THREAT HUNTER RESEARCH

H1 2024 Global E-commerce Platform Risk Report

A cross-market review of account abuse, order manipulation, logistics fraud and other risks facing global e-commerce platforms.

Original publication: 2024-08-15
Research team: Threat Hunter Research Team
Source report: 33 pages

Original report text

This text version is reconstructed based on the 33-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 recent years, new international e-commerce platforms have continued to emerge and grow rapidly. Regional marketplaces have strong momentum in Southeast Asia, where they hold a dominant position; a leading regional marketplace performs well in Latin America; niche marketplaces compete strongly in handicrafts, vintage goods and other segments; and four fast-growing Chinese-funded cross-border platforms, known in the industry as the "Four Little Dragons" of cross-border e-commerce, are injecting new vitality into the development of the global e-commerce market.

At the same time, the security challenges faced by global e-commerce platforms are becoming increasingly severe. the cybercrime ecosystem activities such as malicious fraud, discount abuse, and malicious refunds occur frequently. These attacks not only disrupt the market order, but also bring direct economic losses to global e-commerce platforms and enterprises, affecting normal operations and long-term development.

Based on threat intelligence analysis of cybercrime ecosystem in global e-commerce scenarios, Threat Hunter officially released the "H1 2024 Global E-commerce Platform Risk Report". The statistical data period of this report is from January to July 2024. In view of the eight major types of risk scenarios currently faced by global e-commerce businesses, the Threat Hunter intelligence research team provides comprehensive risk insights through in-depth data analysis, helping global platforms and enterprises to effectively identify and prevent potential threats, and achieve sustained and stable business development.

Related noun definitions:

1. Stealing: During the transportation process, the merchant changes the actual shipping address of the goods to a lower-cost address to reduce shipping costs.

fee;

2. Weight theft: refers to the merchant deliberately underreporting the weight during transportation to reduce logistics costs;

3. Darknet: refers to a hidden network that ordinary netizens cannot search and access through conventional means. They need to use some specific software.

Configuration or authorization is required to log in;

4. Private group chat: refers to group chat channels on mainstream messaging apps;

5. Social media: refers to mainstream social media and lifestyle-sharing platforms;

6. Card issuing website: refers to an online platform dedicated to automated sales of virtual goods or services. The card issuance platform has now become

The main transaction channel and collaboration platform of the Internet cybercrime ecosystem, the card-issuing website cannot be retrieved by the web page, and a specific link to the card-issuing product is required to link to the product page;

7. Finished product account and finished product number: refers to accounts that have been bound to personal or corporate information. There is no need to recharge these accounts after purchase.

Register or fill in information externally, and it can be used directly;

8. Scalping: refers to the malicious behavior of cybercrime ecosystem hiring human participants to place orders remotely to collect limited-purchase discounted products in bulk;

9. Access number: refers to cybercrime ecosystem or promotion-abuse actors who use illicit SIM-card phone numbers from the platform to register for platform accounts in batches through the access platform.

Log in to the platform with your account number or authorization to collect platform or mini program activity prizes;

10. CK number: CK number is a way to register the number. The data number contains the platform account login information. It is registered through an independent COOKIE.

Account information can be used to log in without a password. Each CK number will correspond to a numbering device. The CK number can be used to log in frequently regardless of IP, and there is no record of the login device, which can effectively reduce some of the factors that affect the account weight. It is usually used by cybercrime ecosystem for batch registration, authorizing mini programs, and collecting platform activity prizes;

11. Platform entry: refers to merchants who want to enter the platform go through the entry procedures through an intermediary;

12. EIN certificate: EIN is the abbreviation of Employer Identification Number (employer identification number), which is the U.S.

A unique identification number assigned to a business or other organization by the Internal Revenue Service (IRS). An EIN certificate is a formal document that proves that an organization or business has obtained an EIN and that the number has been registered and valid. The certificate usually includes information such as business name, EIN and registration date;

13. VAT Photo: VAT is the abbreviation of Value Added Tax, which is a widely used consumption tax.

Many countries and regions charge this tax on the sale of goods and services. VAT photo usually refers to a photo or scan of the value-added tax registration certificate obtained by a business or individual;

14. human-in-the-loop crowdsourcing: refers to a group of part-time people (mothers, students) who receive bounty tasks and assist through crowdsourcing platforms and crowdsourcing groups.

The cybercrime ecosystem (crowdsourcing task publisher) completes the task and receives the order fee, while the cybercrime ecosystem successfully completes the task and collects the platform reward. The task types include: new users, registration, support, downloads, likes and other high-risk crowdsourcing, and real-name, application and other high-risk crowdsourcing can also be released;

15. Self-supported account traffic manipulation: refers to merchants using fingerprint browsers to purchase foreign servers and IPs to build an order traffic manipulation environment to achieve batch registration

The behaviors of registering a target platform account, maintaining an account, browsing simulations, and placing orders;

16. human participant fraud: refers to cybercrime ecosystem fraud on e-commerce platforms by hiring real users to pretend to be ordinary consumers.

the act of trading;

17. Fingerprint browser: refers to a special browser that can set the language, operating system, and display analysis when accessing a website.

Resolution and hardware configuration and other information to simulate and forge the user's browser fingerprint;

18. Logistics fraud: refers to the behavior of e-commerce sellers using false invoices or technology express delivery orders to steal areas, steal weight, or

Evade taxes and reduce sales costs;

19. Secondary tracking number: refers to the logistics tracking number being leaked or sold by the logistics company for reuse;

20. Lost accounts: refers to logistics accounts that are in arrears with freight or use fraudulent credit cards to pay for freight;

21. Paoshui bill: refers to the logistics bill generated using Paoshui account;

22. Technology orders: refers to the express orders produced by cybercrime ecosystem after cracking the order generation rules. This type of order can be partially ordered.

The number scanner recognizes it normally and can query the corresponding logistics order number and logistics track on the official website;

23. Authentication bypass: refers to cybercrime ecosystem using certain technical means or adopting non-compliant methods during the identity authentication process of e-commerce platforms.

Law, the act of evading authentication;

24. Store account deposit: A certain amount of money that sellers need to pay when registering on the platform to ensure that the store can operate normally.

If there are any violations on the account, the deposit may be banned;

25. Pallet: refers to the company transporting and storing products in batches in warehouses located in the destination market for rapid distribution and sales to the local area.

local or surrounding markets.

Secondary sale).

Global e-commerce platform risk scenarios

1. Risk scenarios for global e-commerce platforms

The following is Threat Hunter's intelligence analysis on global e-commerce, the statistical data period is from January to July 2024:

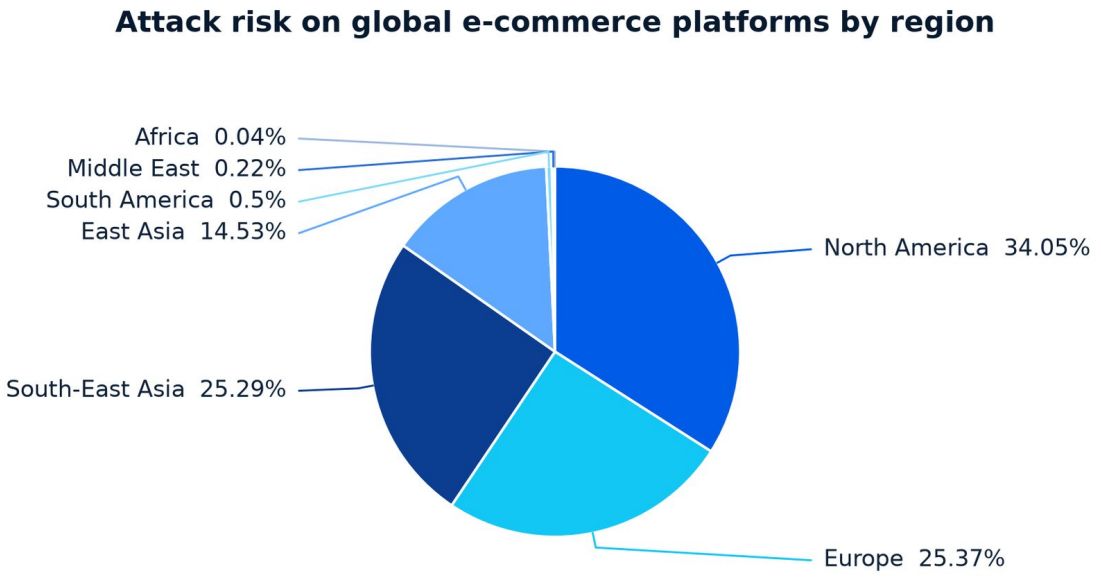
1.1. The total number of risk clues captured for attacks on global e-commerce platforms exceeds 2.01 million

The total number of risk clues captured by Threat Hunter for attacking global e-commerce platforms exceeds 2.01 million, and more than 720,000 accounts used by cybercriminal groups are involved. These accounts used by cybercriminal groups belong to China, Vietnam, Thailand, Spain, Indonesia, the United States, etc.

1.2. Attack risk by region for global e-commerce platforms: North America, Europe, and Southeast Asia rank among the top three

Among e-commerce platforms in various regions around the world, North American e-commerce platforms have received the most attacks, accounting for 34.05%, followed by Europe and Southeast Asia, accounting for 25.37% and 25.29% respectively. The reason why North America accounts for a high proportion of attacks is mainly because there are many global e-commerce companies in North America. These companies have a wide range of business, large scale, and a large number of users, so they have become the main target of cybercriminal attacks.

Note: China's regional e-commerce platform statistics do not include local e-commerce companies, such as the major domestic marketplaces.

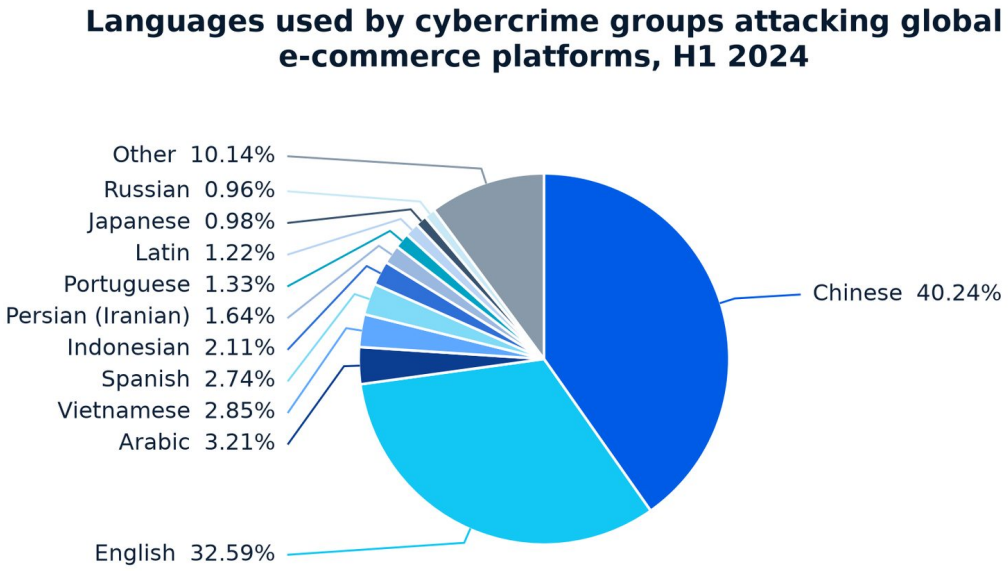


Attack risk on global e-commerce platforms by region: North America, Europe and South-East Asia rank top three

Source: Threat Hunter original report, page 8. Redrawn in English from the original figure.

1.3. Chinese and English have become the main languages used by cybercrime ecosystem to attack global e-commerce platforms.

As of the end of July 2024, Threat Hunter's intelligence statistical analysis of attacks on global e-commerce platforms in platform monitoring channels found that among the cybercrime ecosystem activities, cybercriminal groups used Chinese and English at the highest proportion, accounting for 40.24% and 32.59% respectively.



Languages used by cybercrime groups attacking global e-commerce platforms in H1 2024: Chinese and English dominate

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

Note: Data comes from international messaging apps, social networks and online forums, as well as domestic messaging and social media platforms.

1.4. Global e-commerce platforms mainly face eight major risk scenarios, with account risk, fraudulent orders, and logistics fraud ranking the top three.

Threat Hunter's statistical analysis of attack intelligence captured by the end of July in 2024 found that global e-commerce platforms mainly face eight major risks, namely: account risk, order fraud risk, logistics fraud risk, product information crawling risk, malicious refund risk, authentication bypass risk, internal and external collusion risk, and pallet risk.

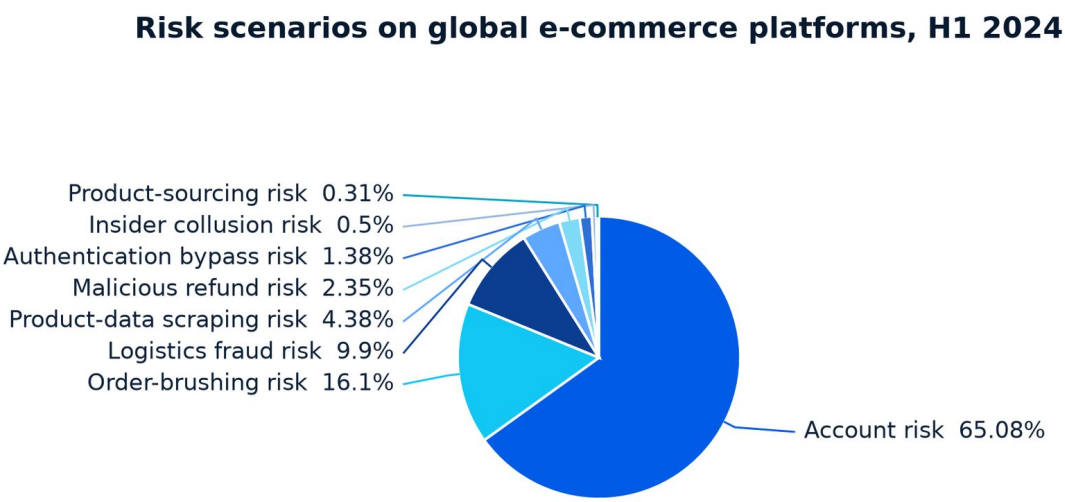
Among them, the three most common risks are: account risk accounting for 65.08%, order fraud risk accounting for 16.1%, and logistics fraud risk accounting for 9.9%.

There are three main reasons why account risk accounts for the highest proportion:

(1) It is easier to register an account on global platforms. You only need an email address to successfully register a buyer account, and there are also anonymous email addresses that can be used. cybercriminal groups are very easy to obtain;

(2) The supply chain for global e-commerce seller accounts is very sound. From the false material information required for registration to the finished accounts, there are a large number of cybercrime-related industries selling;

(3) The account number is the basic material for cybercrime ecosystem to conduct malicious activity in the future. Without an account, you will not be able to receive coupons, and you will not be able to commit fraud. Therefore, cybercriminal groups will conduct a lot of research on account registration.



Risk scenarios on global e-commerce platforms in H1 2024: account risk accounts for almost two-thirds

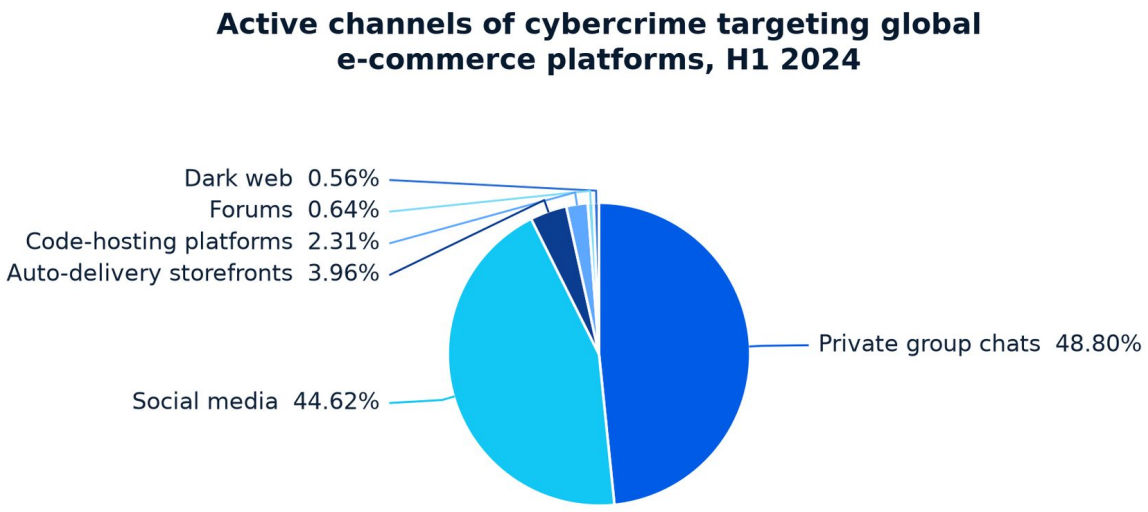
Source: Threat Hunter original report, page 10. Redrawn in English from the original figure.

1.5. Among the sources of risk clues, private group chats have the most clues, followed by social media

cybercrime ecosystem malicious activity deeds around the world are mainly spread and profited through private group chat channels and social media platforms. Among the sources of risk clues on global e-commerce platforms, private group chats accounted for 48.80%, followed by social media, which accounted for 44.62%.

Different countries and regions have differences in the platforms they use. For example, private group chat channels for domestic communication include encrypted messaging apps

and mainstream domestic messaging apps; Vietnam and Indonesia each favour different local messaging apps; social media use in Southeast Asia centres on one dominant global social network, while the Americas and Europe lean more towards microblogging platforms. the cybercrime ecosystem also uses these platforms to spread and illegal activities.



Values as published in the source; they sum to 100.89%.

THREAT HUNTER

Sources of risk leads: private group chats rank first (48.80%), followed by social media (44.62%)

Source: Threat Hunter original report, page 11. Redrawn in English from the original figure.

An analysis of card issuing website channels found that the categories of cybercrime ecosystem products sold abroad and domestically are basically the same. The difference is that the details of the products sold vary according to the characteristics of each country. For example, the sale of personal data abroad usually involves passports and driver's licenses, while in China, ID cards are mainly used. In foreign countries, it is common to register multi-purpose email addresses and various email addresses for sale. Threat Hunter currently monitors a total of 195 international card-issuing websites, and the risk clues provided account for 3.96% of the total.

Card issuing website: refers to an online platform dedicated to automated sales of virtual goods or services. The card-issuing website cannot be retrieved by the web page and requires a specific link to the card-issuing product to link to the product page. It has now become the main transaction channel and collaboration platform of the cybercrime ecosystem on the Internet.

1.6. The risk scenarios of cybercriminal attacks differ between Chinese and global e-commerce platforms.

There are many overlaps in the risks faced by Chinese e-commerce platforms and global e-commerce platforms, but there are differences in the segmented scenarios. both

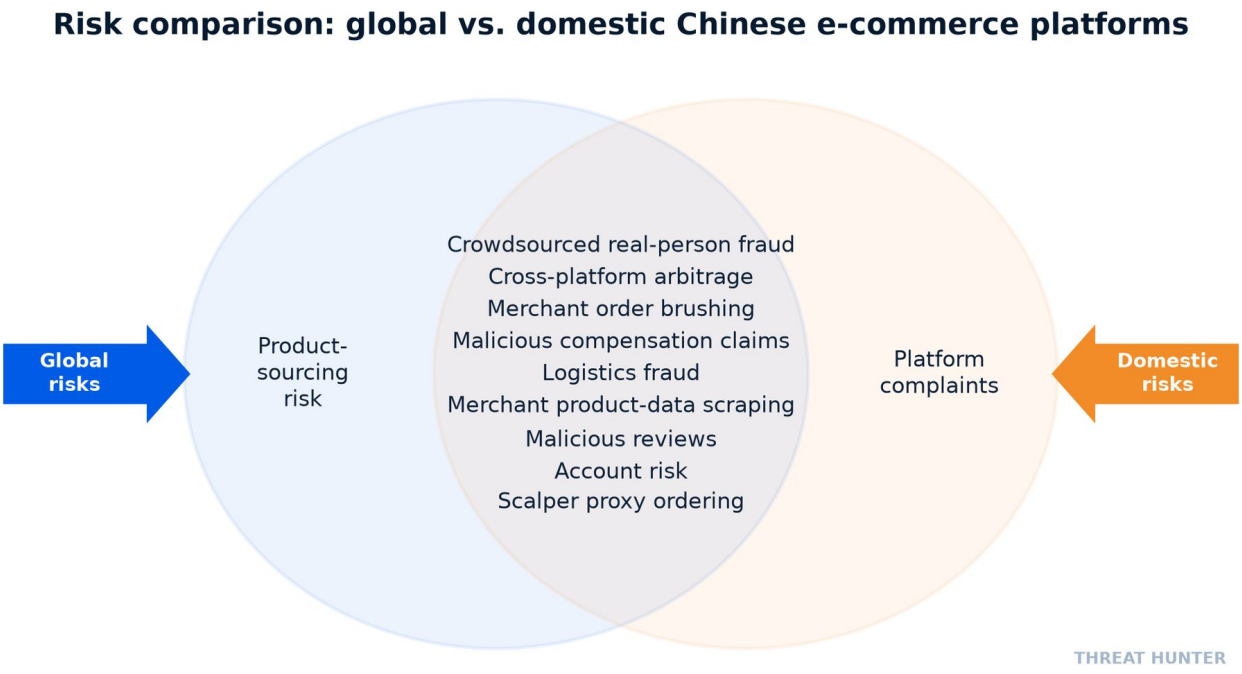
They all face risks such as merchant fraud, scalping, and account fraud, but they are different in terms of operation methods and specific details. For example:

(1) Order fraud scenario: The risk of fraud by domestic merchants is also common on global e-commerce platforms. However, domestic platforms have implemented long-term fraud controls on fraud in stores, resulting in various methods of fraud, such as low-price flash sales through live broadcast rooms, use of preferential platforms such as one-cent purchases, and free trial fraud through mini-programs. In contrast, global e-commerce platforms still mainly rely on human participants and self-supported accounts to manipulate orders.

(2) Scalper generation: Currently, the scalper model emerging in China also exists in other markets, where scalpers also directly use of the price difference between various platforms to buy low and sell high. For example: cybercriminal groups collects lower-priced product information on platform A, registers an e-commerce account on platform B, and sells it at a high price. If a user places an order on platform B, cybercriminal groups will return to platform A to place an order and earn the price difference. The common practice in China is to buy low-priced goods in large quantities and store them in warehouses before selling them.

(3) Account risk: There are account risks in both domestic and foreign e-commerce platforms. In China, the account risk is mainly concentrated on the buyer's side, while on global platforms, the account risk is mainly concentrated on the seller's side. Many domestic marketing activities require the assistance of buyer accounts. In order to complete the activity tasks, cybercriminal groups will need a large number of accounts, so many domestic reception numbers, ck numbers, etc. will be generated.

Registering an account on global platforms is relatively easy. Most of them can register successfully with just an email address. The difficulty of registration is relatively low. There are few buyer accounts for sale by cybercrime ecosystem.



Risk scenarios differ between global and domestic Chinese e-commerce platforms, with most risks shared

Source: Threat Hunter original report, page 12. Redrawn in English from the original figure.

Analysis of specific risk scenarios for global e-commerce platforms

2. Analysis of specific risk scenarios for global e-commerce platforms

Threat Hunter conducted a survey on global e-commerce platforms and found that the main risks they face are: account risk, order fraud risk, logistics fraud risk, product information crawling risk, malicious refund risk, authentication bypass risk, internal and external collusion risk, and pallet risk.

Risk definition:

Account risk: refers to various scenarios involving security threats and potential risks to your account. These scenarios include but are not limited to the following situations: account registration risks, account takeover risks, agency entry risks, finished product account sales risks, account sharing and leasing risks;

Risk of order fraud: It refers to the fraudulent practice in which platform sellers pay to entrust cybercrime ecosystem to purchase goods from designated platform sellers through order fraud tools or human participants, and fill in false positive reviews to increase store sales, credibility and ratings, and obtain platform traffic;

Logistics fraud risk: refers to the behavior of e-commerce sellers using false invoices or technology express delivery orders to deliver goods, which can achieve area stealing, weight theft or tax evasion, thereby reducing sales costs. However, once logistics fraud is detected by the logistics company, the goods may be seized, and the seller will need to pay the freight, which will seriously delay the delivery time of the goods and reduce users' confidence in the platform;

Product information crawling risk: refers to the risk that an e-commerce platform or website may face unauthorized crawler programs (crawlers) to illegally obtain product information on the platform;

Malicious refund risk: refers to users applying for refunds through improper means, thereby obtaining undeserved benefits;

Authentication bypass risk: refers to the behavior of cybercrime ecosystem using certain technical means or adopting non-compliant methods to evade authentication during the identity authentication process of e-commerce platforms;

Internal and external collusion risk: refers to the secret collusion and cooperation between cybercrime ecosystem and platform insiders to achieve non-compliant entry into the platform, unblocking accounts, etc.;

Pallet risk: refers to low-quality pallets stored in destination-market warehouses by cybercrime ecosystem, which can easily bring quality risks and platform performance issues to the platform.

The following will focus on the analysis of these 8 major risk scenarios:

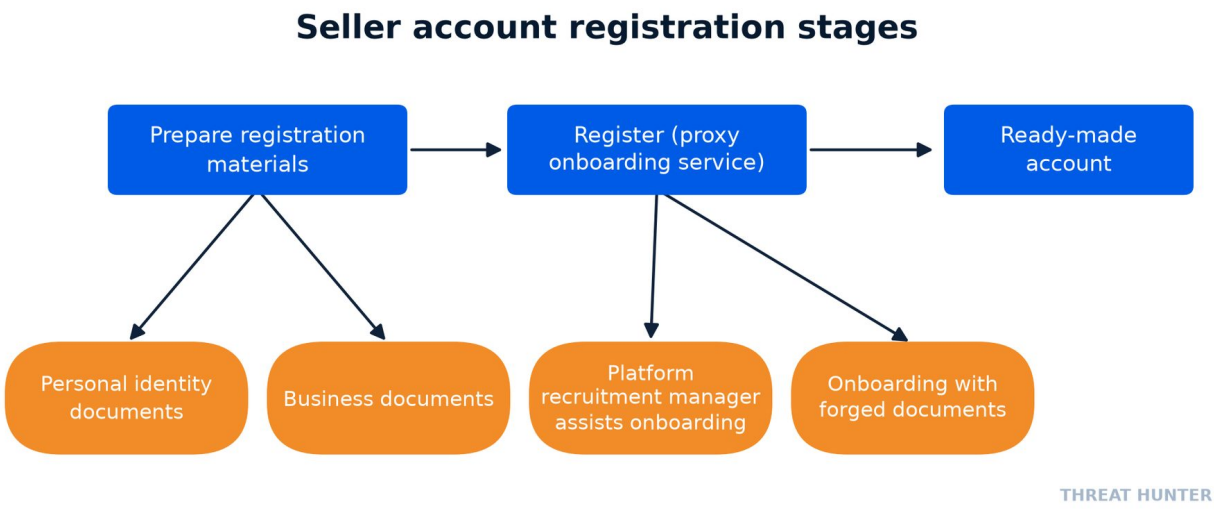
2.1. Account risk scenario analysis

Account risk scenarios: refers to various scenarios involving security threats and potential risks to your account. These scenarios include but are not limited to the following situations: account registration risks, account takeover risks, agency entry risks, finished product account sales risks, account sharing and leasing risks;

There are two main user roles in e-commerce platforms: buyers and sellers. Therefore, account risks on e-commerce platforms are also divided into two categories:

Buyer account risk and seller account risk. The following will focus on the analysis of seller account risks, including seller account registration, platform entry, and selling of sellers' finished product numbers. These risks may lead to an increase in fraud and infringement risks, seriously reducing user trust, and ultimately have a negative impact on the platform's reputation and business development.

To register a seller account, you need to prepare registration materials in advance and follow a series of steps to register. The account that is successfully registered is called the finished product number. That is, there are three stages, namely preparation of registration materials, registration stage, and finished product number stage.



Seller account registration has three stages: preparing materials, registering, and the ready-made account

Source: Threat Hunter original report, page 15. Redrawn in English from the original figure.

2.1.1. In the stage of preparing registration materials, cybercriminal groups will use false information to register an account.

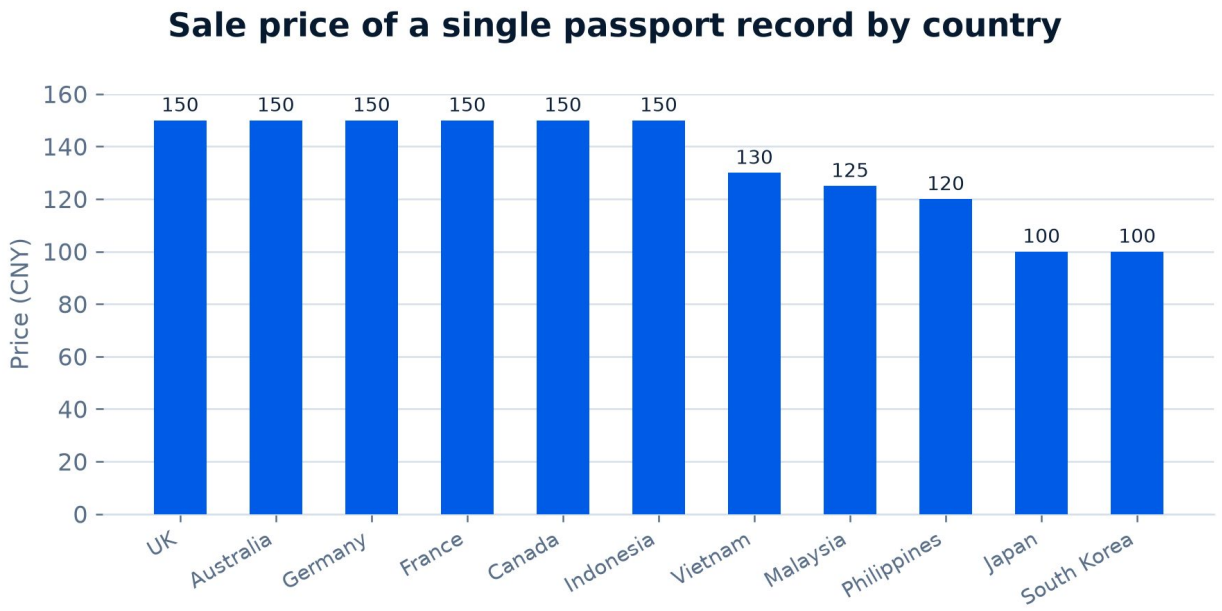
the cybercrime ecosystem usually promotes through private domain channels, publishing and selling basic material information on card issuing websites. According to the requirements for registration materials, there are two main types of basic materials sold by threat actors: personal data and corporate data information sales.

(1)Sale of personal information

Seller account registration on global e-commerce platforms can be done with a driver's license or passport. Supplementary materials such as hand-held photos or bank statements will be added according to the requirements of different platforms.

a. Regarding the selling price of a single passport, passports from American countries and European countries have the highest price, with a selling price of 150 yuan. In Southeast Asian countries, it costs 150 yuan to buy an Indonesian passport, 130 yuan to buy a Vietnamese

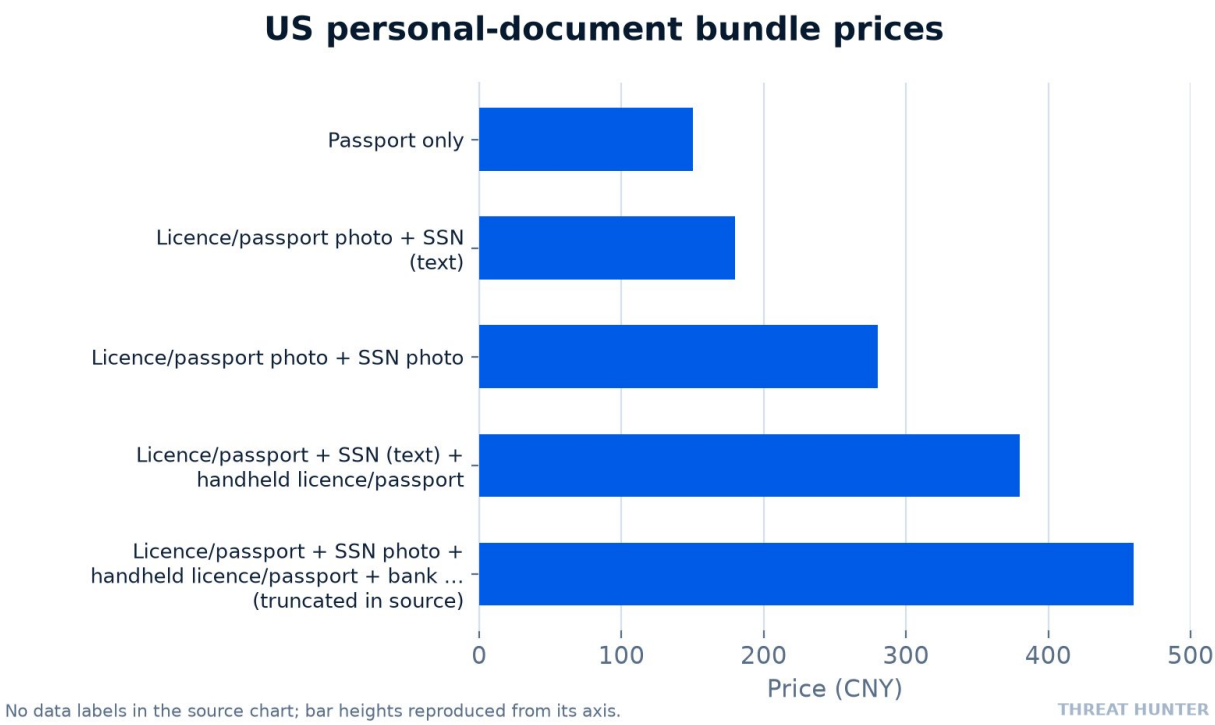
passport, 125 yuan to buy a Malaysian passport, and 120 yuan to buy a Philippine passport. In East Asian countries, it only costs 100 yuan to buy Japanese and Korean passports.



Single passport records sell for CNY 100–150, highest for European and American countries

Source: Threat Hunter original report, page 16. Redrawn in English from the original figure.

b. The United States is one of the countries where the largest number of combinations of personal data are sold. The price increases relatively as the types of materials increase.



In the United States, the price of a personal-document bundle rises as more documents are added

Source: Threat Hunter original report, page 16. Redrawn in English from the original figure.

(2) Sales of corporate data and information Since global e-commerce platforms usually require companies to provide relevant data before they can enter the platform, sales of corporate data and information occur frequently.

Threat Hunter found that there are five common types of combinations in corporate information sold by cybercrime ecosystem in various countries:

1 Enterprise business license + ein certificate/vat photo + legal person passport2 Enterprise business license + ein certificate/vat photo + legal person passport + bank statement within 6 months3 Enterprise business license + ein certificate/vat photo + legal person passport + legal person handheld passport4 Enterprise business license + ein certificate/vat photo + legal person passport + legal person handheld passport + bank statement within 6 months5 Enterprise business license + ein Certificate/VAT photo + legal person passport + legal person hand-held passport + legal person SSN photo + bank statement within 6 months. The specific price is as follows:

Average price of business document bundles

Bundle type	Average price
Business licence + EIN certificate / VAT photo + legal representative's passport	400
Business licence + EIN certificate / VAT photo + legal representative's passport + bank statement (last 6 months)	570
Business licence + EIN certificate / VAT photo + legal representative's passport + handheld passport photo	700
Business licence + EIN certificate / VAT photo + legal representative's passport + handheld passport photo + bank statement (last 6 months)	805
Business licence + EIN certificate / VAT photo + legal representative's passport + handheld passport photo + SSN photo + bank statement (last 6 months)	957.5

Unit not stated in the source table.

THREAT HUNTER

Prices of business document bundles sold for seller registration rise with each added document

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

2.1.2. During the registration stage, cybercriminal groups will provide business agent settlement services.

Merchant registration service mainly refers to sellers without corresponding qualifications purchasing invitation codes through investment managers, or using improper means such as cybercrime ecosystem to apply for registration, thereby bypassing the requirements of the e-commerce platform.

There are currently two main ways for merchants to register on behalf of merchants: 1. Use the invitation code of the investment manager to register; 2. cybercriminal groups provide false registration information to register on the platform.

(1) Use the invitation code of the investment manager to settle in

In order to attract high-quality merchants to settle in, e-commerce platforms often give investment managers a batch of invitation codes. When merchants with invitation codes settle in, the platform will provide certain discounts or privileges. For example, merchants can settle in quickly and easily get traffic tilt from the platform, etc.

In order to make profits, some investment managers choose to cooperate with threat actors. threat actors are responsible for finding merchants who want to enter the platform. The investment manager is mainly responsible for providing invitation codes to enter the platform. After merchants settle in, threat actors and investment managers will distribute the benefits. Therefore, there is a risk of internal and external collusion in the way of entering the platform through the invitation code of the investment manager.

(2) cybercriminal groups provide false entry information to assist sellers in entering the platform. cybercriminal groups' entry method mainly appears in cross-border store accounts of e-commerce, that is, stores that ship from China and sell into other markets. The cybercrime ecosystem proxy entry method provides entry services for users who do not understand the e-commerce platform, as well as some users who want to quickly enter the platform.

a. The price of entry varies according to the materials provided by the user.

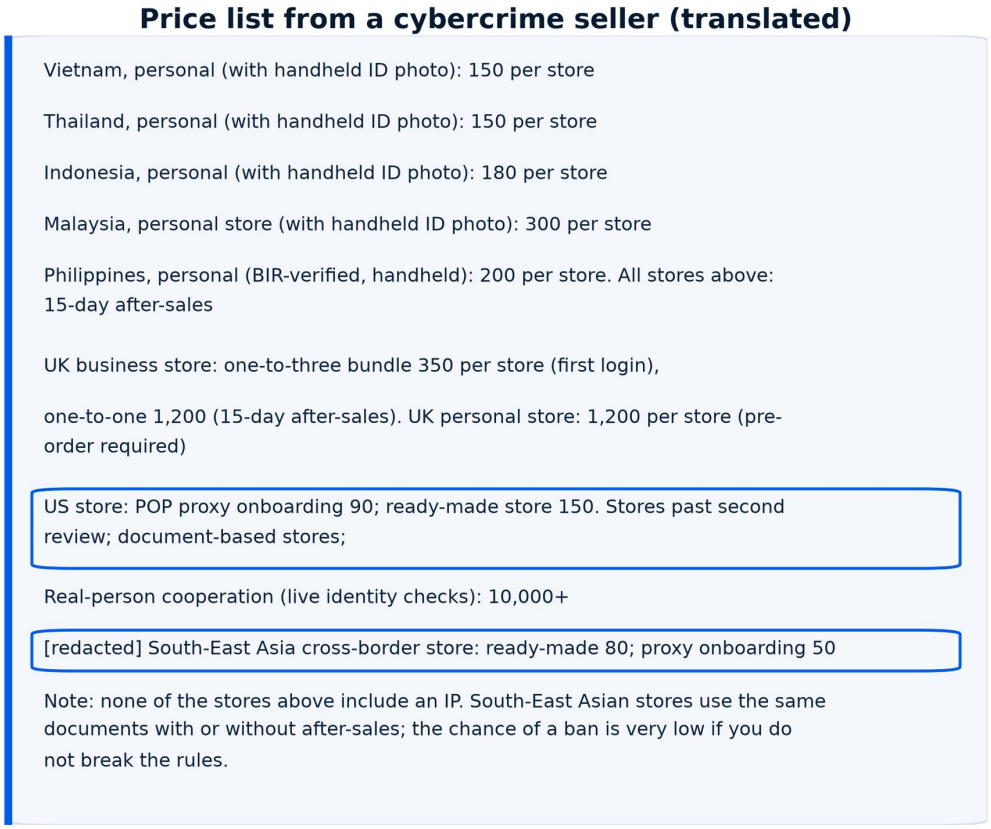
Taking an e-commerce platform as an example, if users only provide personal identity information, threat actors will use this information to register a business license and prepare documents such as bank statements and destination-market warehousing certificates. Therefore, compared to those users who provide complete materials, the price of entry for those who only provide part of the materials will be much higher.

b. The price of agency settlement varies greatly depending on the type and region, ranging from 50 yuan to 13,000 yuan. Such as:

- The cost of setting up an ordinary cross-border store in the United States is only 100-200 yuan. The registration materials required to open this type of store are only plain text information, such as ID card information, business license information, and a photo of the ID card in hand.
- Those with higher agency fees, such as cross-border crystal stores in the United States, where the agency fee is as high as 13,000 yuan. The registration materials required for this type of store are relatively complex. In addition to ID card information, business license information, and handheld ID photos, store statements, brand qualifications, product information and other materials are also required.
- In addition, the price of agents in Southeast Asia is generally lower than that in the United States. The registration price in Southeast Asia is 50 yuan.

The entry price for the US area is 90 yuan.

The following is a quotation from a cybercrime ecosystem, showing the specific price of selling store accounts:



A cybercrime seller's price list for seller-store accounts by country (highlights added by Threat Hunter analysts)

Source: Threat Hunter original report, page 19. Redrawn in English from the original figure.

2.1.3. Seller account transaction risks

The risk of seller account transactions means that cybercriminal groups obtains real-name authenticated accounts through batch registration and crowdsourcing, and sells them directly to users who want to join the platform, thereby bypassing the entry threshold.

(1) Account transaction According to the account type of each platform, there are various types of stores for sale. For example: the account types of a certain merchant’s finished product account transaction mainly include: cross-border store account, local store account, and brand store account. Among them, the brand store has the highest price, which costs 3,000 yuan. This is mainly because the qualifications of brand stores are not easy to obtain, the entry process is cumbersome, and the review is strict, resulting in relatively high prices. Prices at other local and cross-border stores range from 300 to 450 yuan. At the same time, the prices of local stores in different countries are also inconsistent.

(2) Local store account transaction price list, as shown in the figure below.



Local-store seller account prices differ by country, ranging from CNY 350 to 450 in the sample quotes

Source: Threat Hunter original report, page 20. Redrawn in English from the original figure.

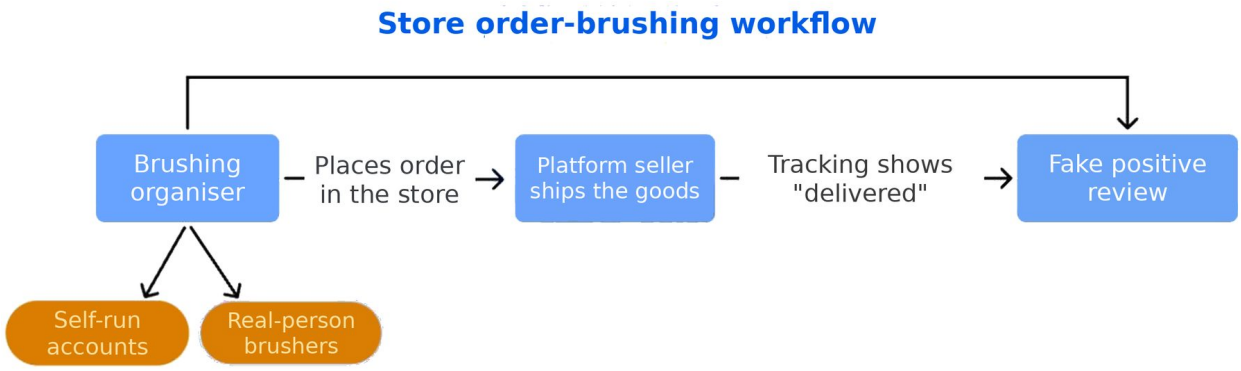
2.2. Risk analysis of shop fraud

Store fraud generally refers to the fraudulent practice of platform sellers paying to entrust cybercrime ecosystem fraud. They purchase goods from designated platform sellers through fraud tools and human-operated fraud, fill in false positive reviews to increase store sales, credibility and ratings, and gain platform traffic.

Shop fraud not only misleads consumers' shopping decisions, but also easily leads to unfair competition in stores, seriously affecting the normal operation of the platform. Global e-commerce platforms have long-term fraud controls on fraudulent orders, and the awareness of fraud controls among fraud groups has increased. The common machine fraud in the past has disappeared. Currently, there are two main types of order fraud services provided: self-supported account fraud and human-operated fraud.

(1) Self-supported account traffic manipulation: usually refers to the behavior of merchants using fingerprint browsers to purchase foreign servers and IPs to build a traffic manipulation environment to achieve batch registration of target platform accounts, account maintenance, browsing simulation, and order placing.

(2) human participant fraud: refers to the behavior of cybercrime ecosystem by hiring real users to pretend to be normal consumers to conduct false transactions on e-commerce platforms. These "swipers" usually follow the requirements of cybercrime ecosystem and use their real identity information, payment method and address to complete the purchase process on the e-commerce platform.

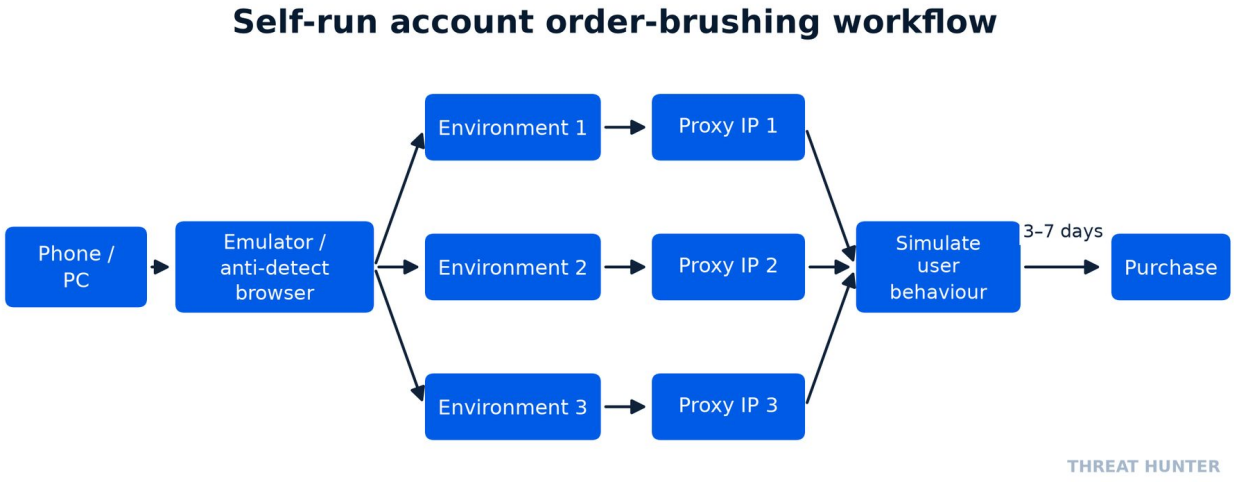


Fake store orders: the organiser places orders, the seller ships, and fake reviews follow once tracking shows delivery

Source: Threat Hunter original report, page 21. Original figure with Chinese text replaced by English.

2.2.1. Self-supported account traffic manipulation

Self-supported account traffic manipulation is relatively rarely used in China, but it is very common in cross-border e-commerce operations. This type of behavior usually teaches technology in the form of online and in-person instruction. cybercriminal groups provide a series of tutorials and tools to help users build self-built servers and order-traffic manipulation environments. Through these resources, users can complete a series of operations such as account registration, account maintenance, and order placement. Therefore, a complete set of order traffic manipulation procedures for self-supporting accounts has now been formed.



Fake orders from self-run accounts: device, anti-detect environment and proxy IP, then simulated browsing before purchase

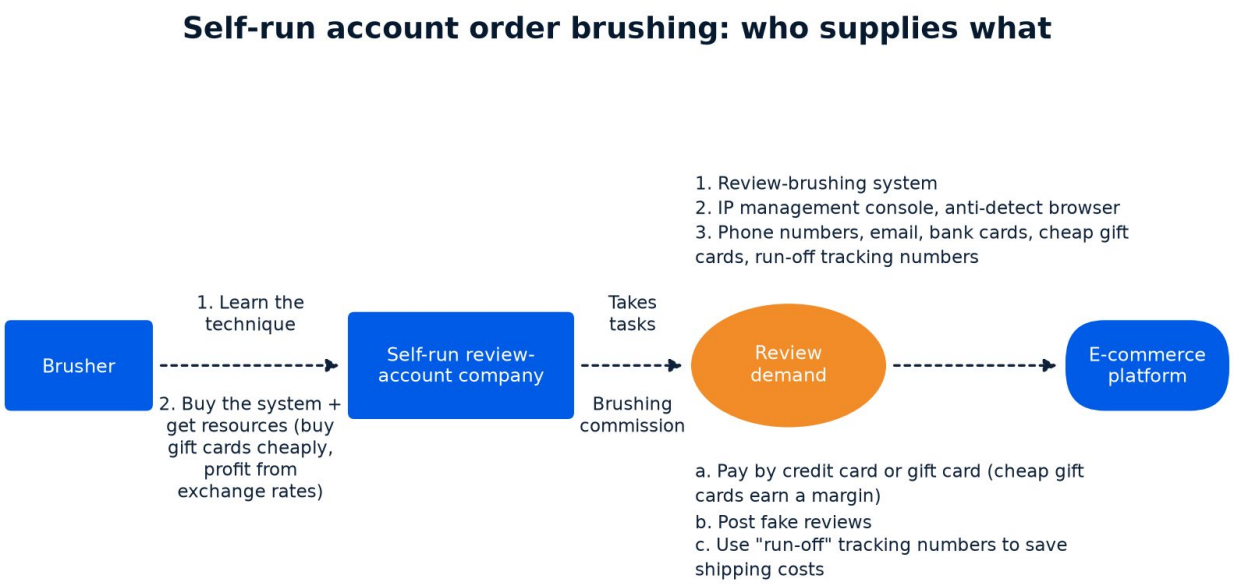
Source: Threat Hunter original report, page 21. Redrawn in English from the original figure.

(1) Threat Hunter, an analysis of self-supporting account technology incubation, found that the industry chain of self-supporting accounts is relatively complete, and there are evaluation technology incubation companies that specialize in selling tutorial technology. From the perspective of the entire self-supporting account industry chain, the profit from fake orders is composed of exchange rate difference + gift card price difference + fake order commission. The specific process is as follows.

1 The evaluation technology incubation company provides: foreign phone number, full set of identity information, gift card, scam number, IP, anti-correlation browser;

2 cybercriminal groups' profit from using a self-supported account to swipe orders consists of three parts, namely total profit = exchange rate difference + gift card price difference +

traffic manipulation commission.



Self-run accounts: fake-order operators buy systems and resources from review-account companies, then order, review and ship with run-off tracking numbers

Source: Threat Hunter original report, page 22. Redrawn in English from the original figure.

(2) Analysis of typical tools for self-supported account fraud cybercrime ecosystem In order to achieve unified management of multiple accounts, and isolate the environment and stable IP lines, "fingerprint browser" is generally chosen as the environmental basis for opening multiple stores. The fingerprint browser can ensure that each browser instance runs in an isolated environment, which means that each account runs in an independent browser to avoid the risk of accounts being associated and blocked.

Threat Hunter extracted 9 fingerprint browsers and analyzed their platform login methods, IP dimension usage, browser settings, and environment usage and found that:

a. How to log in to the platform: Analysis found that the fingerprint browser supports automatic login covering more than 100 e-commerce platforms, payment platforms, and mailboxes. For other platforms that do not support automatic login, you can also log in manually after creating a new browser.

b. IP dimension used: Through analysis of 9 fingerprint browsers, it was found that a total of 58 dynamic IP proxy platforms and 12 cloud service providers are supported. Among them, the cloud server platform supported by the most fingerprint browsers is a major US cloud provider, supported by 5 of them, followed by two major Chinese cloud providers, each supported by four.

c. Optional configurable browser settings:

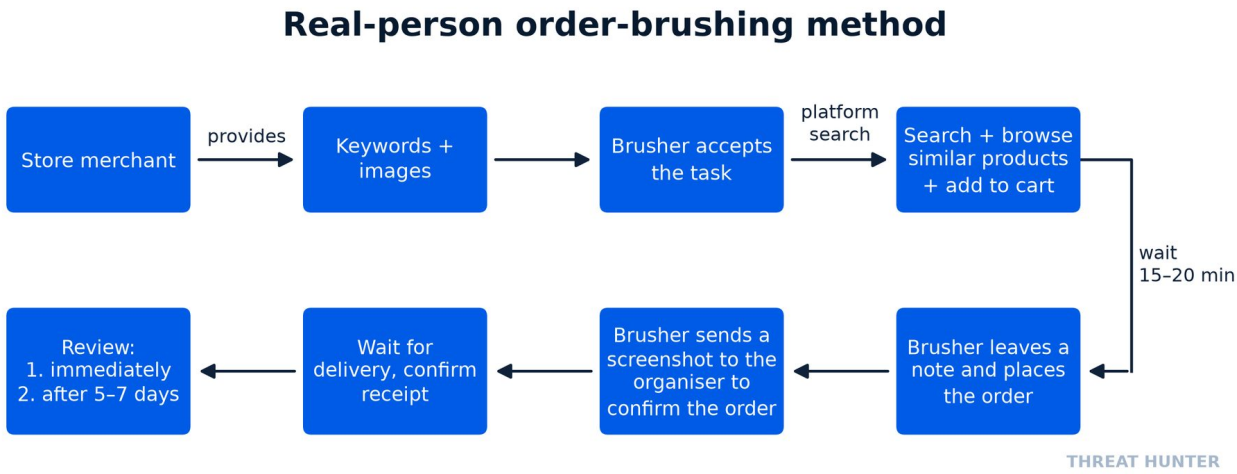
- Browser kernel version (you can select a specific version number)
- Operating system (optional: windows, mac OS, linux, Android, iOS)
- UA settings (version number and User-Agent can be set)
- WebRTC settings (can be set to hide real IP)
- Geographical location (the geographical location that follows the proxy IP can be set)
- Window size, resolution, font
- Port scanning protection
- Media device fingerprint settings: video input, audio output, audio input
- Hardware device settings (device name, MAC address, CPU core, device memory)

d. Environment usage: There are two usage methods:

- Open the browser directly and create a new environment for visual page use;
- Use the environment through the api interface.

2.2.2. human participant swiping orders (1) How to swipe orders

The cybercrime ecosystem traffic manipulation technique is shown in the figure below:



Fake orders by hired human buyers: the merchant supplies keywords and images, the buyer orders, confirms receipt and reviews

Source: Threat Hunter original report, page 23. Redrawn in English from the original figure.

(2) The Threat Hunter survey found that the price of traffic manipulation orders is the main influencing factor of the price is the content type and area of the review. There are currently four types of review content:

Star and rate comments, article comments, picture comments, and video comments. Taking the price in a certain area as an example, the price of a video review is up to 80 yuan. The price for giving stars and ratings is as low as 30 yuan. Price comparison is shown in the table below.



No data labels in the source chart; bar heights reproduced from its axis. Example region.

Review prices in one region: video reviews cost the most (CNY 80) and star-rating reviews the least (CNY 30)

Source: Threat Hunter original report, page 24. Redrawn in English from the original figure.

2.3. Logistics fraud risk analysis

Logistics fraud refers to e-commerce sellers using false delivery notes or technology express delivery notes to deliver goods in order to steal areas, steal weight or evade taxes and reduce sales costs. Once logistics fraud is detected by the logistics company, the goods may be seized, and the seller will need to pay the freight, which will not only seriously delay the delivery time of the goods, but also reduce users' confidence in the platform. In addition, sellers may also use false order numbers to obtain logistics subsidies and price difference benefits from the platform.

Currently, there are three main types of fraudulent logistics tracking numbers on the market: secondary tracking numbers, fraudulent tracking numbers, and technology tracking numbers.

(1) Secondary tracking number means that the logistics tracking number is leaked or sold by the logistics company for reuse.

a. Sales channel: cybercriminal groups sells through single-number sales websites or connects through private domain channels.

b. Conditions of use: The corresponding order number can be matched by delivery time, delivery address, shipping address, postal code, and even delivery time.

c. Update quantity: Taking the US logistics tracking number as an example, on a single sales tracking number website, more than 4,000 are updated every day.

A single number.

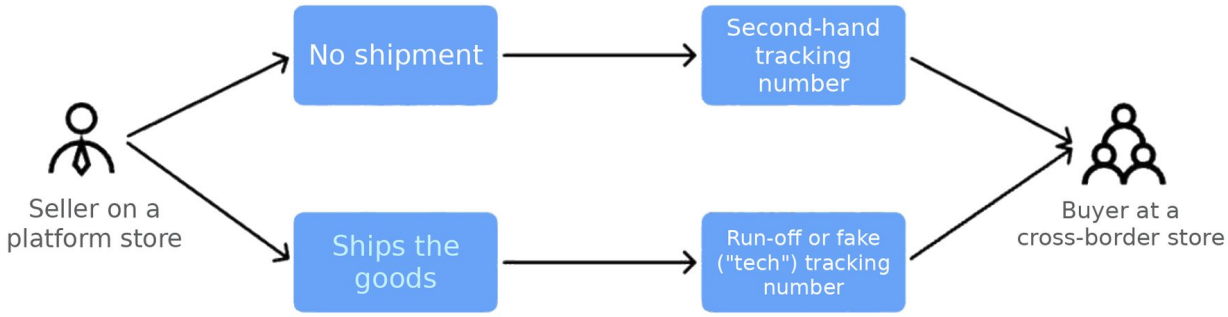
(2) Technology receipts refer to the express delivery receipts produced by cybercrime ecosystem after cracking the receipt generation rules. This type of receipt can be recognized by some tracking number scanners and the corresponding logistics order number and logistics track can be queried on the official website.

a. Current situation: Although after many upgrades and crackdowns by the US Postal Service, the number of such slips in circulation has been reduced, but there are still some cybercrime ecosystem claims that there are still available slip numbers.

b. Conditions of use: Print the order number through the actual address for actual delivery.

(3) Off-the-shelf order number refers to the order placed using the off-the-shelf account. The order itself is a regular order number, but because the associated ordering account defaults on freight or uses a fraudulent credit card to pay for freight, all documents and warehouses associated with the account are exposed to freight risks, resulting in losses and a certain probability of being punished.

a. Conditions of use: Print the order number according to the actual address and carry out actual delivery.

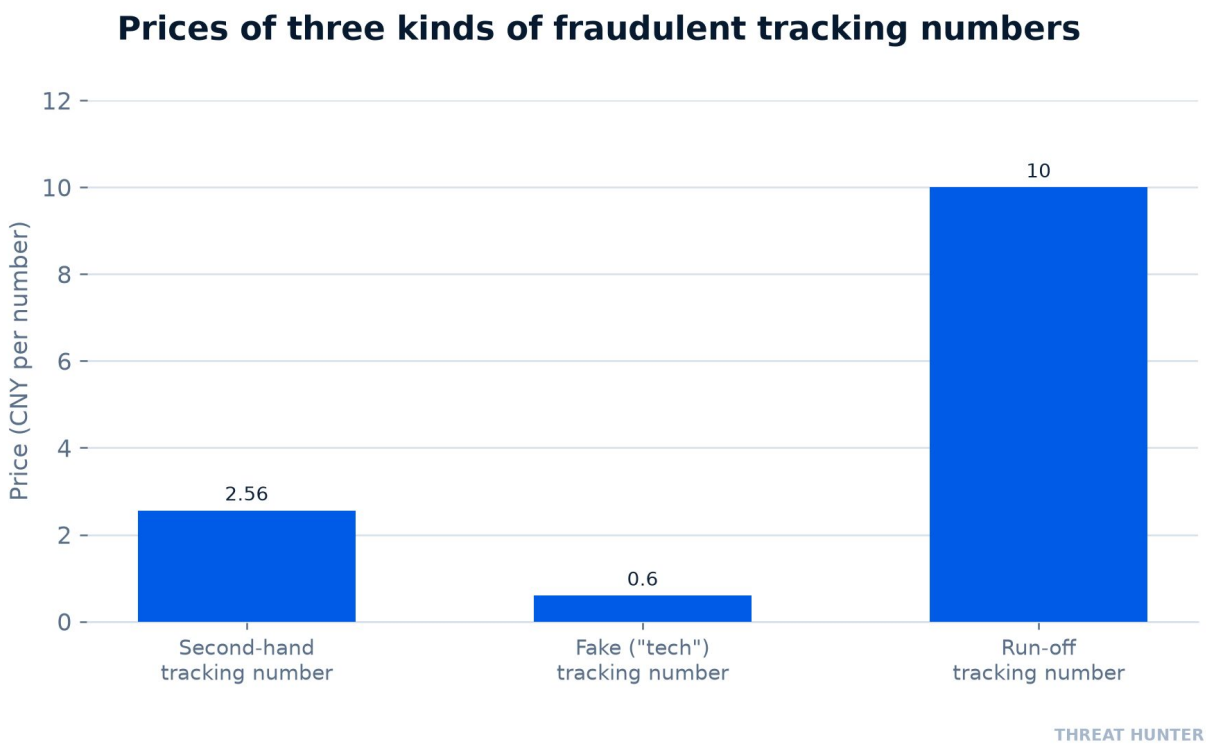


Logistics fraud: sellers either ship nothing and use a second-hand tracking number, or ship with run-off or fake tracking numbers

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

2.3.1. Logistics order number price

Among the above three types of fraud logistics tracking numbers, technology tracking numbers have the lowest price and can be purchased for only 0.6 yuan. This is mainly because technology tracking numbers are obtained by cracking tracking number rules, and the single cost is relatively low. Second is the secondary order number, with an average price of 2.56 yuan/order. The secondary order number matches the order number through shipping time, receiving address, shipping address, postal code and other information. The highest price is a shipping order number, with an average price of 10 yuan/order. A shipping order number requires a real delivery address for delivery, and the price will fluctuate based on the size and weight of the product.



Values from the report text (average price per tracking number).

Fake ("tech") tracking numbers are cheapest at CNY 0.6, second-hand numbers average CNY 2.56 and run-off numbers CNY 10

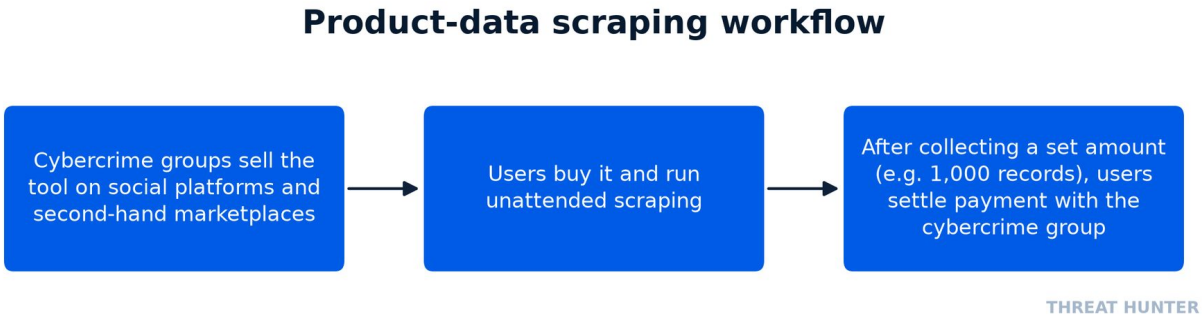
Source: Threat Hunter original report, page 26. Redrawn in English from the original figure.

2.4. Risk analysis of product information crawling

The risk of product information crawling refers to the risk of unauthorized crawler programs illegally obtaining product information on the e-commerce platform or website. This behavior may infringe copyright or intellectual property rights, may also lead to the leakage of sensitive data of the platform or merchants, and may also disrupt the normal market order by performing browser traffic manipulation operations on specific products.

The upstream cybercrime ecosystem mainly publishes posts related to making money through social platforms and second-hand trading websites, inducing users to use AFK tools to browse the number of products on the e-commerce platform and collect data. After the user collects a certain amount of data, unified settlement will be carried out.

For example, on an e-commerce platform, you can get a commission of 7 yuan for collecting 1,000 pieces of data.



Product-data scraping: cybercrime groups sell scraping tools, users run them and are paid per batch of records

Source: Threat Hunter original report, page 26. Redrawn in English from the original figure.

Examples of sales of related tools:



A scraping tool for sale: photo of many browser sessions running at once, and the second-hand marketplace listing (CNY 40)

Source: Threat Hunter original report, page 27. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Listing price: CNY 40
2	"3 people want this · 11 views"
3	Listing text: "Scraping, scraping. 1. Project: [redacted] collecting data for merchants; works on PC or phone, several instances at once. 2. Pay rate: [redacted] 70 per 1,000 records; [redacted] 10 per 1,000; [redacted] 10 per 1,000. 3. Payout: the platform pays automatically every Monday, Wednesday and Friday. Back-end access and script: 50 (repeated three times)."
4	Marketplace buttons: "I want it", "Order in app", "Save"

2.5. Malicious refund risk analysis

Malicious refunds refer to users applying for refunds through improper means to obtain undeserved benefits. This behavior will cause economic losses and other negative impacts to e-commerce platforms and merchants.

Common malicious chargeback behaviors include:

(1) False declaration that the goods have not been received: The user claims that the goods have not been received, but has actually received them, thereby requesting a refund;

(2) Falsely claiming quality problems: After receiving the goods, the user falsely claims that the goods have quality problems or are inconsistent with the description, and requires a refund or partial refund while retaining the goods;

(3) Deliberately damaged goods: The user intentionally damages the goods after receiving them, and then requests a refund on the grounds that the goods are defective.



Malicious refunds: after receiving the goods, users damage the packaging or goods or invent a quality problem to get a refund while keeping the item

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

cybercriminal groups will spread malicious refund methods through group chats and tutorials, such as selling refund tutorials on the cybercrime ecosystem website.

2.6. Authentication bypass risk analysis

Authentication refers to confirming a user's identity to determine whether they have the right to access and use specific resources. On e-commerce platforms, certification is mainly used to confirm whether the seller is qualified to open a store and ensure the normal operation of the store. However, in order to achieve the goal of opening stores in batches, the cybercrime ecosystem often tries to bypass identity authentication.

Authentication bypass refers to the behavior of cybercrime ecosystem using certain technical means or adopting non-compliant methods to evade authentication during the identity authentication process of e-commerce platforms.

2.6.1. Methods and techniques for authentication bypass (1) Live person bypass

When threat actors use human-in-the-loop crowdsourcing for account registration, they will sign a contract or agreement with the crowdsourcing personnel, requiring them to assist in completing the authentication process when encountering the authentication link, in order to achieve the purpose of bypassing authentication.



Chat with a seller of stores registered under genuine local identities: local people in the US and UK register the store and join live verification checks

Source: Threat Hunter original report, page 28. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Buyer: "Are stores of this type registered under genuine identities?"
2	Quoted reply: "Yes. Here is how it works: personal store 12,800; business store 35,800."
3	Buyer: "[They] can help pass verification at any time" (as written)
4	Seller: "We don't do POP stores; that kind of store gets banned a lot."
5	Seller: "Yes, they are registered under genuine identities, not document-based stores."
6	Quoted message: "Are stores of this type registered under genuine identities?"
7	Buyer: "You register them directly with local people? Can they help pass verification at any time? Is there an extra charge for verification?"
8	Seller (highlighted): "Yes. Registered with the real documents of local people in the US and UK; the registrant helps the store pass the second and third reviews; no extra fee for the reviews."
9	Seller (highlighted): "We will arrange the verification and cooperate at any time."

(2) Image synthesis bypass Image synthesis bypass refers to threat actors using technical means to synthesize photos into a video. When the platform requires authentication, the synthesized video is directly uploaded to the platform, thereby bypassing the requirements for real authentication.

The human-assisted bypass and image synthesis bypass methods are mainly used in the second review stage of the account. At this stage, the face information of the seller's account needs to be authenticated.

(3) Camera Bypass There are currently two types of camera bypasses discovered, namely: 1. Virtual camera bypass; 2. Camera hijacking bypass.

a. Virtual camera bypass Virtual camera bypass refers to threat actors using virtual camera software to replace the computer's own camera. In this way, the recorded video can be transmitted as a real-time video stream to bypass authentication.

Case: In this case, the virtual camera is recognized as a real camera in the system by hard modifying the XCMS tool and modifying the system driver. In this way, when the software and

platform call the camera, they will mistakenly think that the connected camera is a real one and accept its input.



Camera bypass, case 1: an advert for a hard-modded virtual-camera tool and the spoofed devices it adds to Windows Device Manager

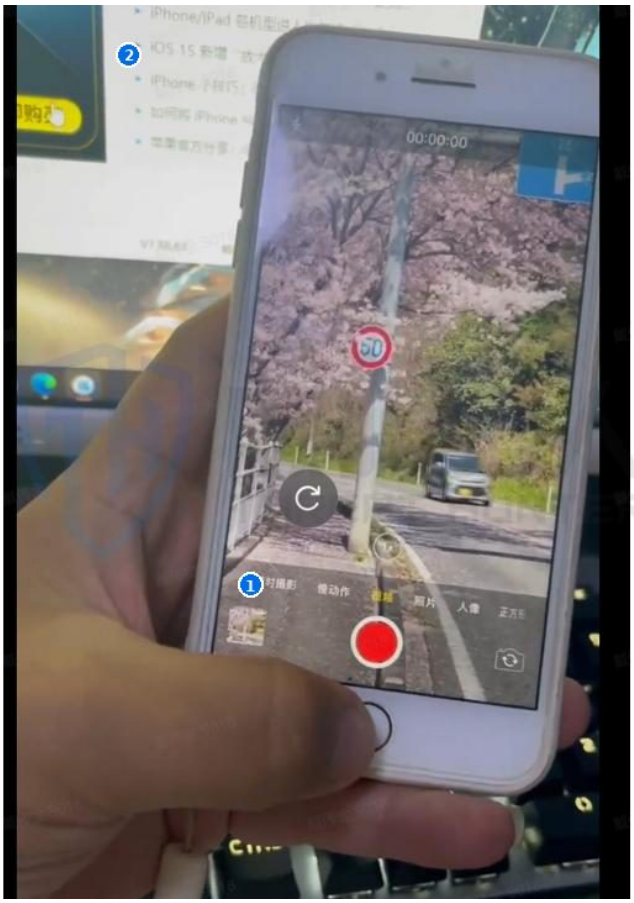
Source: Threat Hunter original report, page 29. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Advert headline: "Hard-modded XCMS" (tool name)
2	"Works on every platform / built for unattended live streams / makes your live room harder to take down"
3	Tool settings panel: camera selection, resolution and image-adjustment controls (labels too small to transcribe individually)
4	"Turns a virtual camera into a hardware camera to evade non-live-feed checks"
5	Windows Device Manager; menus: File, Action, View, Help
6	Audio devices "Speaker A" and "Microphone A"
7	Mice and other pointing devices; Universal Serial Bus controllers (incl. "Intel USB 3.10 eXtensible host controller", "USB Root Hub (USB 3.0)" and an "XCMS" device)
8	Network adapters; System devices; Display adapters
9	Audio inputs and outputs: Stereo Mix, "Microphone (Microphone A)", Microphone Array, Speakers, "Speakers (Speaker A)"
10	Red annotation in the original: "Generates real-looking microphone and camera devices"
11	Cameras: "ov9734_azurewave_camera", "Camera A", "Camera B"

b. Camera hijacking. Bypassing camera hijacking means that threat actors obtain the ROOT permissions of mobile phones, install specific software or plug-ins, record videos in advance and automatically load them into these software or plug-ins. When the platform performs authentication, the software or plug-in on the mobile phone will use the recorded video for authentication, thereby bypassing fraud-control measures. The application scenarios for camera bypass are e-commerce live streaming and traffic diversion scenarios.

Case: This case is realized through an app running on a 6s-generation or newer smartphone of a major brand. As shown in the figure below, the information captured by the camera in real time is replaced with video information recorded in advance.



Camera hijack, case 2: a phone camera feed replaced with pre-recorded video

Source: Threat Hunter original report, page 30. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Camera app mode bar: time-lapse, slow motion, video (selected), photo, portrait, square
2	Background screen: tutorial page for smartphone and tablet models (partly visible)

2.7. Risk analysis of internal and external collusion

Internal and external collusion refers to the secret collusion between cybercrime ecosystem and platform insiders, through improper behavior, to achieve the purpose of non-compliant entry into the platform, unblocking accounts, etc.

In the e-commerce scenario, internal collusion usually occurs in the following three scenarios: entering the investment invitation code on the platform, forcing the store account deposit to be withdrawn, and the store account being unblocked.

(1) Investment invitation code to enter the platform. The investment manager will sell the invitation code issued by the platform at a high price to users who want to enter the platform, or collude with threat actors to directly sell the invitation code to obtain profits. Usually, the price of investment invitation codes is relatively high. A recent case captured by Threat Hunter shows that the invitation code of an e-commerce platform was sold for as high as 80,000 yuan.

(2) Store account deposit forced withdrawal The store account deposit refers to a certain amount that sellers need to pay when registering on the platform to ensure that the store can operate normally. If there are violations in the account, the deposit may be banned, and e-commerce platforms generally prohibit withdrawal of deposits. However, some threat actors

By colluding with insiders, this deposit can be forcibly withdrawn, and the fee usually charged is about 30% of the deposit.

(3) Store account unblocking Store account blocking means that the seller triggers the platform's fraud-control rules due to improper operation or violation of regulations, and the account is blocked. However, some cybercrime ecosystem help stores unblock accounts by colluding with internal platform employees. It is worth mentioning that the unblocking of this kind of store account is not absolutely effective. When fake shipping is banned, it is usually impossible to unblock it.

Another situation is when the seller has exhausted the appeal opportunities provided by the platform (generally, the platform will give users two appeal opportunities)

If it still cannot be unblocked, at this time, criminals may also collude with internal personnel to assist the seller in unblocking the account for a fee.

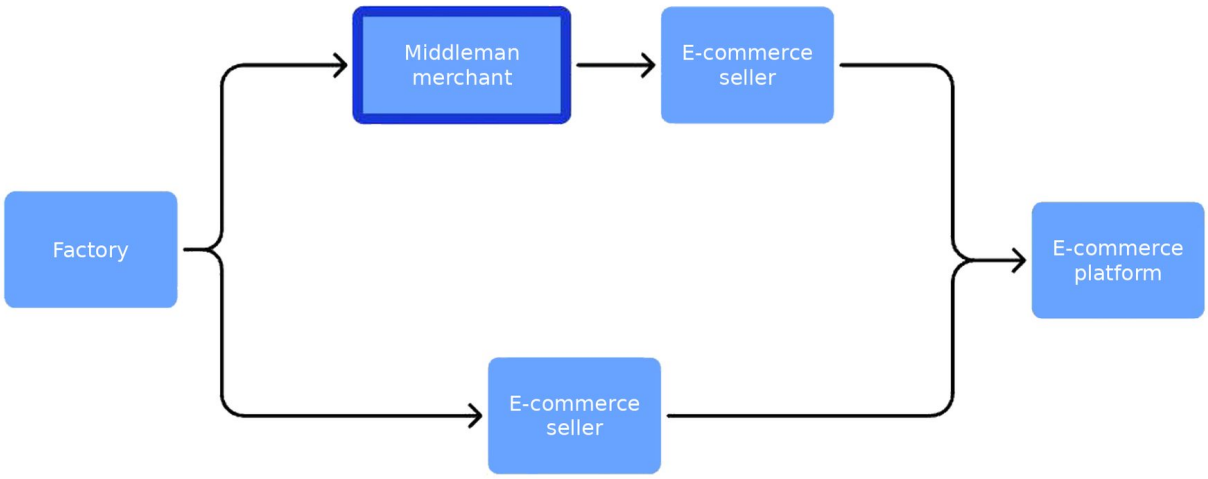
2.8. Pallet risk analysis

Pallets refer to companies transporting goods in batches and storing them in warehouses in the destination market for rapid distribution and sales to local or surrounding markets. However, some individual sellers are worried about poor sales after the goods are shipped abroad. Therefore, they will directly purchase pallets already stocked in destination-market warehouses, similar to the domestic no-source model. Although this can reduce the seller's financial risk, it can also easily lead to product quality problems and reduced fulfillment rates:

(1) Low-quality risk: The supply of pallets mainly comes from low-quality products or unsalable products sent directly from the factory. This type of pallet usually has no threshold and is a popular pallet. It is often tail goods, clearance goods, or products that have been removed from the shelves for various reasons. These products have quality hazards and are prone to consumer complaints.

(2) Decline in fulfillment rate: Since the pallets are managed by a third party, platform sellers cannot directly control the delivery and after-sales service of the goods, which may lead to a decrease in the seller's fulfillment rate.

At present, there are pallets found in the United States and Southeast Asia, and the product categories involved include daily household products, digital 3C, hardware supplies, pet supplies and other categories.



Product-sourcing (pallet) supply: goods reach e-commerce platforms from factories either directly through sellers or via middleman merchants

Source: Threat Hunter original report, page 32. Original figure with Chinese text replaced by English.

3. Conclusion

Through the above risk analysis, it is not difficult to find that global e-commerce is facing an increasingly complex and changeable risk environment. For platforms, cybercriminal attacks usually involve network attacks and marketing fraud, which may lead to financial losses and infringement of consumer rights. For enterprises, there may be operational financial risks such as blocked sales, frozen accounts, and blocked brands.

Global e-commerce platforms and enterprises need to remain vigilant against cybercrime ecosystem at all times, continuously improve their technical capabilities and risk management levels, and with the support of professional security intelligence vendors, establish more complete security protection and marketing fraud-control systems based on specific business scenarios, so that they can more comprehensively respond to threats from the cybercrime ecosystem and achieve healthy and sustainable development of their international business.