verification of local delivery and timely fulfillment;

Under this model, logistics fraud has become the infrastructure for "industrial replication" and rapid distribution of branded counterfeit pallets, and illegal sellers can complete short-term realization more quickly.

2) The amplification effect on the risk of malicious refunds: the extension of contract performance fraud to after-sales arbitrage. The risk of logistics fraud does not end after "shipment is completed", but can also be released in the after-sales link.

The introduction to false logistics tracking (FTID) refund fraud mentioned that in this type of scenario, the core is not the real return, but the construction of a false logistics status of "return completed". the cybercrime ecosystem usually first completes the ordering and receipt of high-value goods, and then obtains or forges a false logistics tracking ID that matches the prepaid return label through illegal channels, so that the system shows that the return package has been "delivered" to the merchant or designated address. Once the false track hits the platform's automatic identification logic of "delivered" status, the refund process may be triggered, but the

actual goods are not returned, ultimately causing the merchant to "lose both money for the goods."

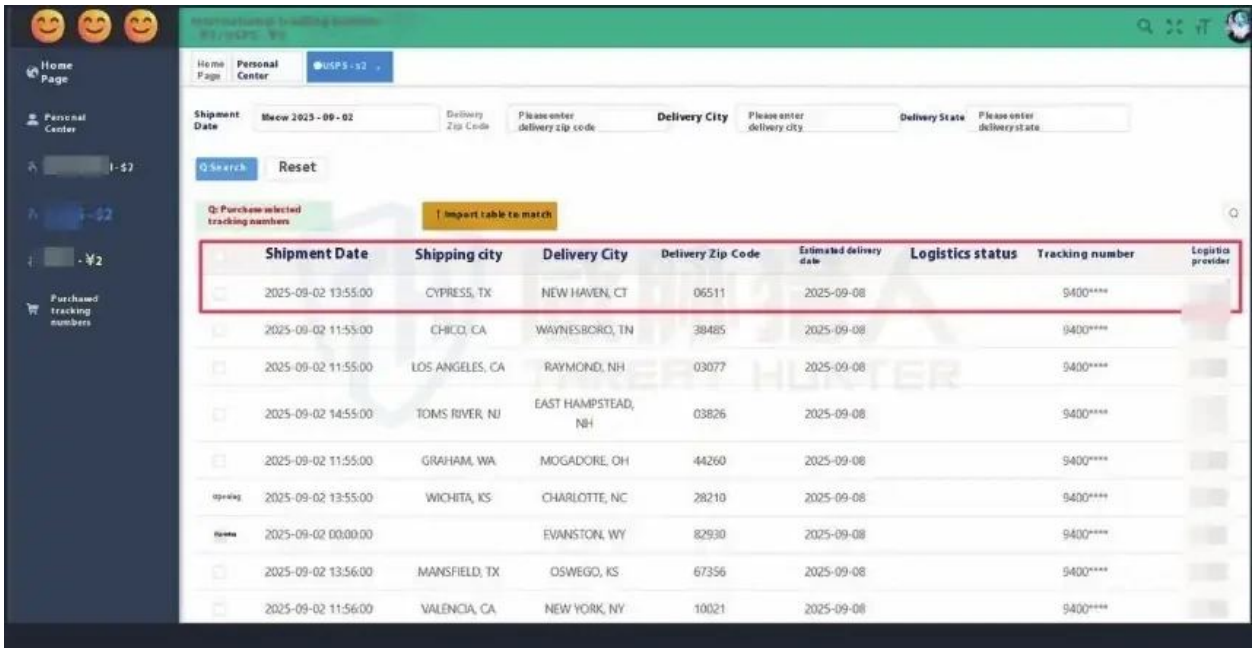
The risk amplifier effect of logistics fraud: the linked evolution of pallet dumping and malicious refunds Large-scale dumping of counterfeit brand pallets Logistics fraud: risk amplifier malicious refunds and capital losses Local spot goods damaged goods Bypassing local delivery verification False returns Logistics forgery tracking status Ben Ye Guan made orders hot to process and organize the system side compliance, reality is distorted Low price sales Virtual warehouse Pre-netbook North spot)

AB single performance order

- The system misjudges that the goods have been delivered, the goods are quickly realized, and the performance information is misjudged. The system misjudges that the goods have been paid. The performance information is divided. The system trusts the logistics status. One front-end: Pallet scale, Guanhuo contract information, and the system trusts the goods status. The back-end: Refund arbitrage and capital loss. Logistics fraud is no longer a single point of violation, but a key hub that amplifies front-end and back-end risks at the same time.

3.4.2. Typical cases of AB order utilization

Threat Hunter discovered that there are threat actors selling real face order number information of well-known international logistics companies, which can be used for A side order in AB orders.



A website sells existing logistics tracking numbers by country and address to fake local compliance.

Source: Threat Hunter original report, page 26. Original image retained.

threat actors use special means to collect face orders with existing tracks into private websites. Illegal sellers can query the corresponding face orders through the website for purchase, and upload them to the e-commerce platform to forge delivery times and logistics trajectories, bypassing the limitations of local delivery and delivery time rules on the platform.

Checking the private website of threat actors, we found that local tracking numbers are available for sale in multiple sites and countries, such as the United Kingdom, France, Germany, the United States, etc.; Australian tracking numbers are also available.

AB orders use two order numbers:

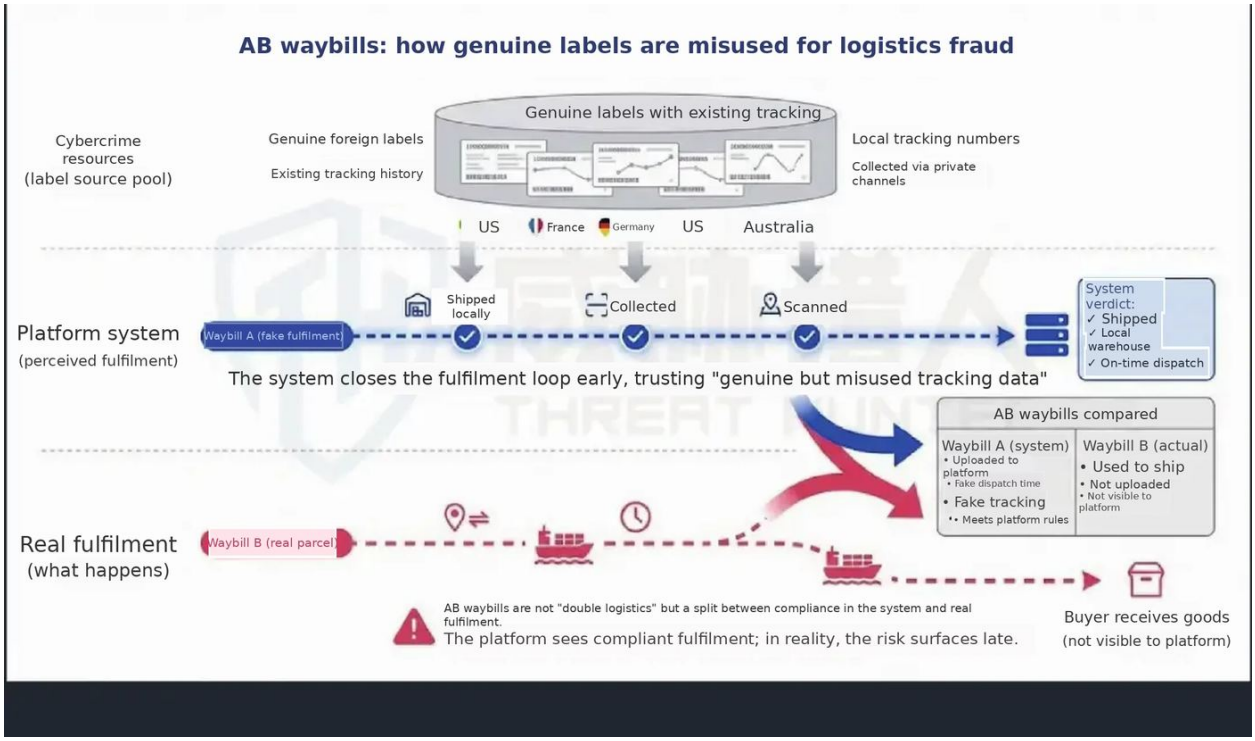
- A-order (False order number): The seller uses a false logistics order number (A-order) that is inconsistent with the actual delivery to upload to the e-commerce platform to meet the platform's delivery timeliness requirements and create the illusion that the goods have been shipped.
- B order (real package): The seller uses the real logistics order number (B order) to send the actual goods to the buyer through other logistics channels. Order B is usually not uploaded to the platform and is only used for actual delivery and buyer receipt.

AB order mechanism: Logistics fraud path where the real order is abused. There are real order resources on the logistics track. threat actors. Resource side. Real foreign order local order number (face order source pool).

Historical rail speeds have been collected through private channels United Kingdom 1) France, Germany and the United States Australian domestic shipments TC Pakistan received 2 Scanned system determination:

(Perceived fulfillment perspective)

Order A on the platform system side (false performance order)



By misusing genuine tracking that already exists, AB waybills make the platform misjudge fulfilment while the real goods follow a path it cannot see.

Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.

<--V The local warehouse has completed the closed loop of salt system side performance ahead of schedule, and the platform trusts the "real but misused logistics data" delivery time compliance AB order comparison instruction A order (system performance order)

- Used for actual issuance of daily orders (orders actually fulfilled)
- Fake goods delivery time
- Fake goods change track
- Not uploaded to the platform
- Meet the platform house arrangement
- The real fulfillment side B order (real package) is not visible on the platform

(actually happened)

What the platform sees is compliance, but what actually happens is delayed risk exposure.

AB order is not "dual logistics", but the separation of "compliance performance on the system side" and "real performance behavior".

The buyer actually receives the goods (not visible on the platform)

How threat actors operate:

]Fast order selection and purchase:

A form upload platform:

The seller delivers goods independently:

After the illegal seller places an order, the illegal seller uploads the purchase order number to the e-commerce platform for delivery from threat actors based on the buyer's delivery address.

The private website that directly sends the product package with the order form searches and receives the goods to the buyer's delivery address, and the local delivery with the same address completes a closed transaction loop.

Face sheet, purchase the corresponding face sheet.

I-$2Q SearchReset3-$2Q: Purchase selectedtracking numbers1 Import table to match•¥2Shipment DateShipping cityDelivery CityDelivery Zip CodeSmand delleryLogistics statusTracking numberprovidePurchased2025-09-02 13:55:00CYPRESS, TXNEW HAVEN,CT065112025-09-089400**tracking2025-09-02 11:55:00CHICO, CAWAYNESBORO, TN384852025-09-089400*32025-09-02 11:55:00LOS ANGELES, CARAYMOND, NH030772025-09-089400* **2025-09-02 14:55:00

TOMS RIVER, NJEAST HAMPSTEAD,ZH038262025-09-089400* GRAHAM, WAMOGADORE,OH442602025-09-089400*Opening2025-09-02 13:55:00WICHITA, KSCHARLOTTE,NC282102025-09-089400*2025-09-02 00:00:00EVANSTON, WY829302025-09-089400*big*2025-09-02 13:56:00MANSFIELD, TXOSWEGO, KS673562025-09-089400*2025-09-02 11:56:00VALENCIA, CANEW YORK, NY100212025-09-089400***

Summary:

In 2025, cybercriminal groups will no longer just carry out malicious activity around a single rule vulnerability or local business scenario, but will use the platform business process as the attack blueprint to build a full life cycle and replicable malicious activity method covering accounts, supply, contract fulfillment and after-sales.

In this process, logistics fraud, false evidence generation, real-life resources, etc. are no longer isolated risk fraud methods, but have gradually evolved into basic capabilities for cross-scenario reuse. These capabilities are embedded in multiple high-risk scenarios such as brand counterfeiting, malicious refunds, and marketing arbitrage, resulting in a trend of joint amplification.

In the face of this trend, a single "defense strategy" is no longer effective. The platform must build a multi-layered intelligence-driven defense system and upgrade "seeing risks" to "system engineering to compress threat actors ROI": The technical level and tactical level of the multi-layered intelligence-driven defense system should be cross-checked through multi-modal information. The strategic level needs to shift from blocking single methods to identification, business logic counter-verification and cost relief. Establish reusable attack capabilities and behavior modeling mechanisms for cross-regional liquidity and attack migration, and continue to compress cybercriminal. The core risk warning mechanism is the transfer capability of underground, focusing on its scale and automatic input-output ratio (ROI), forcing it to attack and identify in advance the basis of the cybercrime ecosystem resources;

The hit path keeps failing.

Transfers and reorganizations between markets;

Looking to the future, e-commerce security will no longer be a single technical issue, but a long-term game centered on the depth of business understanding and closeness to the business. Threat Hunter will continue to pay attention to relevant fraud trends and provide enterprises with the latest intelligence support and prevention suggestions.

Threat HunterTHREAT HUNTER builds the cornerstone of digital security with intelligence. Scan the QR code to follow and obtain the latest anti-fraud report in the industry. Service hotline: 400-809-3699S Official website: www.threathunter.cn Contact email: marketing@threathunter.cn Headquarters address: Room 1705, Building B2, Kexing Science Park, No. 15 Keyuan Road, Science and Technology Park Community, Yuehai Street, Nanshan District, Shenzhen, Guangdong Province