THREAT HUNTER RESEARCH

2025 Annual Cybercrime Ecosystem Trends Report

An annual assessment of malicious-resource shifts, AI-enabled automation, business fraud and brand abuse during 2025.

Original publication: 2026-01-11
Research team: Threat Hunter Research Team
Source report: 88 pages

Original report text

This text version is reconstructed based on the 88-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate 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.

About Threat Hunter

Threat Hunter was founded in 2017 and helps organizations identify and respond to business fraud, external digital risk, and API security threats. Its work combines cybercrime intelligence, risk data, product platforms, and specialist services.

The company provides mature and diverse products and services focusing on risk scenarios such as business fraud, data leakage, phishing and counterfeiting, and API attacks that different industries face in the process of digital development. It has been selected as a representative vendor in Gartner's technology maturity curve report and IDC's threat intelligence field for many times.

Headquartered in Shenzhen, Threat Hunter also operates offices in Beijing, Shanghai, and Chongqing, with Digital Risk Response Centers in Shenzhen and Chongqing. The company supports customers in China, Europe, the United States, South America, and Southeast Asia.

Preface

In the past year, the cybercrime ecosystem of the Internet has not retreated due to tighter supervision. Instead, it has undergone significant evolution in its resource structure, malicious methods, and technical paths.

务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85%头部互联网企业，每年帮助客户减少数十亿资金损失。

Original report charts, processes and cases

Source: Threat Hunter original report, page 2

Figure guide

1	Threat Hunter helps protect customers' business operations and data.
2	Threat Hunter has served more than 300 customers across finance, government services, logistics, internet, technology, and retail.
3	The report states that its services reach 85% of leading internet companies and help customers reduce financial losses.
4	Risk-data products, anti-fraud intelligence, data-leak intelligence, phishing and impersonation intelligence, API security, and specialist services.
5	24/7 Digital Risk Response Center (DRRC)
6	Open-source intelligence
7	Closed-source intelligence
8	Cybercrime-tool intelligence
9	Intelligence-led defense: identify attack surfaces before adversaries do.

Based on the continuous monitoring of the intelligence system of threat actors, Threat Hunter found that in 2025, cybercriminal groups are shifting from the traditional model of "stacking resources and manpower" to a stage of "human-like and intelligent malicious activity" that is more covert, lower-cost, and closer to real user behavior.

Summary of key points in the report:

Attack resource level: human-operated resources such as interception cards, hijacking agents, and human-in-the-loop crowdsourcing have replaced traditional SIM pool cards on a large scale; compared with the highly identifiable black resources in the past, these resources are closer to real

users and real device forms, significantly improving the concealment and survival period of attacks, and making traceability and governance more difficult.

Attack technology level: The explosion of generative AI and agent technology not only brings opportunities for business innovation, but also provides low-threshold, high-efficiency automated malicious tools for the cybercrime ecosystem. At the same time, in terms of non-AI technology, automated tools break through the "three-color glare" defense line of face liveness detection, and traditional defense strategies based on color matching face challenges. In terms of attack scenarios, · Business fraud: with high subsidies and high traffic scenarios as the core, threat actors systematically exploit marketing subsidies and business rules; threat actors automatically conduct malicious activity and enter the "agent stage."

· Credit fraud: The discussion volume on professional debt risks has increased by 168% compared with 2024. In terms of loan types, corporate loan fraud risks, credit loan fraud risks, and housing loan fraud risks rank among the top three; the risk value of malicious loan fraud in Guangdong far exceeds that of other regions.

· Phishing and counterfeiting: It has evolved from traditional "point linking" to "GEO poisoning" cognitive hijacking, which contaminates high-weighted information sources referenced by AI searches and induces users actively seeking help to call fake customer service numbers.

· Data leakage: The risk of leakage is highly concentrated in the "pan-financial" sector, and threat actors have entered a new stage of using AI models to clean and quality control high-value data such as "finance applications" to improve the fraud conversion rate.

In the face of the evolving cybercrime ecosystem threats, Threat Hunter released the "2025 Internet cybercrime ecosystem research report". Based on the massive risk data and typical case analysis captured by the platform, it presents a panoramic view of the current development trend of threat actors from dimensions such as attack resources, technology evolution, and key scenarios. It aims to provide practical intelligence support for fraud-control development in various industries and help improve the insight and defense against new threat actors.

Analysis of attack resources used by cybercriminal groups in 2025

1. Analysis of attack resources used by cybercriminal groups on the Internet in 2025

1.1 Analysis of malicious mobile-number resources in 2025

1.1.1 The number of new domestic malicious phone numbers exceeded 11 million in 2025, an increase from 2024

Reported share: 30.02%

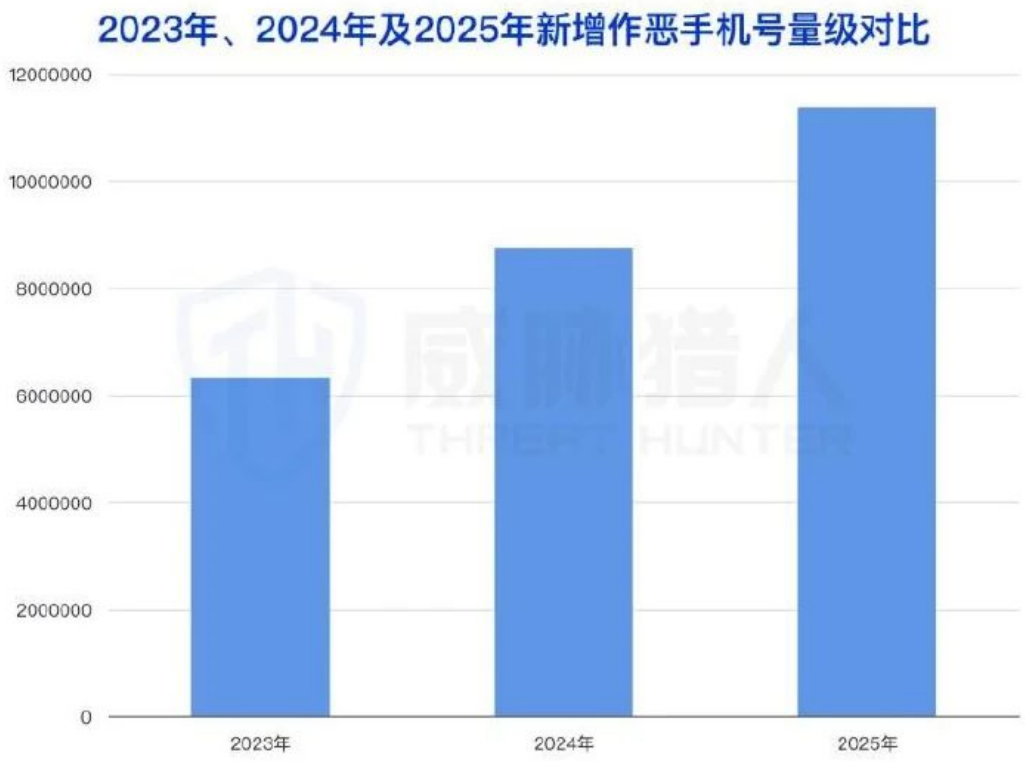
According to data from the Threat Hunter intelligence platform, the number of newly identified malicious mobile numbers in China exceeded 11 million in 2025, up 30.02% from 2024.

There are two main types of mobile-number resources used by threat actors to conduct malicious activity:

SIM-pool cards: Threat actors load physical SIM cards into multi-slot SIM-pool devices to send and receive SMS verification codes at scale. These cards are a traditional source of verification-code numbers.

Interception SIM cards: A physical SIM remains in a genuine user's device, but malicious software or a compromised component intercepts incoming SMS verification codes and relays them to threat actors.

According to data from the Threat Hunter intelligence platform, interception SIM cards accounted for 69.23% of newly identified malicious mobile numbers in China in 2025, up from 39.5% in 2024. Sections 1.1.2 and 1.1.3 examine changes in SIM-pool cards and interception SIM cards in greater detail.



Newly identified malicious mobile numbers increased for a third consecutive year and exceeded 11 million in 2025.

Source: Threat Hunter original report, page 5

Figure guide

1	New malicious mobile numbers identified in 2023, 2024, and 2025

1.1.2 Change trend of domestic SIM pool cards resources in 2025

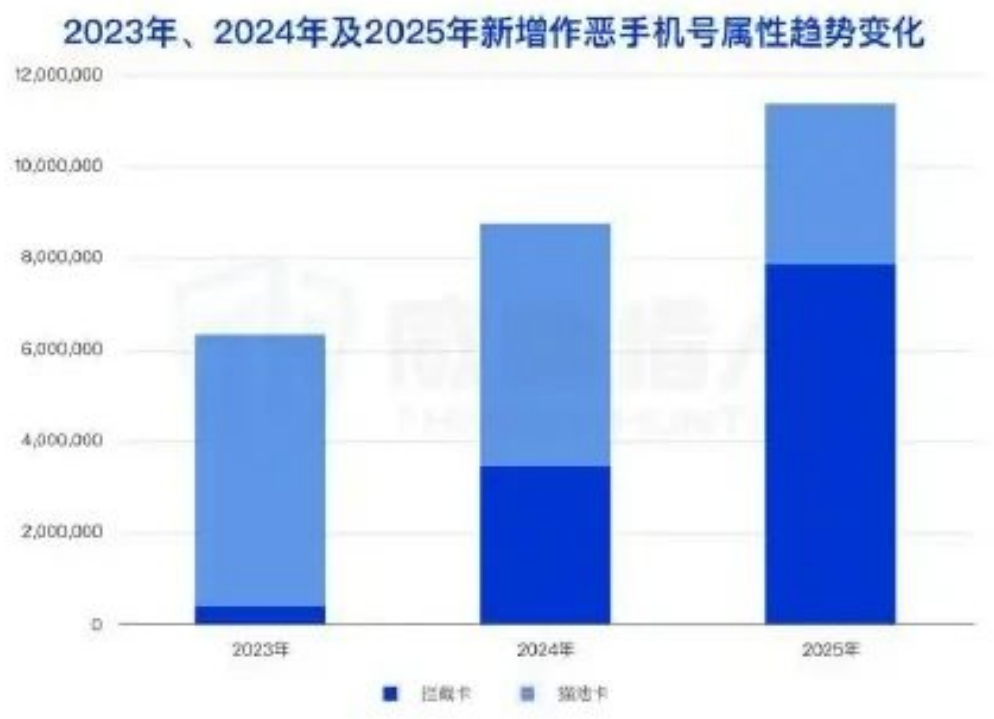
(1) There were 3.49 million new SIM pool cards in the country in 2025, a 33.85% decrease from 2024. According to data from the Threat Hunter intelligence platform, 3.49 million new SIM pool cards were captured in the country in 2025, a decrease of 33.85% from 2024.

Judging from the changing trend of the number of domestic SIM pool cards in 2025, since April, the number of new domestic SIM pool mobile phone cards has shown a downward trend.

According to analysis by Threat Hunter intelligence experts, the main reasons for this trend are:

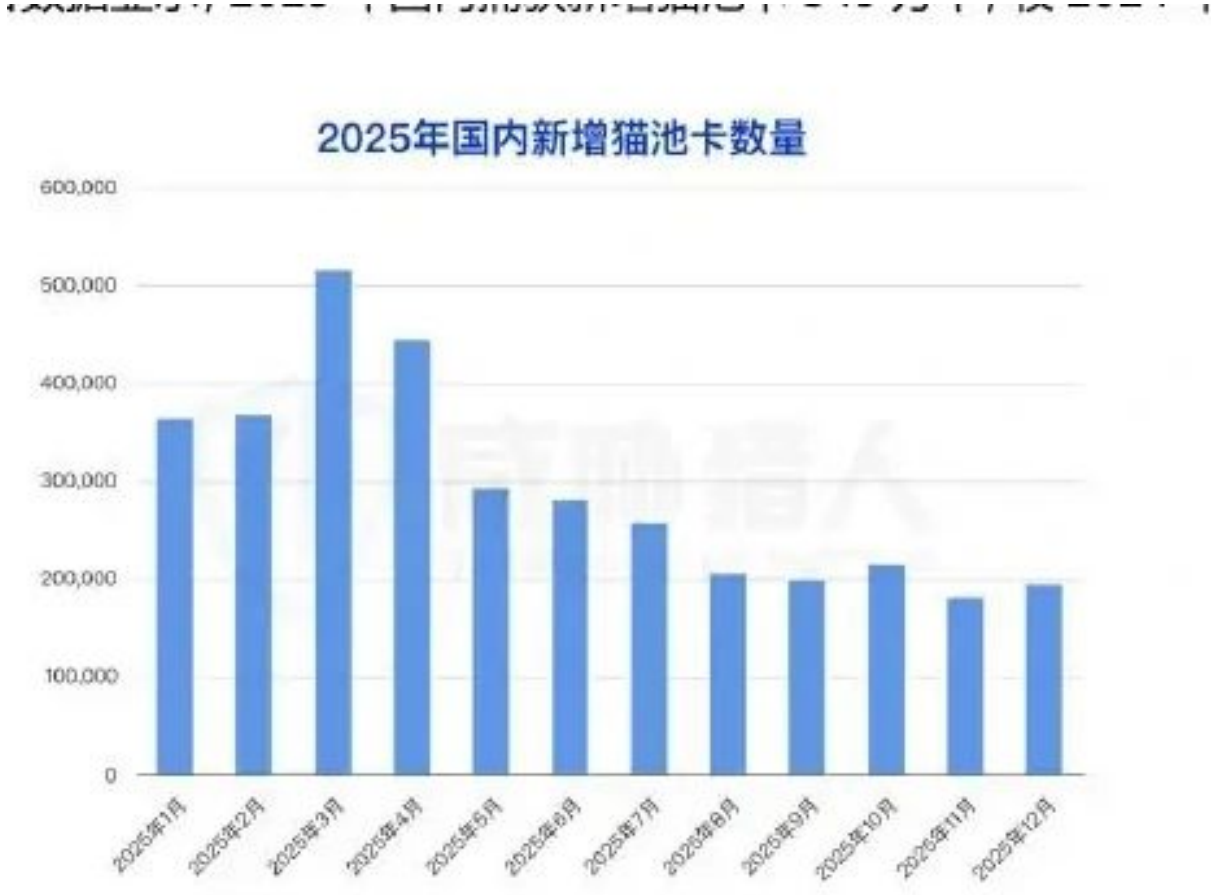
1. The supply of upstream black card dealers shrinks

Affected by regulatory crackdowns, many card dealers' computer rooms were shut down and some card dealers were arrested. The overall supply capacity of SIM pool cards has shrunk significantly, which directly led to a decrease in the number of new SIM pool cards.



Trends in domestic SIM pool card resources, 2025 (Chart 1)

Source: Threat Hunter original report, page 7



Trends in domestic SIM pool card resources, 2025 (Chart 2)

Source: Threat Hunter original report, page 7

According to Threat Hunter monitoring data analysis, Shanghai card dealers have become the leading card source for SIM pool cards supply in recent years. From January to April 2025, the number of new SIM pool cards in Shanghai continued to rise and reached a phased peak in March. The new SIM pool cards from Shanghai in that month accounted for 1% of the total new domestic SIM pool cards.

23.42%.

However, in the intensive regulatory crackdown in May 2025, Shanghai card dealers were the first to be hit. Many computer rooms were shut down and card dealers were arrested, which led to a rapid contraction of the supply side and a decrease in the number of new SIM pool cards. In May, only 8.32% of the new domestic SIM pool cards came from Shanghai.

The number of new black cards in Shanghai dropped sharply during the regulatory crackdown, leading to a decline in the overall number of SIM pool cards nationwide.

2. A mainstream SMS verification-code receiving service ceased operations.

新增猫池卡数量下降。

威胁猎人监控数据分析，上海卡商近年跃升为猫池卡供应的头部卡源。2025 年 1—4 月期间，上海地区猫池卡新增数量持续上升，并于 3 月达到阶段性峰值，当月来自上海的新增猫池卡占国内新增总量的 23.42%。

然而，2025 年 5 月监管集中打击行动中，上海卡商首当其冲受创，多个机房关停、卡商被捕，导致

Trends in domestic SIM pool card resources, 2025

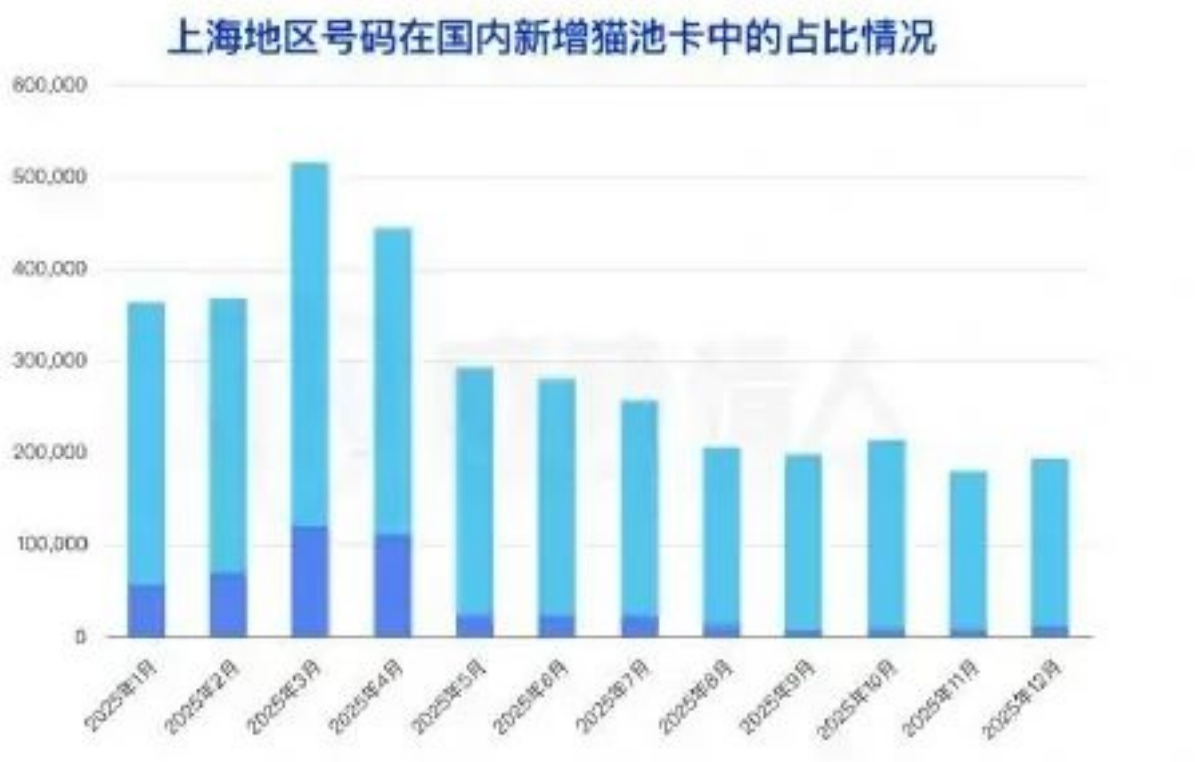
Source: Threat Hunter original report, page 8

From January to September 2025, monitoring of a major SMS verification-code receiving service identified more than one million SIM-pool cards supporting cybercriminal verification workflows.

However, during the year, the platform experienced frequent server fluctuations, and the stability of the platform dropped significantly, resulting in a sudden drop in the success rate of receiving codes, and the daily illegal operation rhythm of threat actors was continuously disrupted; after entering September, the platform finally stopped operations completely; this further blocked the downstream black card supply link.

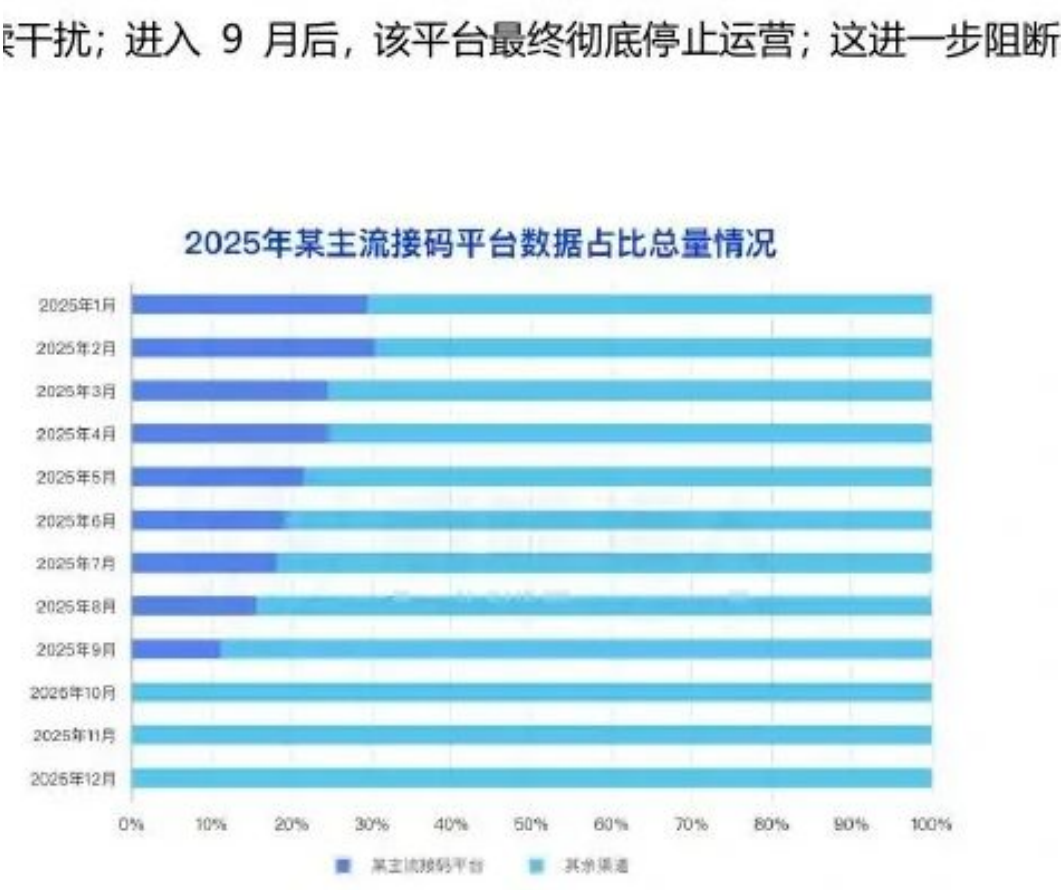
(2) Top 3 provinces for new domestic SIM pool cards in 2025: Chongqing, Shanghai, and Guangdong. The number of new SIM pool cards belonging to the Chongqing area rose from ninth in 2024 to first in 2025. Threat Hunter conducted a statistical analysis of the new domestic SIM pool cards in 2025 and found that Chongqing, Shanghai, and Guangdong (including municipalities directly under the Central Government) are the three provinces with the largest number of SIM pool cards.

Among them, the number of SIM pool cards located in Chongqing increased by 106.63% compared with 2024, and the ranking increased by 8 places compared with 2024.



Trends in domestic SIM pool card resources, 2025 (Chart 1)

Source: Threat Hunter original report, page 9



Trends in domestic SIM pool card resources, 2025 (Chart 2)

Source: Threat Hunter original report, page 9

Threat Hunter noticed that this year, the number of SIM pool cards in Chongqing has remained relatively high in every month throughout the year.

Trends in domestic SIM pool card resources, 2025

Source: Threat Hunter original report, page 10

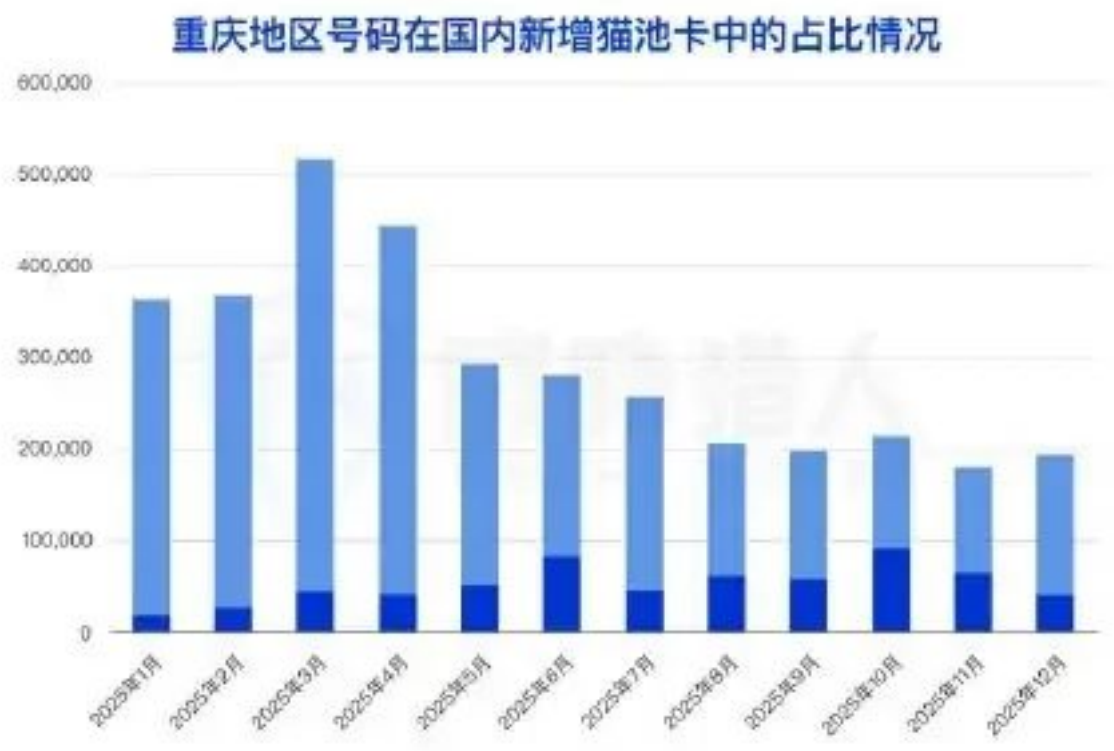
Threat Hunter researchers further analyzed and found that the distribution of new SIM pool cards operators in Chongqing shows obvious phased migration characteristics. During the period from March to June, the newly added SIM pool cards mainly belonged to operator D, and reached the peak in June; but after entering July, the source of its operators changed significantly and quickly concentrated on operator A.

(3) The proportion of new domestic SIM pool cards belonging to the three major operators in 2025 is 71.77%, 4.65% lower than last year. Threat Hunter intelligence data shows that among the new SIM pool cards monitored in 2025, the proportion of SIM pool cards belonging to the three major operators is

71.77%.

1.1.3 Change trend of domestic mobile phone card interception resources in 2025

(1) There were 7.86 million new domestic interception cards in 2025, an increase of 127.77% compared with 2024. According to data from the Threat Hunter intelligence platform, the number of new domestic interception cards captured by Threat Hunter increased significantly in 2025, reaching 7.86 million cases, an increase of 127.77% compared with 2024. Behind the surge in popularity of interception cards is the fact that more and more companies have strengthened fraud controls over traditional code-receiving phone numbers. Coupled with the gradual decline in the number of traditional code-receiving phone numbers, threat actors can only turn to interception cards that are "more like human participants".



Trends in domestic SIM pool card resources, 2025

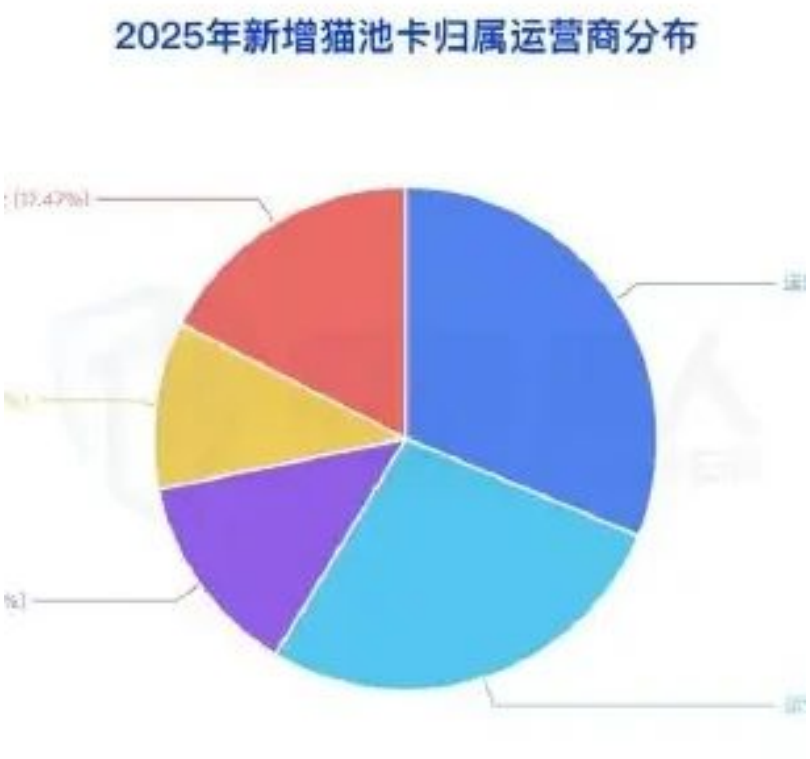
Source: Threat Hunter original report, page 11

Further analysis of the supply of cybercrime ecosystem interception cards shows:

Intercepting cards is an malicious activity act carried out by threat actors using specific "black card materials". The physical number card is held by ordinary people, but the device used by the user is implanted with viruses or backdoors by threat actors or device companies, causing the permission to receive SMS messages to be stolen, and then the verification code SMS messages are hijacked. Most of these devices are low-end devices such as mobile phones for the elderly and watches for children.

Since 2024, threat actors related to interception cards have shown a cycle of "strike-shrink-rebound" - the platform will quickly hide after being hit, and after the blow weakens,

the malicious activity links will be quickly restarted, making it difficult to eradicate the behavior of this type of threat actors from the source.



Trends in resources for the domestic interception of mobile cards, 2025

Source: Threat Hunter original report, page 12

From the second half of 2024 to the first half of 2025, mainstream interception card platforms continued to be attacked by regulatory forces, resulting in a significant decline in the scale of the card supply side.

From January to April 2025, of the six originally active card interception platforms (card supply channels), only two remained in a semi-stagnant state;

持。此类设备多为老人机、儿童手表等低端设备。

Trends in resources for the domestic interception of mobile cards, 2025

Source: Threat Hunter original report, page 13

In late May, monitoring revealed that 4 new card supply channels had been added, and the 2 card supply channels that had been in a semi-stagnant state before, threat actors changed their domains.

After renaming and receiving the code tool, it will be active again.

After threat actors completed the preliminary preparation work, they began to supply cards in large quantities in September, and the number of active interception card platforms on the market increased significantly.

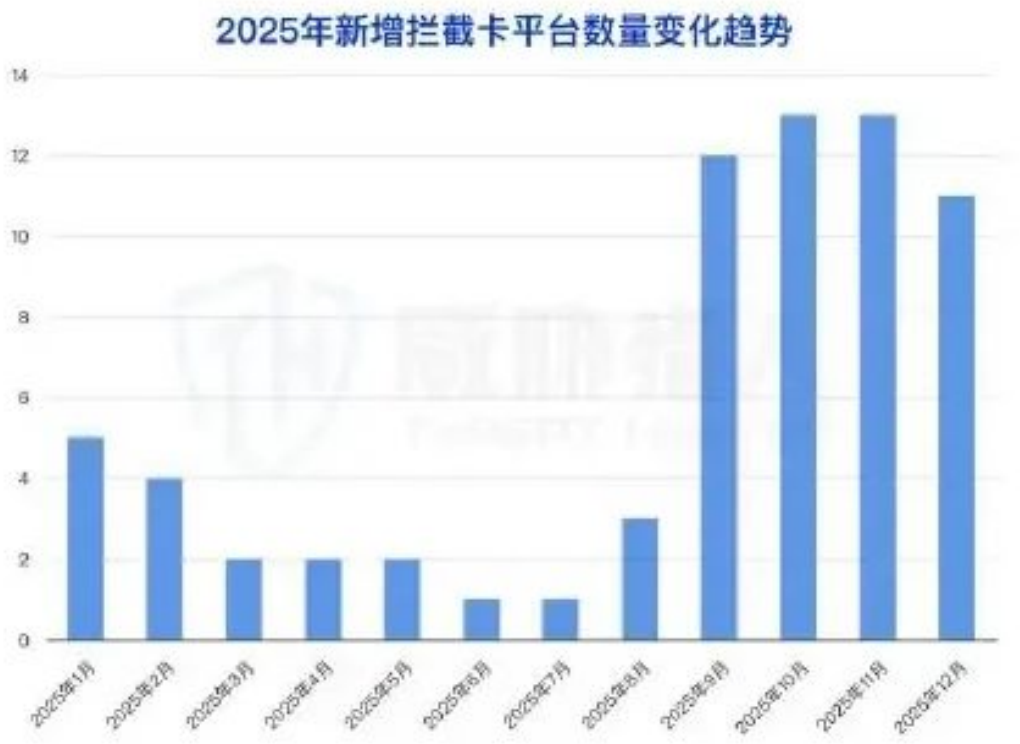
Comparison of the advantages and disadvantages of intercepting phone numbers and SIM pool cards:

Threat Hunter's research found that with the core feature of "SIM cards registered to genuine users", threat actors have gradually abandoned the use of traditional SIM pool cards in their malicious activities in multiple industries, and instead used interception card phone numbers to conduct malicious activity. The difference between this and traditional code-receiving phone numbers is shown in the figure below.

From the above comparison, it can be seen that interception cards have the characteristics of high concealment, similar to real users, and difficult corporate fraud controls, which greatly improves the success rate of threat actors in conducting malicious activity. Some threat actors are committed to seeking high-quality interception cards for use in malicious activity attacks.

(2) Top 3 provinces to which new domestic interception cards belong in 2025: Guangdong, Henan, and Sichuan A statistical analysis of the domestic interception cards captured in 2025 found that Guangdong, Henan, and Sichuan are the three provinces with the most interception cards.

(3) Among the new interception cards captured in 2025, 97.8% belong to the three major domestic operators



Trends in resources for the domestic interception of mobile cards, 2025

Source: Threat Hunter original report, page 14

Threat Hunter intelligence data shows that among the new interception cards captured in 2025, interception cards belonging to the three major domestic operators accounted for 97.8%, while the proportion of traditional code-receiving phone numbers belonging to the three major operators was 71.77%. This is one of the reasons why interception cards are different from traditional code-receiving phone numbers and are more like "human participants".

1.1.4 In 2025, there were a new method for threat actors to conduct malicious activity through human-in-the-loop crowdsourcing type SMS verification-code receiving services.

类型	拦截卡	猫池卡
持有人	正常人持有	黑产持有
号码来源	黑产通过低端设备后门窃取	卡商通过营业厅内鬼、地推等方式办新卡
卡获取难度	低；只要有人购买设备插卡即可获取卡	高；需有特殊身份或诱导正常人办卡获取卡
运营商特征	地区分散	地区集中，通常为新卡

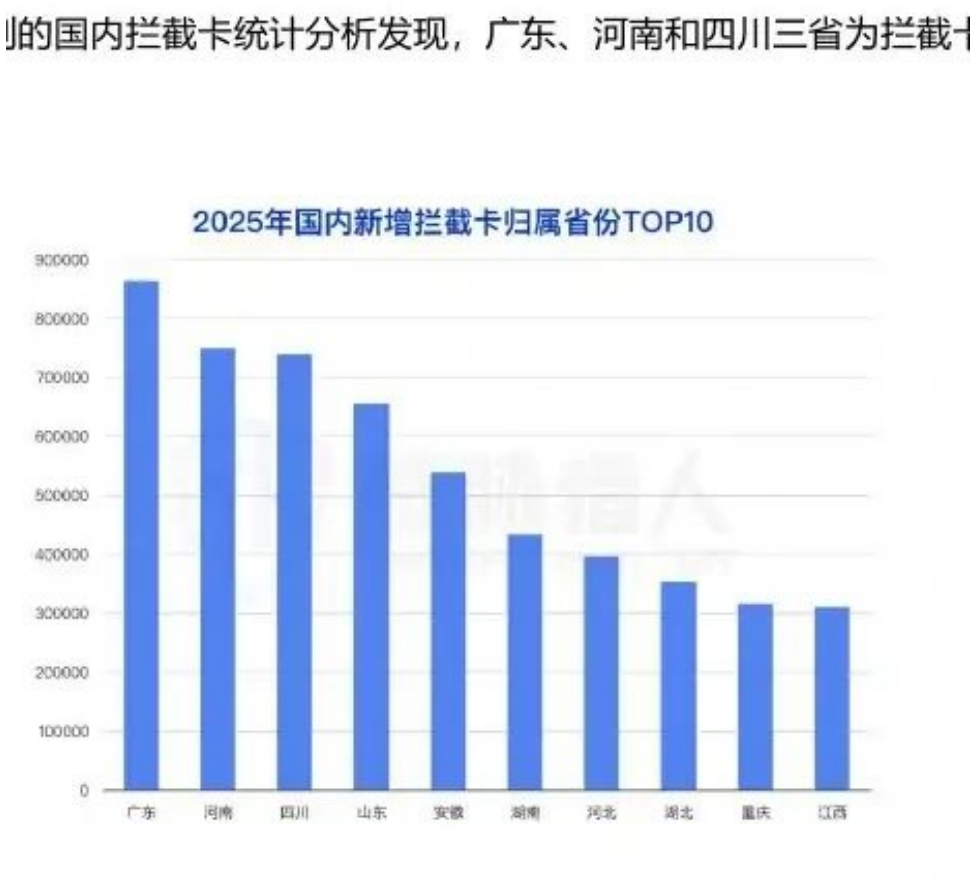
上述对比可见，拦截卡具备隐蔽度高、和真人用户相仿、企业风控难度大的的特点，使得黑

Trends in resources for the internal interception of mobile cards in 2025 (Chart 1)

Source: Threat Hunter original report, page 15

Figure guide

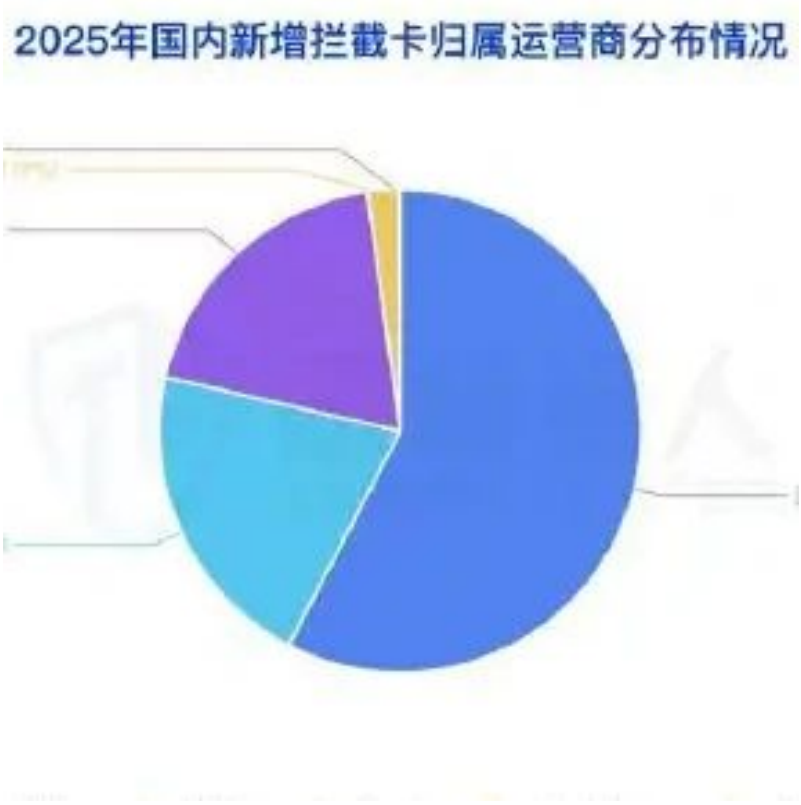
1	Comparison of interception SIM cards and SIM-pool cards
2	Resource source
3	Cybercriminal groups obtain cards through low-cost devices or insider channels
4	Card dealers acquire new cards through business-hall insiders and offline promotion
5	Difficulty of obtaining cards
6	Low: a willing cardholder can provide the card
7	High: requires identity theft or inducement of a genuine user
8	Carrier characteristics
9	Geographically dispersed
10	Concentrated by region and usually newly issued
11	Resource-control comparison



Trends in resources for the internal interception of mobile cards in 2025 (figure 2)

Source: Threat Hunter original report, page 15

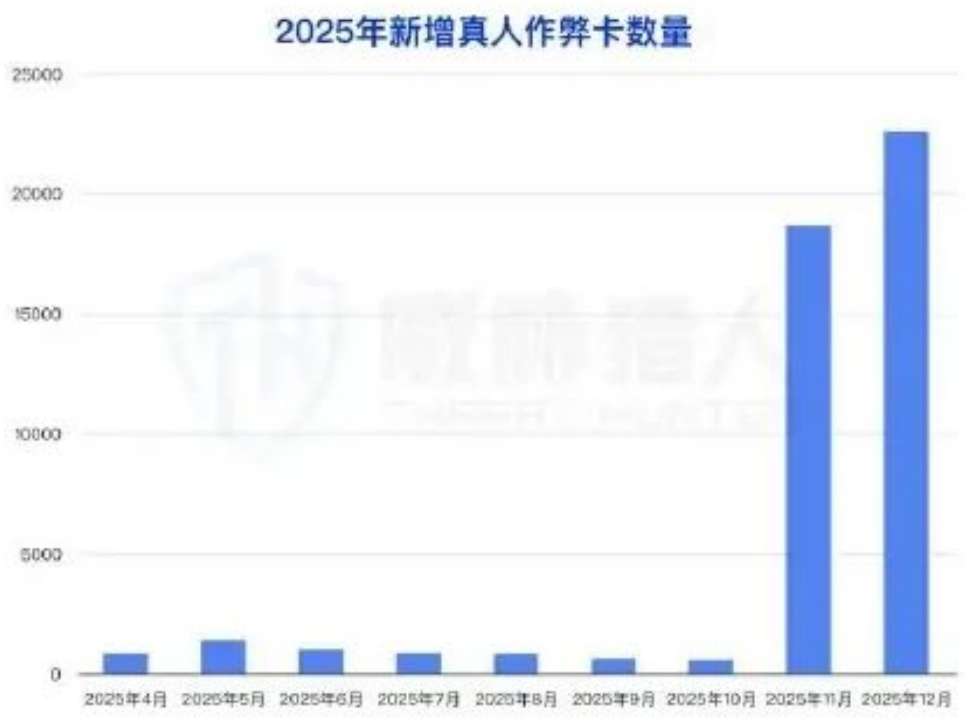
Through research on human-operated fraud number resources, Threat Hunter found that there were multiple human-in-the-loop crowdsourcing code-receiving platforms for malicious purposes in 2025, and the trend of threat actors using human-in-the-loop crowdsourcing platforms to conduct malicious activity is on the rise.



Trends in resources for the internal interception of mobile cards in 2025 (Chart 1)

Source: Threat Hunter original report, page 16

平台进行作恶趋势上涨。



Trends in resources for the internal interception of mobile cards in 2025 (figure 2)

Source: Threat Hunter original report, page 16

human-operated fraud refers to cybercrime ecosystem recruiting a large number of real part-time users such as mothers and students through crowdsourcing platforms, private domain groups or special apps, etc., and allowing these users to use their real accounts and devices to complete various illegal or false tasks to earn commissions.

Common ones include boosting popularity in live broadcast rooms, boosting orders on e-commerce platforms, boosting likes and comments on short videos, as well as malicious reports, batch registration of accounts, simulated users to crawl platform data, etc.

The human-in-the-loop crowdsourcing code-receiving platform uses "low-threshold part-time jobs, instant settlement commissions" as bait, attracting a large number of ordinary people seeking sideline income to register and participate. Driven by interests, many participants gradually become "tools" of threat actors and flock to the platform to carry out illegal and malicious activities such as batch code-receiving, account registration, and verification code reselling.

Example of human-in-the-loop crowdsourcing SMS verification-code receiving service:

Compared with the traditional SIM pool cards platform and interceptor card platform that use exclusive verification-code reception tools to receive codes, the advantages of this model are:

- Higher concealment. Using a phone number registered to a genuine user can circumvent the fraud-control monitoring of most platforms, making it more difficult for companies to identify;

真人作弊是指黑灰产通过众包平台、私域群组或专项 APP 等渠道，招募宝妈、学生等大量真实兼职用户，让这些用户用自己的真实账号和设备，完成各类违规或虚假任务以赚取佣金这些任务。常见的有直播间刷人气、电商平台刷单、短视频刷赞刷评，还包括恶意举报、批量注册账号、模拟用户爬取平台数据等。

真人众包型接码平台以“低门槛兼职、即时结算佣金”为诱饵，吸引了大量寻求副业收入的普

New methods of hacking through real-people-packaged-type interfaces in 2025 (Chart 1)

Source: Threat Hunter original report, page 17

验证码倒卖等违规作恶行为。

平台样例：

A task-platform example showing app selection and verification-code submission in a human-operated fraud workflow.

Source: Threat Hunter original report, page 17

- More convenient to use. threat actors only need to publish crowdsourcing tasks and do not need to issue cards in batches or find card vendors to supply cards;
- The price is cheaper. Human-operated fraud does not require additional hardware investment, and only needs to be settled in the form of commissions to part-time users, and the commissions can be paid flexibly based on the results of task completion, without having to bear hidden losses such as equipment depreciation and card source failure.

1.1.5 Resource Analysis of “Malicious Mobile Phone Numbers from Non-Mainland China” in 2025

- Non-mainland China: refers to Hong Kong, Macau, Taiwan and overseas regions (1) In 2025, 26.22 million new SIM pool cards were added in non-mainland China, an increase of 117.81% from 2024. In 2025, Threat Hunter strengthened the monitoring of malicious phone numbers around the world. In 2025, 26.22 million new SIM pool cards were added in Hong Kong, Macao, Taiwan and overseas regions, an increase of 117.81% from 2024. 117.81%.

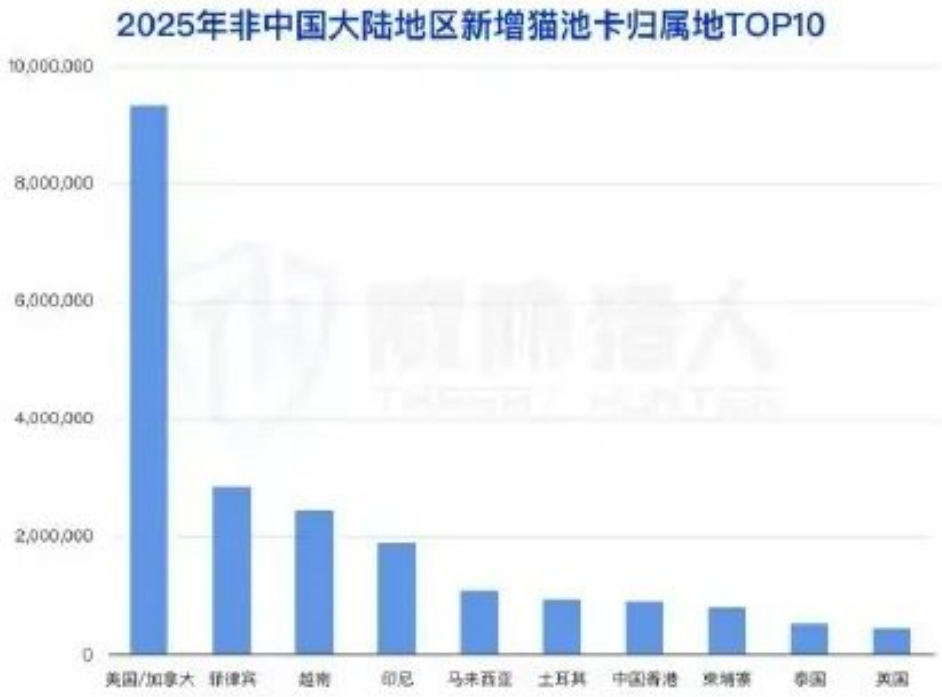
(2) Top 3 destinations for new SIM pool cards in non-mainland China in 2025: the United States/Canada, the Philippines, and Vietnam. Threat Hunter intelligence data statistics show that the new SIM pool cards in Hong Kong, Macao, Taiwan, and overseas regions in 2025 will mainly be located in the United States/Canada, the Philippines, and Vietnam.

At the same time, Threat Hunter noticed that threat actors also adopted the "link code" trading model for verification-code reception services in the United States/Canada.

Different from traditional code access platforms, the distinctive feature of "Link Code Access" is the "one-to-one" model. Specifically, it has an exclusive mechanism of "one number, one item, one link". When cybercrime ecosystem users use the link code, each phone number will generate an exclusive link for each project, and receive the verification code text message for the corresponding project through the exclusive link. Each number only serves a single project, and each link only displays the verification code of the corresponding attack project.

The link code process is as follows:

For threat actors, the link connection code has higher privacy and anti-tracing capabilities, which effectively avoids common risks in traditional connection codes:

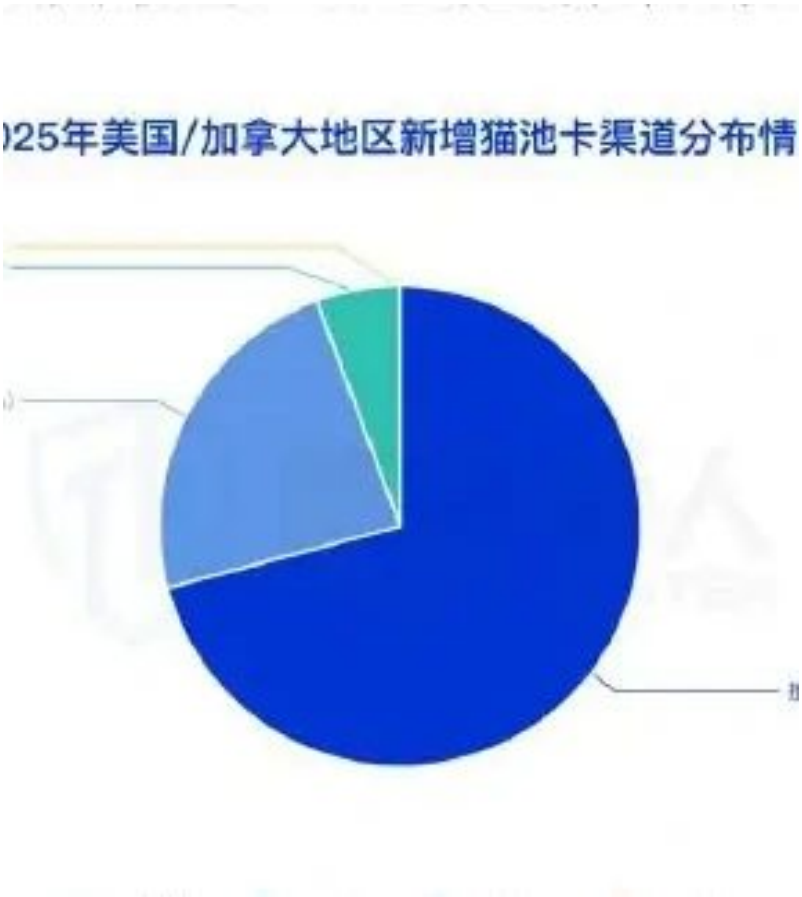


Analysis of the resources of the Non-Mainland Malicious Phone Number, 2025

Source: Threat Hunter original report, page 18

- First, the results of account maintenance are stolen. Traditional code connection usually shares the connection code or transcoding room, causing the clear text or mask of the number to be read by other threat actors, and the malicious accounts that have been developed are hijacked;
- Second, it is easy to be traced by supervision. Card dealers usually set the domain name used for the link code to be different from the domain name of the threat-actor platform, or sell it to distributors to use independent domain names, making it difficult to trace the domain name to the source platform.

1.2 Analysis of malicious IPs resources in 2025



Analysis of the resources of the "N.C.U.N.N." (Chart 1)

Source: Threat Hunter original report, page 19

Analysis of the resources of the "N.C.U.N.N." in 2025 (Chart 2)

Source: Threat Hunter original report, page 19

Figure guide

1	1. Cybercriminal user purchases a phone number
2	3. User applies the number to malicious activity
3	Unauthorized users cannot access the verification flow
4	Select number type and quantity
5	Choose the usage period and method
6	Use the assigned number
7	Carry out the fraudulent workflow
8	Other users cannot reuse the link
9	The link is bound to the specified number
10	2. Platform generates a verification link
11	4. Obtain the verification code
12	Platform creates a unique link
13	Verification code returned to the authorized user

1.2.1 There are 14.984 million daily active malicious IPs in 2025, an increase of 27.20% compared with 2024

According to Threat Hunter intelligence data, the number of daily active malicious IPs has continued to rise in recent years. In 2025, the number of daily active malicious IPs reached 14.984 million, an increase of 27.20% from 2024.

1.2.2 Analysis of domestic malicious IPs resources in 2025

(1) There were 80.316 million domestic malicious IPs in 2025, a decrease of 0.64% year-on-year in 2024. Threat Hunter research found that the scale of domestic malicious IPs in 2025 will not fluctuate significantly compared with 2024, and the magnitude of malicious IPs will basically remain stable.

Among them, from the perspective of the types of malicious IPs, after experiencing rapid growth in 2024, the development of "hijacking shared proxy" IPs will gradually stabilize in 2025.

Data shows that in 2025, a total of more than 45 million "hijacking shared proxy" IPs were captured, accounting for 11% of the total in 2024.

50.77% increased to 57.23% in 2025; its scale has no significant fluctuation compared with 2024

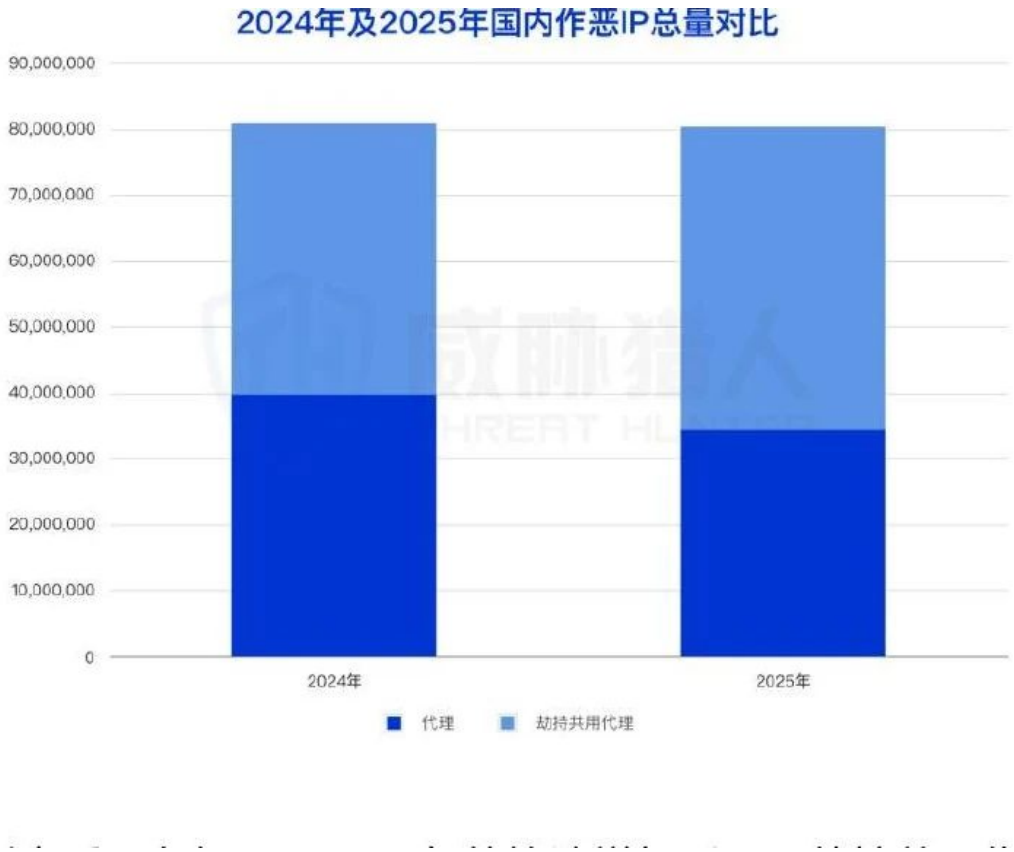
Hijacked shared proxy IP: refers to normal user IP resources maliciously hijacked by threat actors. threat actors implant Trojans into normal user equipment, and use Trojans to establish proxy channels on normal user networks. Each use time is very short, so it is difficult for ordinary users to perceive that their IP has been stolen.

Threat Hunter has marked this type of IP as a "hijacked shared proxy IP" risk label in January 2024.

(2) Top 3 provinces to which domestic malicious IPs belong in 2025: Zhejiang, Guangdong, and Jiangsu Threat Hunter intelligence data statistics show that the provinces (including municipalities) that are active in domestic malicious IPs in 2025 are mainly concentrated in Zhejiang Province, Guangdong Province, and Jiangsu Province.

Monitoring data shows that in 2025, the level of malicious IP in Zhejiang Province increased by 14.02% year-on-year, ranking first in the country. The regional ranking jumped from fourth place in 2024 to first in the country;

At the same time, Threat Hunter also observed that the proportion of Zhejiang IPs in the hijacking shared proxy platform has also increased significantly, with its proportion increasing from 5.42% to 7.13%; in the future, Threat Hunter will continue to monitor and track the activity of malicious IPs and changes in proxy resource distribution in relevant areas.



The total number of illegal IPs in the country has remained almost stable, but the share of co-agents for hijacking has continued to increase.

Source: Threat Hunter original report, page 19

1.2.3 Analysis of foreign malicious IPs resources in 2025

(1) In 2025, 165 million foreign malicious IPs were captured, an increase of 9.74% compared with 2024. In 2025, Threat Hunter strengthened the monitoring of overseas malicious IPs, and a total of 165 million overseas malicious IPs were captured in 2025, an increase of 9.74% compared to 2024.

(2) Top 3 countries of foreign malicious IPs in 2025: the United States, Brazil, and India. Threat Hunter intelligence data statistics show that the countries of active foreign malicious IPs in 2025 are mainly concentrated in the United States, Brazil, and India.

Monitoring data shows that the level of malicious IP in the United States increased most significantly in 2025, an increase of 80.91% compared to 2024.

Threat Hunter researchers analyzed and found that this growth is mainly related to changes in agent resources, which is specifically reflected in two aspects:

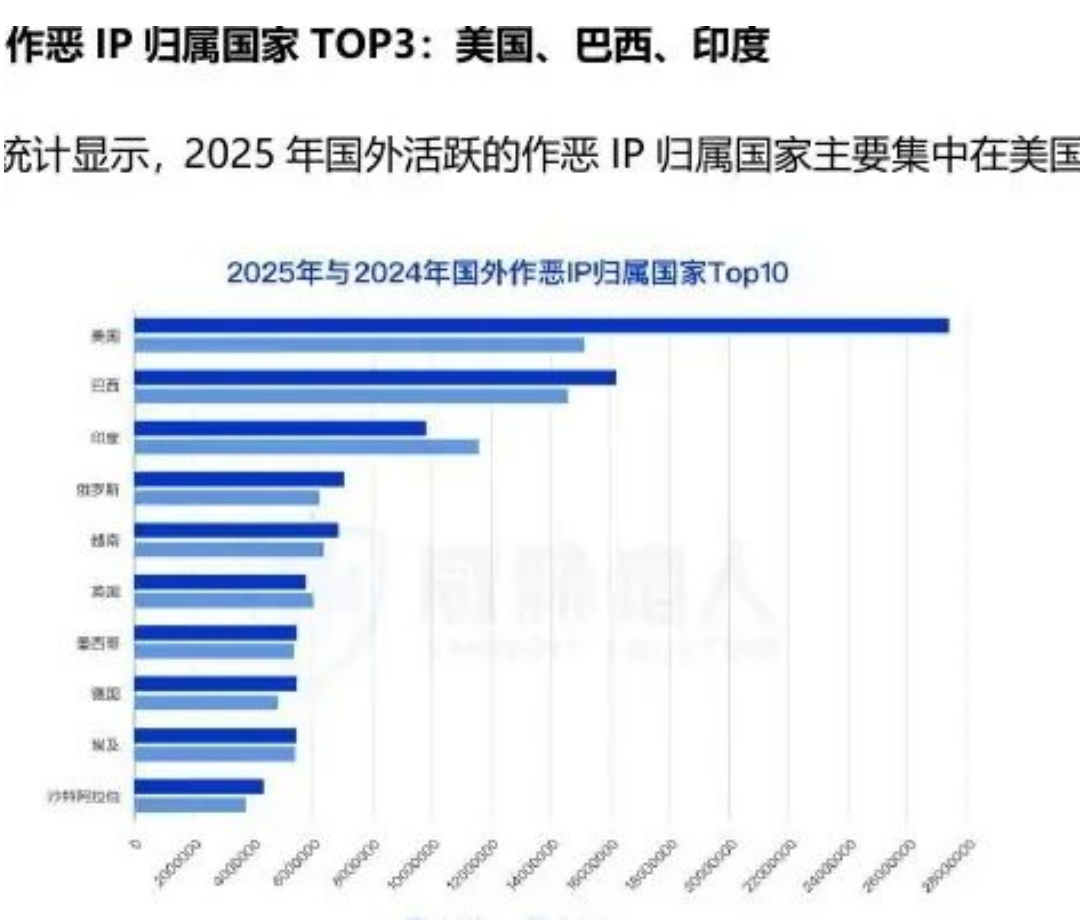
Analysis of domestic corruption in 2025 IP resources

Source: Threat Hunter original report, page 22

On the one hand, the core resources of newly monitored proxy platforms this year are mainly IPs from the United States, which has become the core source of contribution to the increase in malicious IPs in the region;

On the other hand, overseas agent platforms that have been active before are also continuing to expand their agent resource pools. Monitoring found that these platforms are also significantly increasing agent resources in the United States.

(3) There are differences in the proportion of malicious IP types at home and abroad. The proportion of foreign mobile networks far exceeds that of domestic ones. Threat Hunter analysis found that there are also certain differences in the malicious IP resources in different countries:



IIP Resource Analysis for Perpetrators Abroad 2025

Source: Threat Hunter original report, page 23

- Domestic malicious IPs use home broadband as the core type, accounting for more than 90%, mainly because domestic malicious activity proxy IPs, speed dial IPs, and hijacking shared proxy IPs are all generated based on home broadband resources;
- Although foreign malicious IPs still ranks first in household broadband, mobile network accounts for more than 20%.

1.3 Analysis of Internet Money Laundering Resources in 2025

1.3.1 Analysis of bank card resources involved in money laundering in 2025

(1) Among the bank cards involved in money laundering in 2025, gambling-related cards accounted for the largest proportion, accounting for 68.15%. Threat Hunter analyzed the 290,000 money-laundering bank cards monitored throughout 2025 and found that the risk types are mainly concentrated in two categories: gambling-related cards and fraud-related cards. Among them, gambling-related cards accounted for the highest proportion, accounting for 68.15%.

Gambling-related cards: Bank cards that are active in gambling platforms and used to collect payments on gambling platforms are often used on gambling platforms for recharge and collection, and the associated assets involve gambling money laundering. Threat Hunter uses a combination

of manual and automated methods to collect bank card account information used for payment behavior from various gambling platforms.

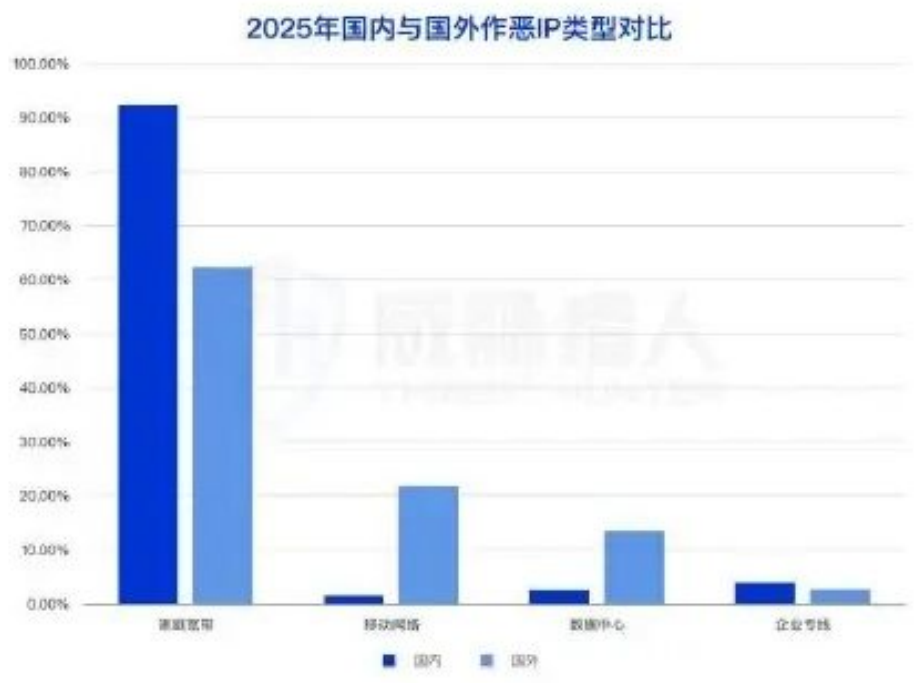
Fraud-related cards: In various anonymous social threat actors group chats, bank cards purchased by fraud gangs for money laundering are often used for fraudulent fund transfers.

Threat Hunter uses automated methods to extract bank card account information used by fraud gangs from records sent in group chats of anonymous social threat actors.

(2) Among the bank cards used for money laundering in 2025, the six major state-owned banks still account for the largest proportion, accounting for 71.29%. (3) Among the cities where bank cards involved in money laundering belong to in 2025, the top 3 cities are: Chongqing, Shenzhen, and Guangzhou

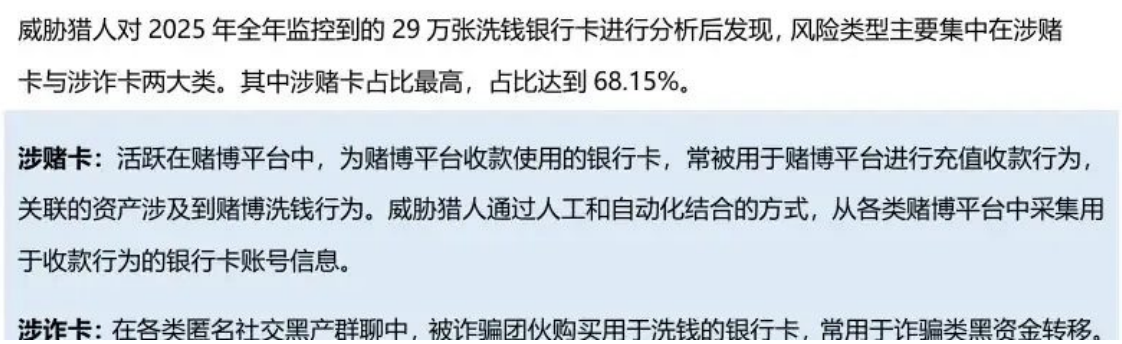
Among them, gambling-related cards and fraud-related cards present the following two characteristics in urban distribution:

- The cities where gambling-related cards belong are mainly concentrated in Chongqing, Shenzhen, and Guangzhou, and the magnitude is significantly higher than other cities.
- The cities where fraud-related cards belong are mainly concentrated in the “southern coastal + southwest nodes”, showing a double concentration pattern.



Analysis of Bank Card Resources Related to Money Laundering, 2025 (Chart 1)

Source: Threat Hunter original report, page 24


威胁猎人对 2025 年全年监控到的 29 万张洗钱银行卡进行分析后发现，风险类型主要集中在涉赌卡与涉诈卡两大类。其中涉赌卡占比最高，占比达到 68.15%。

涉赌卡：活跃在赌博平台中，为赌博平台收款使用的银行卡，常被用于赌博平台进行充值收款行为，关联的资产涉及到赌博洗钱行为。威胁猎人通过人工和自动化结合的方式，从各类赌博平台中采集用于收款行为的银行卡账号信息。

涉诈卡：在各类匿名社交黑产群聊中，被诈骗团伙购买用于洗钱的银行卡，常用于诈骗类黑资金转移。

Analysis of Bank Card Resources Related to Money Laundering, 2025 (Chart 2)

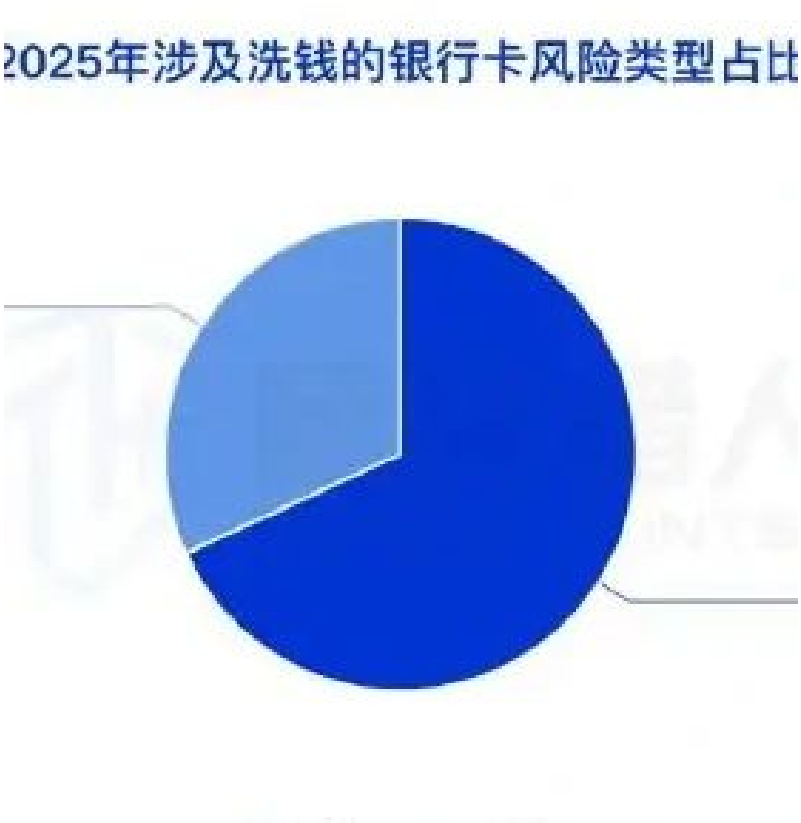
Source: Threat Hunter original report, page 24

1.3.2 Analysis of changes in corporate account resources involving money laundering in 2025

(1) In 2025, a new method of threat actors using the pretense of "optimizing flow" but actually manipulating corporate accounts to launder money emerged. Threat Hunter discovered that threat actors gangs used forged bank "loan approval" materials to induce companies to cooperate in so-called "flow packaging". In essence, they used corporate accounts to launder money. Relevant threat actors have formed a relatively mature operating process and rhetoric system, and quickly transfer money according to established paths to conceal the true source of funds.

The main process used by threat actors to defraud corporate accounts and use them for money laundering is as follows:

- In the public account defrauding stage, threat actors disguise themselves as financial lending companies or financial service personnel, contact companies in the name of loans and financing services, build trust through professional speaking skills, and then defraud the company's public account information and operating permissions.
- During the money laundering implementation stage, threat actors will connect the obtained public accounts to fraud gangs to receive fraudulent funds. At the same time, they used words to appease the corporate legal person on the grounds of "washing the flow and packaging the flow", inducing them to cooperate in completing multiple capital transactions and actually completing the money laundering operation.



Analysis of Bank Card Resources Related to Money Laundering, 2025 (Chart 1)

Source: Threat Hunter original report, page 25

Analysis of Bank Card Resources Related to Money Laundering, 2025 (Chart 2)

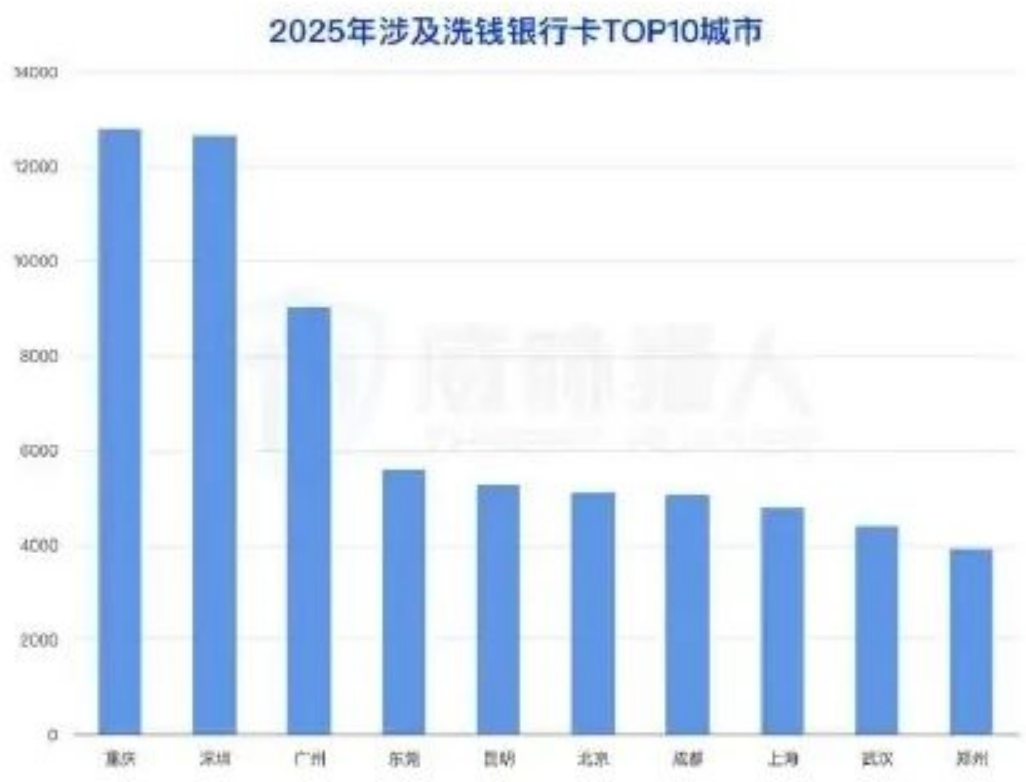
Source: Threat Hunter original report, page 25

- Money laundering completion stage After the money laundering is completed, threat actors immediately cut off ties with corporate legal persons. Because their identity information is all falsely packaged, it is difficult for companies to hold them accountable and ultimately bear losses.

(2) The change trend of money laundering corporate accounts in 2025 was broadly the same as in 2024

(3) Among the banks with money laundering corporate accounts in 2025, city commercial banks accounted for 36.12%, and have maintained growth for three consecutive years. Threat Hunter research found that from 2023 to 2025, the proportion of money laundering corporate accounts showed an obvious trend of "systematic transfer from the six major banks to small and medium-sized banks":

From 2023 to 2025, the proportion of money laundering public accounts of the six major state-owned banks decreased year by year, from 34.03% to 10.78%;

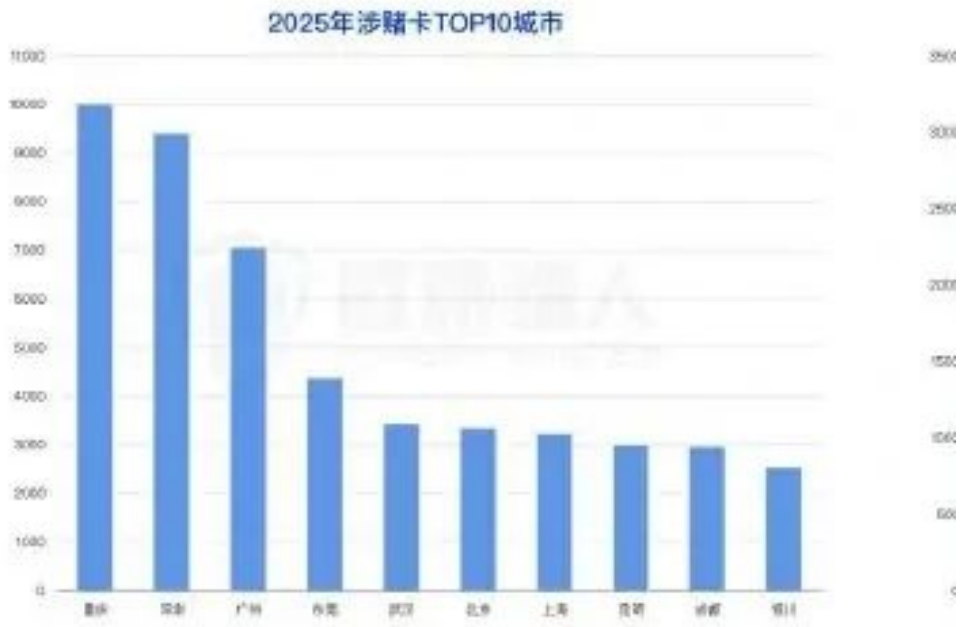


Analysis of changes in public account resources in 2025 involving money-laundering (Chart 1)

Source: Threat Hunter original report, page 26

Analysis of changes in public account resources in 2025 involving money-laundering (figure 2)

Source: Threat Hunter original report, page 26



Analysis of changes in public account resources in 2025 involving money-laundering (Chart 3)
Source: Threat Hunter original report, page 26

At the same time, urban commercial banks and rural credit cooperatives increased rapidly, with their combined share increasing from 29.21% to 54.34%.

This phenomenon reveals that threat actors' money laundering activities are gradually shifting their targets from the six major state-owned banks with stricter supervision and higher acquisition costs to urban commercial banks and rural credit cooperatives. This may reflect that compared with major state-owned banks, urban commercial banks and rural credit cooperatives have relatively lower thresholds for obtaining public accounts, and there may be certain weaknesses in money laundering risk management and control.

(4) Among the provinces where money laundering corporate accounts belong in 2025, the top three provinces are Guangdong, Shandong, and Jiangsu

(5) Among the cities where money laundering corporate accounts belong in 2025, the top 3 cities are Shenzhen, Beijing, and Guangzhou (6) Among the industries where money laundering corporate accounts belong in 2025, the top 3 industries are wholesale, retail, and business services

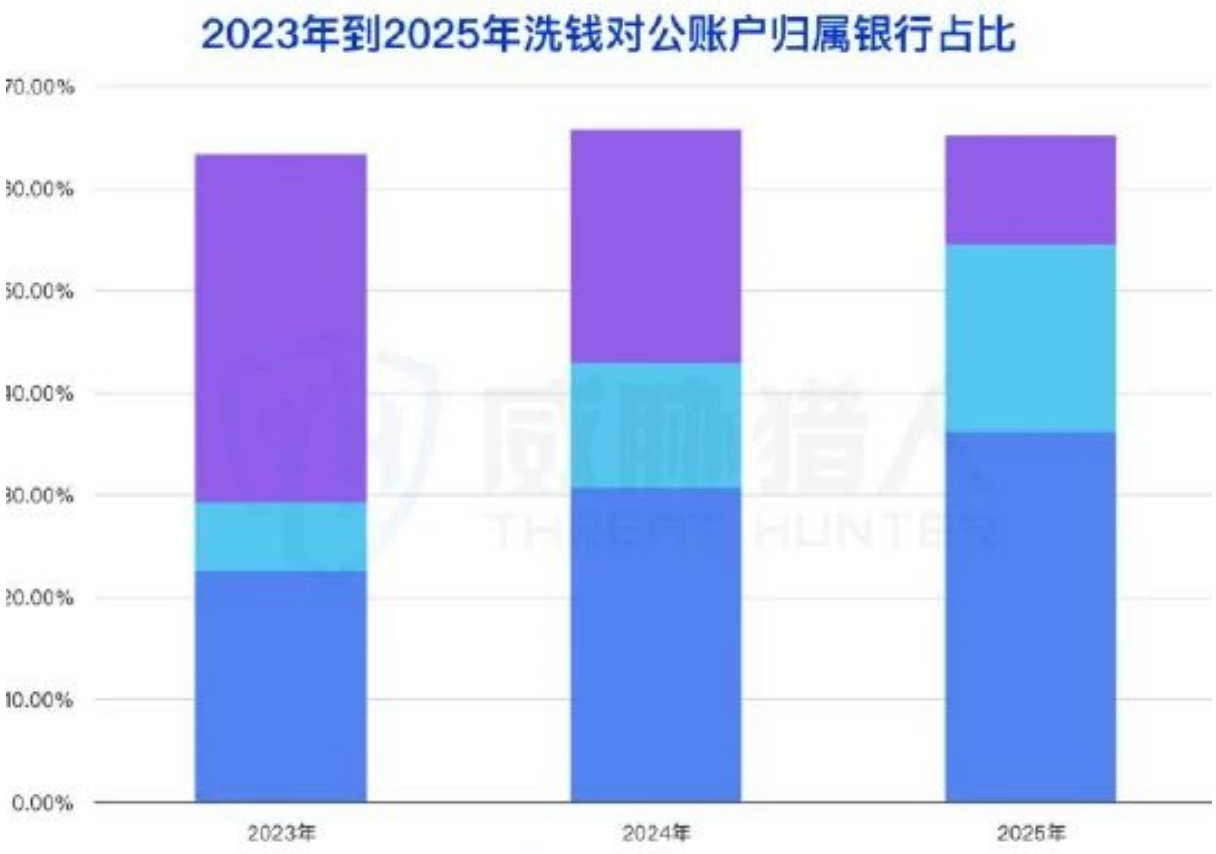
Money-laundering groups use recruited individuals and shell companies to distance criminal operators from business accounts.

Source: Threat Hunter original report, page 27

1.3.3 Analysis of changes in merchant resources involved in money laundering in 2025

"Merchant" usually refers to merchants and merchant accounts with legal business qualifications. In recent years, fraud or money laundering gangs have begun to use merchant accounts to collect "black money" to launder money. Collection accounts opened with merchant qualifications basically have no collection limit and can support multiple payment methods such as Huabei and credit cards. Compared with traditional money laundering methods, they are more covert and efficient.

(1) Among the merchants used by threat actors to launder money in 2025, black merchants account for the highest proportion, reaching 85.87%. Threat Hunter research found that there are two types of merchants used by threat actors to launder money, one is "black merchant" and the other is "white merchant".



Money-laundering to public accounts are moved from banks in six major countries to commercial banks in urban areas and rural credit unions.

Source: Threat Hunter original report, page 27

Black merchants: threat actors use illegal means such as forging materials, qualification transactions, and agency account opening to bypass platform review at a low cost, obtain and control merchant accounts. After merchants successfully open accounts, they are sold or leased to money laundering gangs in batches for the purpose of accepting and transferring illegal funds. These merchants have obvious instrumental characteristics.

White merchant: a normal merchant payment account obtained by threat actors through offline street canvassing, online shopping, etc. Since the merchant itself has a real business background, its account generally has the characteristics of high transaction frequency, large capital flow, and support for multiple payment methods. Through seemingly normal consumption behaviors, threat actors mix illegal funds into real transaction flows to achieve fund cover and transformation. Merchants have not actively participated in money laundering, but their accounts have objectively become an important channel for illegal fund flow.

(2) Merchant money laundering gangs will maintain an upward trend in 2025, and the number of merchants used by threat actors to launder money increased by 91.53% month-on-month. Threat Hunter monitoring shows that the number of merchant accounts used by threat actors for money laundering increased by 91.53% month-on-month in 2025, showing a significant upward trend overall. This phenomenon shows that merchant accounts are becoming an important carrier that is frequently used in money laundering activities.

Whether it is a "black merchant" or a "white merchant", the growth trend is mainly driven by two factors: the low cost of acquiring merchant accounts, and the high fit between merchant transaction characteristics and money laundering capital flow needs.

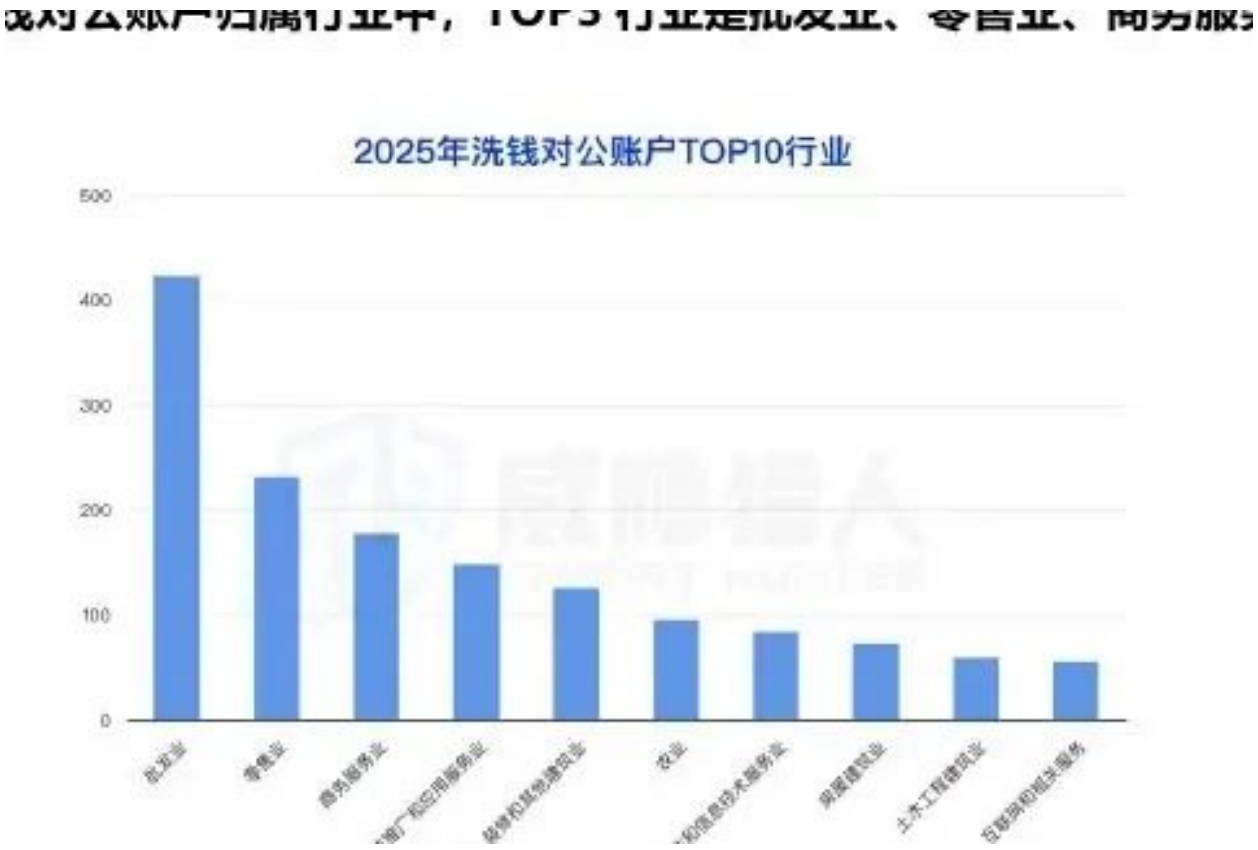
Threat Hunter monitoring data shows that in 2025, the number of active merchant money laundering gangs increased by 89.44% month-on-month.

This data reflects the expansion of merchants' money laundering risks, and the model is evolving towards organization and scale.

(3) Among the provinces where money laundering merchants belong in 2025, the top three provinces are Guangdong, Zhejiang, and Hubei

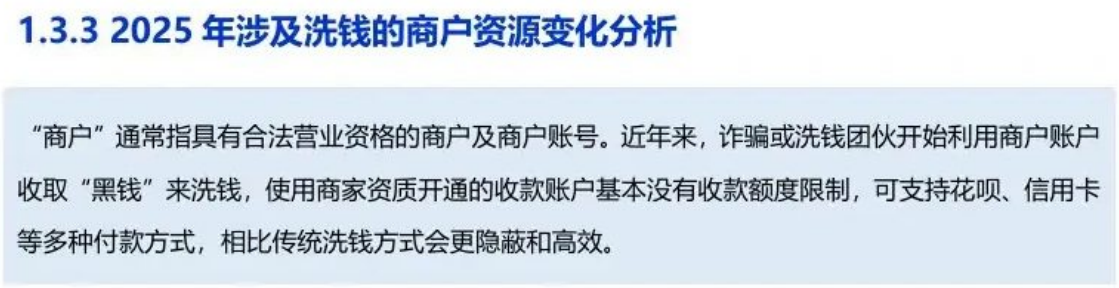
Analysis of changes in business resources involving money-laundering in 2025 (Chart 1)

Source: Threat Hunter original report, page 29



Analysis of changes in business resources involving money-laundering, 2025 (Chart 2)

Source: Threat Hunter original report, page 29



Analysis of changes in business resources involving money-laundering in 2025 (Chart 3)

Source: Threat Hunter original report, page 29

(4) Among the cities where money laundering merchants belong in 2025, the top 3 cities are Guangzhou, Wuhan, and Chengdu (5) Among the industries where money laundering merchants belong in 2025, the top 3 industries are retail, wholesale, and catering industries

1.4 Risk Email Resource Analysis in 2025

In 2025, Threat Hunter identified 138,800 email domain names, of which high-risk temporary email addresses accounted for the largest proportion, reaching 69.08%.

（1）2025 年被黑产用来洗钱的商户中，黑商户占比最高，达到 85.87%

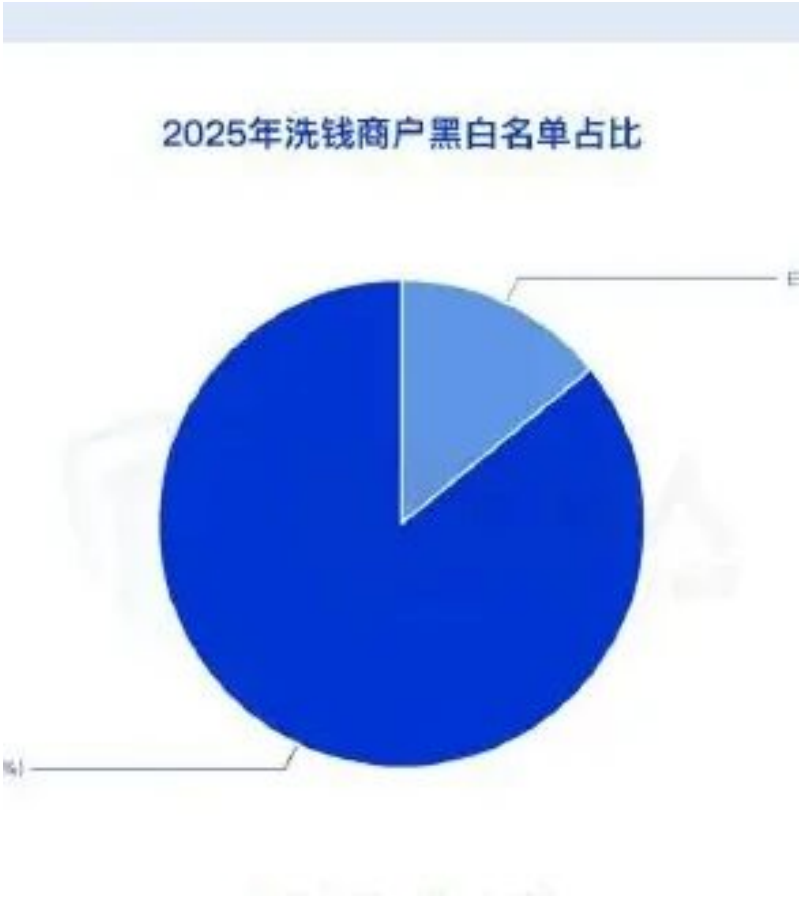
威胁猎人研究发现，被黑产用来洗钱的商户存在两种情况，一种是“黑商户”，一种是“白商户”。

黑商户：黑产通过伪造材料、资质交易、代办开户等非法手段，以较低成本绕过平台审核，获取并控制商户账户。商户开户成功后被批量出售或租赁给洗钱团伙，用于承接和转移非法资金，这些商户具备明显的工具化特征。

白商户：黑产通过线下“扫街”、线上购物等方式获取到的正常商户收款账号，由于商户本身具备真实经营背景，其账户普遍具有交易频次高、资金流水大、支持多种支付方式等特征。黑产通过看似正常的消费行为，将非法资金混入真实交易流水中，实现资金掩护与转化。商户并未主动参与洗钱，但其账户客观上成为非法资金流转的重要通道。

Analysis of changes in business resources involving money-laundering in 2025 (Chart 1)

Source: Threat Hunter original report, page 30



Analysis of changes in business resources involving money-laundering, 2025 (Chart 2)

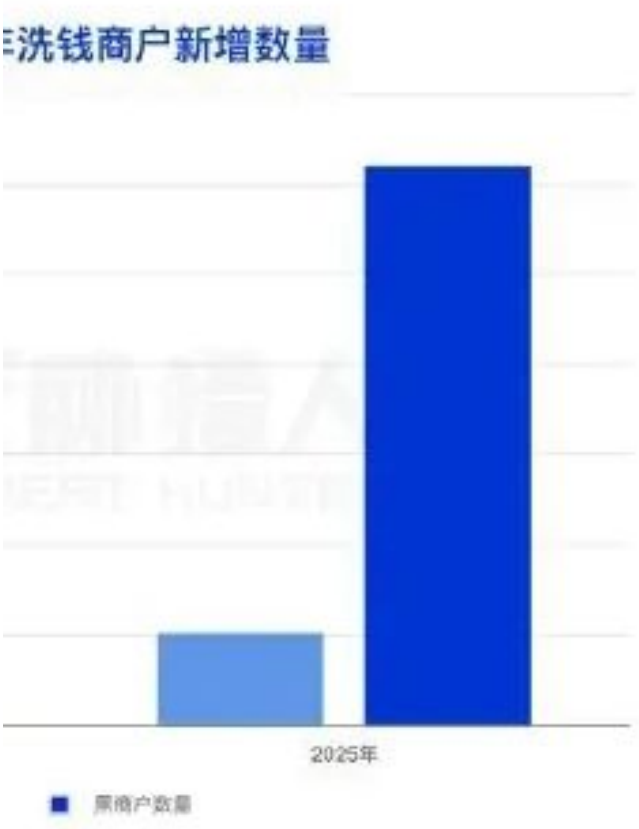
Source: Threat Hunter original report, page 30

Among them, the number of high-risk email domain names represented by temporary email addresses in 2025 increased approximately 9 times compared with 2024.

Temporary email address: It is an email address that does not require registration and can be used for a short period of time. Users usually use it to generate different email accounts in batches to

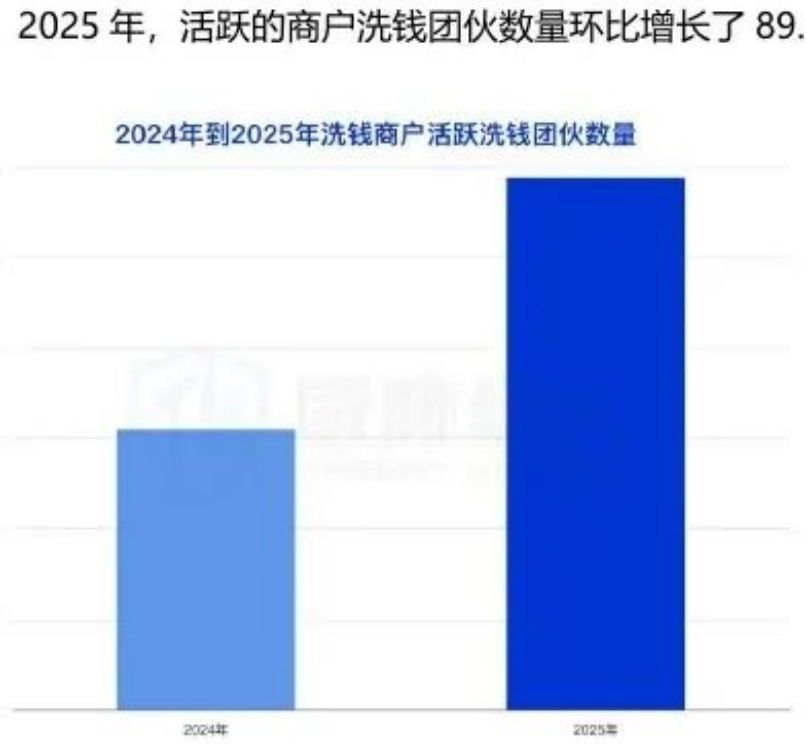
receive verification codes or registration information. The use time ranges from a few minutes to a few hours. After expiration, the email will automatically become invalid and can no longer be used.

Because temporary mailboxes have the characteristics of low acquisition cost, strong anonymity, and the ability to frequently change domain name suffixes, they are easily used by threat actors as a basic tool for batch registration and automated attacks, and they can bypass traditional detection methods by constantly changing domain names.



Analysis of changes in business resources involving money-laundering in 2025 (Chart 1)

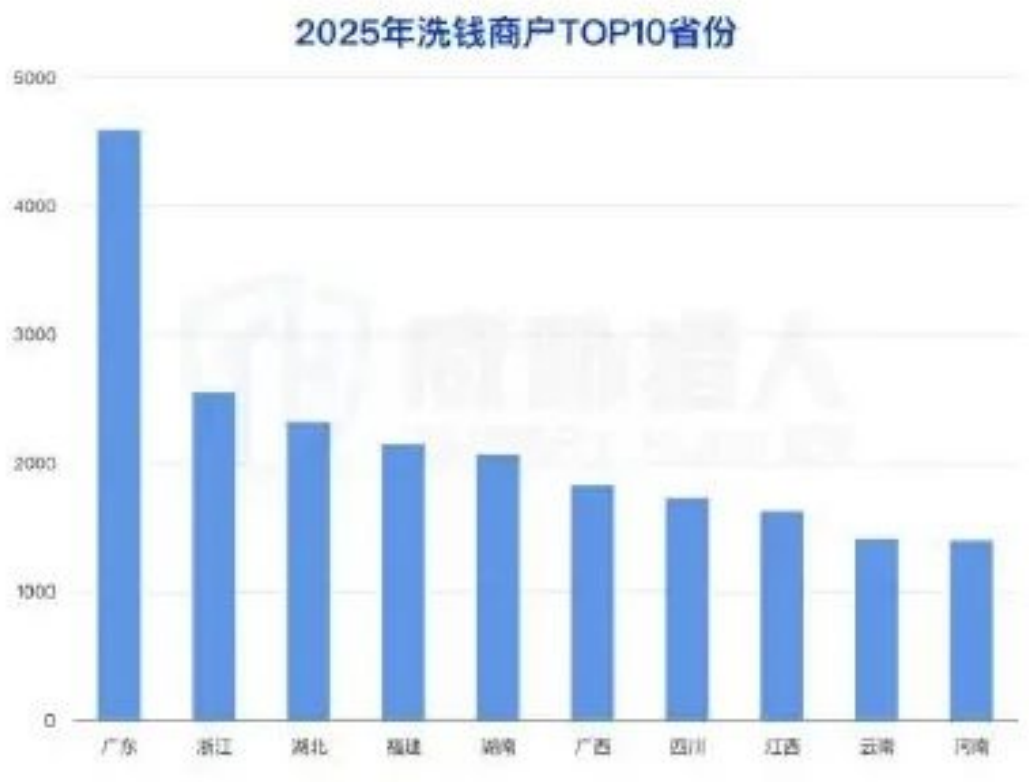
Source: Threat Hunter original report, page 31



Analysis of changes in business resources involving money-laundering, 2025 (Chart 2)
Source: Threat Hunter original report, page 31

In response to this characteristic, the Threat Hunter intelligence operations team continues to improve its ability to identify and cover high-risk temporary mailboxes. By continuously monitoring the latest changes in temporary mailbox services, it can promptly determine whether the mailbox belongs to the temporary mailbox service, helping customers make faster risk decisions in business fraud controls, account registration, and transaction scenarios, and reducing the risk of attacks by threat actors.

Analysis of common attack techniques by threat actors in 2025



Analysis of changes in business resources involving money-laundering in 2025 (Chart 1)

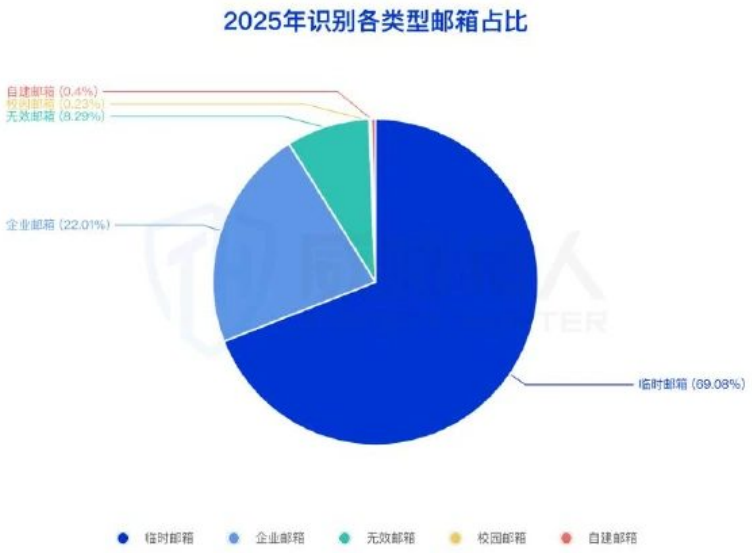
Source: Threat Hunter original report, page 32

Analysis of changes in business resources involving money-laundering, 2025 (Chart 2)
Source: Threat Hunter original report, page 32

2. Analysis of common attack techniques by threat actors in 2025

In 2025, Threat Hunter observed a clear trend of changes in cybercriminal groups attack technologies. Among them, the iteration of AI technology is the most obvious, such as the emergence of smart phones, the iterative evolution of AI-generated videos, and the rise of online workflow engine websites. The emergence and popularity of such technologies or applications have made attacks by threat actors faster and the cost of attacks has dropped significantly.

In addition, in terms of non-AI technologies, the emergence and popularity of face glare bypass tools and methods have also made attacks by threat actors more secretive. Scenarios that were relatively safe in the past will also face large-scale and normalized attacks in the future.



High-risk temporary mailboxes accounted for 69.08 per cent of the risk mailbox domain names identified in 2025.

Source: Threat Hunter original report, page 30

2.1 Security fence and risk of unauthorized access of mobile phone agents

2.1.1 Risk evolution: Risk of abuse of intelligent agent capabilities by threat actors

In 2025, with the launch of mobile phone-side agents (such as Doubao Mobile and AutoGLM), large model-driven autonomous agents began to be integrated into mobile operating systems. This type of device allows users to complete complex tasks such as ticket booking, transfer, and social interaction through natural language instructions. While improving interaction efficiency, this deep system authority and autonomous decision-making capability also introduces a new automated attack surface. Once the AI □□agent is combined with the existing threat actor infrastructure (such as SMS verification-code receiving service, cloud mobile phone cluster), its natural language drive, adaptive UI, human-like behavior and other characteristics will significantly reduce the attack threshold and improve concealment.

2.1.2 Defense status: double-layer protection system of agents

Currently, mainstream intelligent agents generally have a built-in two-layer safety architecture. The system layer and the agent layer jointly form a security boundary to limit their high-risk operation capabilities at the physical perception and logical execution levels.

System layer restrictions:

- Visual masking: When the user enters highly sensitive interfaces such as bank payment and identity verification, the system forcibly turns on the anti-screen capture and anti-screen recording flags, making it impossible for the agent to obtain private images.
- Permission locking: Strictly restrict the intelligent agent from calling high-risk automation interfaces to prevent it from operating the phone independently without authorization.

Agent layer restrictions:

- Intent interception: Before AI initiates an operation command, the security model will perform semantic filtering. Once sensitive keywords or high-risk intentions such as "transfer" and "send verification code" are identified, the task will be directly blocked.
- Strong interaction confirmation: It stipulates that all key actions involving assets and privacy must be manually clicked and confirmed by the user, and fully automatic operation cannot be achieved.

Two-tier security boundary architecture

2.1.3 Attack risks: from semantic bypass to system hijacking

Risk evolution: the risk of misuse of intelligence capabilities by cybercriminal groups (Chart 1)

Source: Threat Hunter original report, page 36

Risk evolution: the risk of misuse of intelligence capabilities (Chart 2)

Source: Threat Hunter original report, page 36

Risk evolution: the risk of misuse of intelligence capabilities (Chart 3)

Source: Threat Hunter original report, page 36

However, what needs to be paid attention to is that the currently deployed double-layer security boundary still has technical breakthrough points that can be exploited in actual operation. Under certain conditions, the cybercrime ecosystem may still pose a systemic bypass risk to the overall protection system.

(Breakthrough in security boundary architecture)

Risk 1: There is a risk of evasion in agent-side detection. Although mechanisms such as sensitive word filtering and multi-modal fraud controls are deployed on the agent side, because the large language model (LLM) is essentially based on semantic inference rather than hard code execution, attackers can use its deep semantic understanding and context association features to achieve a flexible bypass of agent-side security policies.

Risk 2: The security boundary on the system side is at risk of being breached. The multi-modal perception capability (visual + text) of the AI agent is highly dependent on the real-time capture of screen content. By cutting off the visual input of the AI agent, it is unable to recognize UI elements and continue automated operations. However, this mechanism still has weaknesses that can be exploited. Attackers can use technical means to make the screen content intercepted or recorded again, so that the large model agent can successfully obtain UI information and complete automated operations, thereby bypassing system security protection.

In summary, although the current security protection system for mobile phone agents has been initially constructed, its boundaries are still fragile when faced with AI agents with autonomous decision-making and cross-application operation capabilities. The dual lines of defense of system

isolation and semantic control have not yet formed seamless coordination, and there is a real risk of being systematically bypassed.

In the second part of the business fraud scenario section of 3.1, Threat Hunter will also use specific cases to demonstrate the above cases to more intuitively present the actual impact that may arise after the AI agent's capabilities are abused.

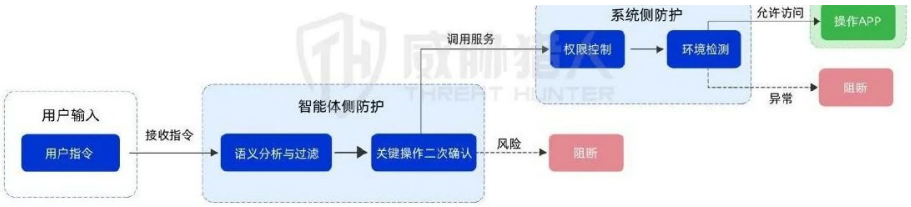
2.2 AI face-changing technology upgrade: from “single point tool” to “AI workflow”, the cost of threat actors’ attacks has dropped exponentially

2.2.1 Evolution path: from "single point tool" to "AI workflow"

Looking back at the development history of AI face attack technology, we can clearly see an evolution path from "simple animation" to "deep forgery" and now to "AIGC workflow":

Technology evolution chain:

CrazyTalk (early photo animation) → DeepFaceLAB (offline face-swapping model) → DeepFaceLive (real-time face-changing) →ComfyUI (local workflow engine) → online workflow engine (cloud SaaS)



双层安全边界架构

防护维度	系统安全边界	智能体安全边界
防护目标	阻断对敏感环境的感知与操作	阻止高风险意图的执行
核心机制	• 屏幕保护标志（（防止截屏/录屏）） • 高危权限管控（无障碍、通知等） • 自动化接口限制（如 UI Automator）调用限制	• 敏感词/语义规则过滤（如转账、验证码） • 多模态上下文风控（结合屏幕图像+文本判断风险） • 关键操作二次确认（如支付需用户手动点击）
防护思路	隔离：确保敏感信息不可见、关键操作不可达	管控：确保高风险意图可识别、越权行为可阻断

Mobile smarts need to be co-regulated by system-side isolation and smart-side control to form secure borders.

Source: Threat Hunter original report, page 35

This evolution reflects four key changes in attack techniques:

- Leap in production quality: visual effects move from “rigid” to “pore-level realism”.
- Free content generation: From relying on original video actions to unlimited generation driven by text/audio.
- Minimalist operation process: Complex code training is encapsulated into visual "one-click" operations.
- The hardware threshold has been reduced to zero: from relying on expensive local graphics card workstations to cloud computing power that can be called by the browser.

Risk of attack: from semantic bypass to system hijacking (Chart 1)

Source: Threat Hunter original report, page 39

Risk of attack: from semantic bypass to system hijacking (Chart 2)

Source: Threat Hunter original report, page 39

Timeline comparison: AI face-changing attack technology evolution watershed in 2025, first half of 2025 (single point tool era):

Threat Hunter's monitoring data shows that during this period, producing AI attack materials (such as videos of celebrities bringing goods) was a high-threshold and high-investment project. Due to the lack of integrated tools at the time, attackers had to spread their operations like building blocks:

- Hardware costs money: Running these early AI models requires extremely high-end graphics cards (GPUs), and the equipment cost is high;
- Process fragmentation: The attacker cannot generate the finished product at once. They must first use an AI tool to generate a "fake face video" and then use another AI tool to generate a "fake voice";
- Manual and cumbersome: Finally, like a professional video editor, you need to manually put the video and audio into the editing software and align the mouth shape and sound frame by frame. Producing a video of just tens of seconds often requires hours of labor and computing power.

Second half of 2025 (workflow era): With the popularity of workflow engines such as ComfyUI that can connect multiple AI models in series, attack efficiency will change qualitatively.

- Case A (product delivery video): The attacker only needs "1 picture + 1 audio + 1 action reference video" to generate a lip-sync and natural action delivery video with one click in the workflow.
- Case B (Identity Bypass): The attacker uses the workflow to convert "1 ID photo" into a standard avatar, and then generates a dynamic face video, which is directly used to bypass the face authentication system.

2.2.2 Core comparison: full-dimensional ability jump

The table below provides a detailed comparison of the technology leap from early tools to current AIGC workflows across six key dimensions:

2.2.3 Status quo upgrade: Online SaaS engine reduces attack costs

Although local workflow engines reduce the difficulty of operation, high-quality generation still relies on high-performance graphics cards (GPUs). However, the emergence of online workflow engines (SaaS) has completely broken down this barrier.

Compared with local deployment, online engines have the following salient features:

(1) Computing power in the cloud, zero hardware threshold

- Features: Users do not need to purchase expensive graphics cards (such as NVIDIA 4090), and can call cloud clusters (usually equipped with high-end graphics cards with 24G/48G video memory) through the browser.
- Impact: An attacker only needs a mobile phone or thin and light notebook with Internet access to complete high computing power reasoning in the cloud.

(2) The model is community-based and the attack cost is extremely low. Features: Membership subscription is as low as 100 yuan per month. The platform supports users to upload and share trained workflows (Workflow), and attackers can directly "reuse" other people's high-order attack models with one click.

- Impact: Even "novice" attackers who do not understand technology can obtain top-level attack capabilities at a very low cost.

繁琐： 最后，还需要像专业视频剪辑师一样，手动将视频和音频放入剪辑软件
地对齐口型和声音。制作短短几十秒的视频，往往需要耗费数小时的人工与算

Evolution Path: From "One Point Tool" to "AI Workstream"

Source: Threat Hunter original report, page 41

(3) Typical threat cases: Abuse of LivePortrait Currently, Threat Hunter has detected a large number of threat actors using advanced driver models such as LivePortrait to generate face videos.

- Attack link: The attacker selects the ready-made LivePortrait workflow on the online SaaS platform -> uploads the victim's photo -> quickly generates the video in the cloud -> downloads the video and injects it into the camera.
- Consequences: Such videos are packaged and sold in large quantities and used for face authentication bypass attacks to make illegal profits. Due to the high-quality generation and micro-expressions (blinks, gaze), traditional defense methods are extremely difficult to identify.

2.3 Automated tools break through the "three-color glare" defense line, lowering the threshold for threat actors to attack

Evolution Path: From "One Point Tool" to "AI Workstream" (Chart 1)

Source: Threat Hunter original report, page 42

Evolution Path: From Single Point Tool to AI Workstream (Chart 2)
Source: Threat Hunter original report, page 42

2.3.1 Attack evolution: from "manual pre-made video" to "automated real-time rendering"

In the field of face liveness detection, "active color flashing liveness detection" (often called "colorful" or "three-color" verification in China)

It was once considered a solid line of defense.

What is "Color Flash Live Detection"? This is a common live defense technology. The system will make the mobile phone screen quickly flash different colors (such as red, green, blue), and capture the changes in light reflection on the person's face through the camera. Only real faces will produce natural real-time reflections as the screen color changes, which cannot be achieved with photos or ordinary videos.

For a long time, because this technology requires real-time and dynamic changes in light, threat actors have been difficult to decipher through simple photos or pre-recorded videos. However, in July 2025, Threat Hunter detected that a major facial authentication bypass tool released a major update, adding an "automated glare simulation" function. The emergence of this function completely penetrated this once insurmountable technical defense line.

Before this update, threat actors were often helpless when faced with color flicker verification, or could only try their luck through extremely tedious manual editing; but after the tool update,

attackers have achieved a "fool-like" automated pass. The following is a specific comparison before and after technology iteration:

2.3.2 Technical Review: How do threat-actor tools "cheat" the verification algorithm?

Status upgrade: SaaS engine online reduced attack costs (Chart 1)

Source: Threat Hunter original report, page 43

Status upgrade: SaaS engine online reduced attack costs (Chart 2)

Source: Threat Hunter original report, page 43

After in-depth reverse engineering analysis by Threat Hunter Lab, the tool's glare bypass function is not a simple filter overlay, but a set of real-time rendering mechanisms based on screen interaction. Its core logic can be broken down into three steps:

- Step 1: Preset color coordinates

攻击者可直接“一键复用”他人的高阶攻击模型。

影响： 即使是不懂技术的“小白”攻击者，也能以极低成本获取顶级的攻击能力。

Status upgrade: online SaaS engine reduced attack costs

Source: Threat Hunter original report, page 44

- Step 2: Real-time sampling
- Step 3: Dynamic rendering

2.3.3 Risk analysis: comprehensive downgrading of the defense system

The emergence of this tool has a disruptive milestone:

- Defense failure: This means that "glare/three-color verification", a fraud-control measure that once could block more than 90% of traditional video attacks (such as paper, simple remakes, ordinary deepfake), is no longer safe in the face of new tools.
- Normalization of attacks: As tools reduce the technical threshold to zero, glare verification attacks targeting high-value scenarios such as finance, credit, and social networking will show a large-scale and automated outbreak trend.
- Countermeasure upgrade: Traditional defense strategies based on color matching are facing challenges, and enterprise security teams need to be forced to turn to lower-level countermeasures (such as detecting injected software features, analyzing the rationality of physical reflection of light on facial surfaces, etc.).

Analysis of threat actors attack scenarios in 2025

3. Analysis of threat actors attack scenarios in 2025

3.1 Business scenario analysis

Evolution of attacks: from “manual prefabricated video” to “automated real-time rendering” (Chart 1)

Source: Threat Hunter original report, page 45

曾被视为一道坚固的防线。

什么是“色彩闪烁活体检测”？ 这是一种常见的活体防御技术。系统会让手机屏幕快速闪烁不同的颜色（如红、绿、蓝），并通过摄像头捕捉人脸上的光线反射变化。只有真实的人脸才会随着屏幕颜色的变化产生自然的实时反光，而照片或普通视频则无法做到这一点。

Evolution of attacks: from “manual prefabricated video” to “automated real-time rendering” (Chart 2)

Source: Threat Hunter original report, page 45

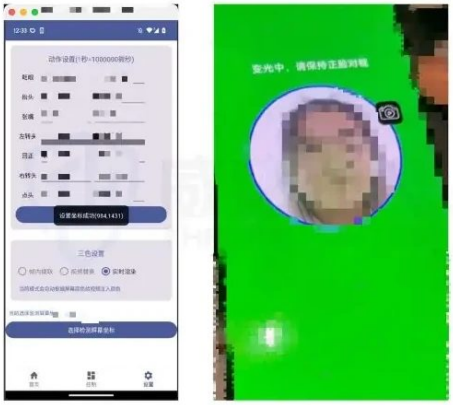
1) The risk of online business fraud remained widespread in 2025, with the amount of related attack intelligence exceeding 1.3 billion. In 2025, the Threat Hunter anti-fraud intelligence platform captured approximately 1.31 billion pieces of attack intelligence related to online business fraud.

Judging from the trend throughout the year, the overall attack intensity of threat actors remains at a high level: the number of attacks continued to rise in the first half of the year, and reached the peak of the year in June due to the superposition of mid-year promotions and summer activities; although there were some fluctuations in the second half of the year, the overall level was still at a high level, and there was a slight decline at the end of the year.

2) There were 4,271 fraud risk events in the early warning business in 2025. Threat Hunter recorded 4,271 fraud risk events in the early warning business in 2025, a year-on-year increase of approximately 2.7%. The distribution of events throughout the year shows phased characteristics. The number is higher in the first half of the year, then falls overall in the second half of the year, and rebounds at the end of the year.

3) The industry distribution of threat actor attacks is mainly concentrated in high-frequency transactions, high subsidies, and high-traffic Internet business scenarios. According to monitoring data from the Threat Hunter anti-fraud intelligence platform, threat actor attacks in 2025 are mainly concentrated in high-frequency transactions, high subsidies, and high-traffic Internet business scenarios. From the perspective of industry distribution, the e-commerce industry is still the area with the most concentrated risks, accounting for 20.5%, followed by banking (11.99%), tourism services (12.03%), local life (12%) and other industries;

- 步骤二：实时采样
- 步骤三：动态渲染



Technological reset: How do cybercrime tools “deceptively” validate algorithms?

Source: Threat Hunter original report, page 47

4) The average number of threat actor groups & forums captured throughout the year exceeds 500,000 per month. According to monitoring data from the Threat Hunter anti-fraud intelligence platform, the average monthly number of threat actor groups and forums involved in marketing activities captured in 2025 is approximately 500,000.

5) The number of malicious threat actor accounts captured throughout the year exceeded 1.3 million per month on average throughout 2025. Throughout 2025, the Threat Hunter anti-fraud intelligence platform captured more than 1.3 million malicious accounts active in business fraud on a monthly basis.

3.1.1 New Risks in fraud controls in the AI Era: Automated malicious activity Enters the “Agent Stage”

As AI, mobile phone intelligence and other capabilities become increasingly mature, cybercrime ecosystem and promotion-abuse actors are gradually introducing them into business fraud and automated operations. Compared with traditional scripting tools, AI can identify interface elements, simulate real user operations, and continuously perform tasks across multiple apps, making complex processes that originally relied on manual labor capable of large-scale replication.

At the same time, the widespread application of AI has continued to reduce the threshold and cost of malicious activity; Threat Hunter monitoring found that "one-click deployment" intelligent agent services have appeared on the market, which can transform ordinary devices into "operable intelligent agents" with only simple installation, further amplifying the large-scale malicious activity capabilities of cybercrime ecosystem and posing new challenges to the existing fraud-control system.

3.1.2 AI has been used to assist e-commerce arbitrage related operations and is changing some of the ways of conducting malicious activity.

Threat Hunter intelligence monitoring found that with the popularity of generative AI tools, cybercrime ecosystem and promotion-abuse actors have begun to introduce AI into e-commerce arbitrage-related operations, and have shown obvious signs of penetration in typical marketing scenarios such as evaluation, after-sales, and rebates.

Risk assessment: overall downgrading of defence systems

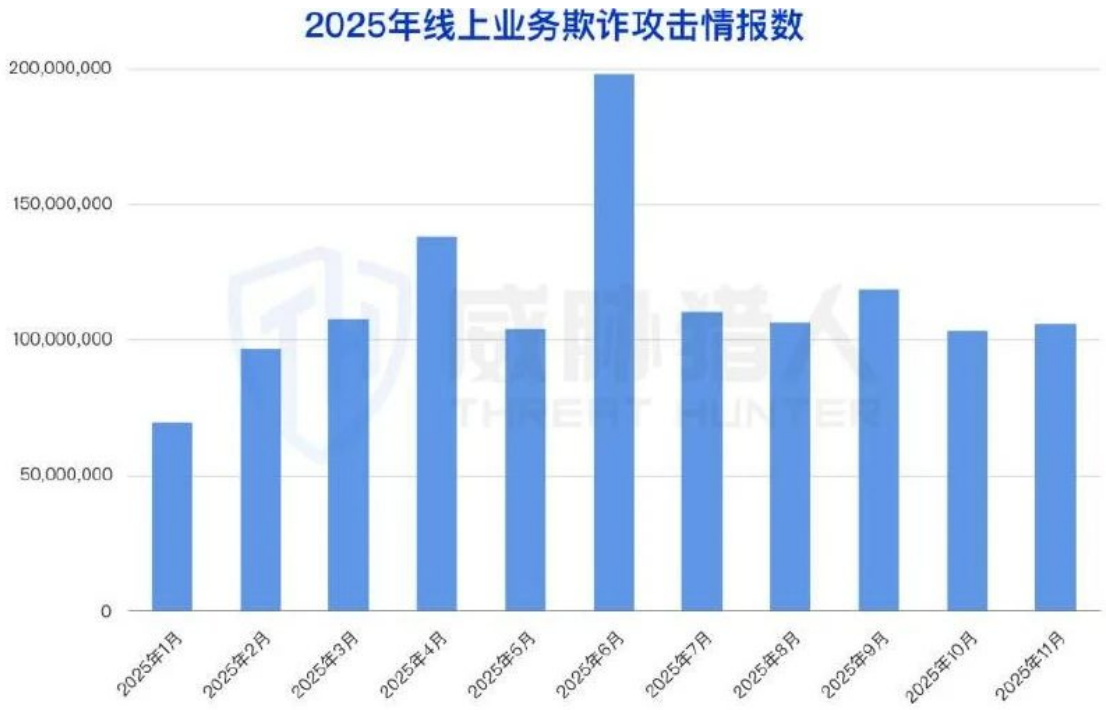
Source: Threat Hunter original report, page 48

Threat Hunter identified 3 types of high-risk fraud:

1. Use AI to generate evaluation content to participate in e-commerce rebate arbitrage

In some promotion-abuse forums and threat actors communication channels, Threat Hunter has detected sharing of operations involving the use of AI-generated evaluation content to participate in e-commerce rebate arbitrage. The relevant malicious methods mainly revolve around the

marketing mechanisms of e-commerce platforms such as "review rebates" and "posting orders and coupons";

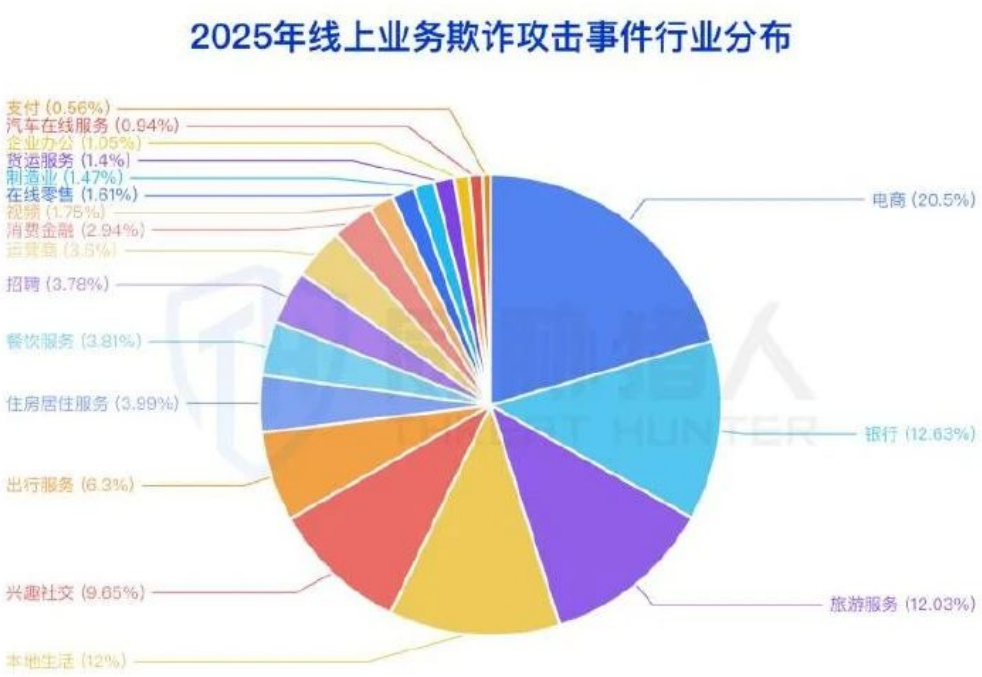


On-line fraud attacks maintained a high level of intelligence throughout the year and reached a high level in June.

Source: Threat Hunter original report, page 47

That is, without actually acquiring the product, AI is used to automatically generate evaluation text, or to generate picture content that is highly relevant to the product, pretending to be a real buyer's evaluation submission, thereby triggering platform cashbacks, coupons, or point rewards.

In this scenario, threat actors do not make real purchases, but obtain platform subsidy resources through false evaluations; after obtaining the subsidy, threat actors will return the goods; but the platform will not take back the subsidy that has been obtained at this time.



e-commerce platforms, banks, tourism services and local life are industries with a high concentration of online fraud.

Source: Threat Hunter original report, page 48

2. Use AI to generate false image materials to implement “refund only” arbitrage

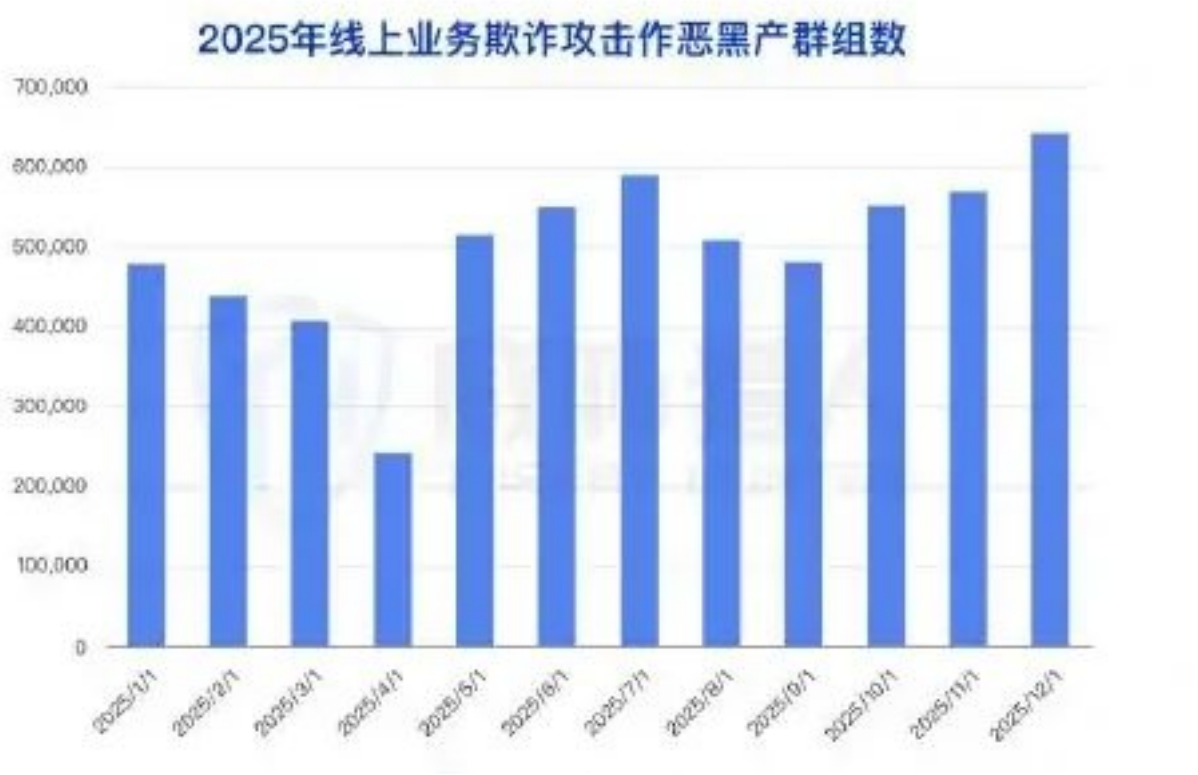
In addition to evaluation rebates, cybercriminal groups have begun to further extend its AI capabilities to after-sales and compensation links. In 2025, Threat Hunter captured multiple cases of using AI to generate false image materials to defraud refunds or compensation. The relevant perpetrators used AI to generate pictures of damaged goods, quality defects, damaged packaging, etc., and submitted them as after-sales or complaint vouchers, successfully triggering the platform's "refund only" and "use now, pay later" processes.

In some cases, the clarity, composition logic, and detail presentation of the images generated by AI are enough to pass the platform's preliminary review. Especially in scenarios that lack manual review or rely on rule judgment, they are more likely to be judged as "reasonable credentials" by the system. This type of behavior further weakens the platform's ability to judge the authenticity of the link "physical delivery - problem occurrence - material evidence", making the after-sales compensation link a high-risk entry point for AI arbitrage.

3. Use AI agents to complete the entire process of e-commerce order placement and contract fulfillment.

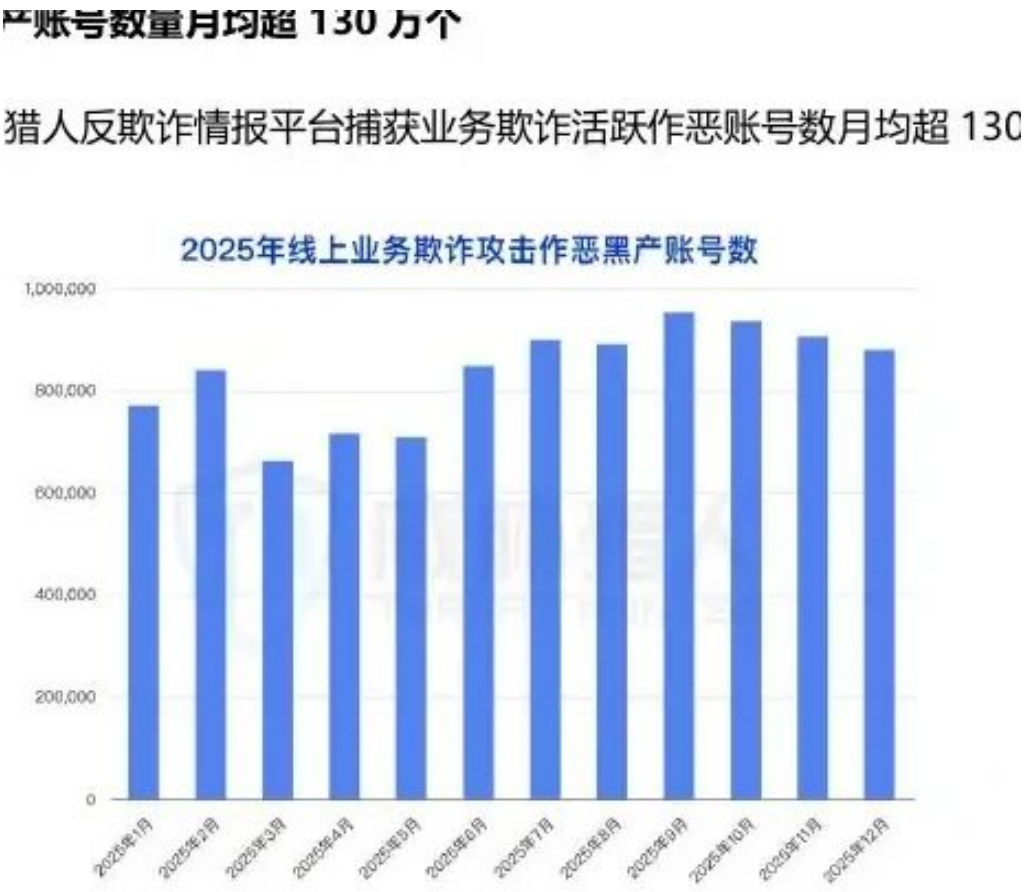
Threat Hunter monitoring found that in some social media and technology sharing channels, operation demonstrations and experience sharing using AI to automatically place orders have appeared. Based on the actual test results, under certain conditions, AI agents can be driven to complete the full-link operation process in e-commerce apps, including product browsing, price comparison, additional purchases, placing orders, and confirmation of receipt. In some scenarios,

third-party payment apps can also be invoked to perform password-free payments or enter specified passwords and other sensitive operations.



AI Times of New Risks for Wind Control: Automation of Vices into the Smart Stage (Chart 1)

Source: Threat Hunter original report, page 52



AI New Risks of Wind Control in the Age: Automation of Vices into the Smart Phase (Chart 2)
Source: Threat Hunter original report, page 52

Once this type of ability is exploited on a large scale by threat actors, it may be introduced into malicious activity scenarios such as order manipulation, false transactions, and marketing resource arbitrage. Compared with traditional scripts or human-in-the-loop crowdsourcing methods, AI agents are closer to real users in terms of operating rhythm, behavior paths and page interactions. If used in conjunction with tools such as simulators, it will significantly reduce the cost of manual participation and increase the difficulty of fraud-risk detection.

AI The New Risks of the Wind of the Age: Automation to the Smart Stage

Source: Threat Hunter original report, page 53

3.1.3 Risks caused by the abuse of AI agents to the financial industry

As AI agents gradually acquire the ability to perform continuous operations within mobile apps, their potential risks in financial scenarios are moving from "theoretical possibility" to the "verifiable stage." Through internal testing and research, Threat Hunter found that under certain conditions, AI agents have the ability to perform some sensitive operations in financial apps. Once exploited by threat actors, it may have a substantial impact on account security and fund security.

1. AI agents can perform sensitive operations such as "checking balances, viewing transaction details, and automatically entering account passwords" in financial apps.

During the internal testing and verification process, Threat Hunter researchers found that while logged in, the AI agent has the ability to perform queries and interactive operations in some financial apps, including querying account balances, transaction details and other sensitive information, and participating in marketing activities within the platform.

It should be noted that most of the intelligent products currently on the market adopt open source architecture. If used by threat actors and implanted with backdoor programs, the relevant agents may transmit sensitive information such as account balances and transaction records back to the threat actors through the "backdoor" while performing normal operations, thereby triggering the risk of account information leakage or even capital loss, which may have a serious impact on both users and financial institutions.

2. After the security policy is circumvented, there is a possibility of being bypassed by combination

In further testing, Threat Hunter found that under specific command combinations and execution paths, AI agents may reinterpret or evade judgments on the built-in security policies of financial apps, thus bypassing security constraints originally used to limit high-risk operations. After the security policy is circumvented, the agent can still continue to perform subsequent steps in high-risk financial operations including transfers, signing contracts, etc.

Although most companies have limited the capabilities of AI in the financial field, Threat Hunter research found that after bypassing prompt words and installing plug-ins to obtain originally restricted screenshot permissions, AI agents can still simulate normal people to perform transfers, signing contracts, and other highly sensitive operations that require bank withdrawal passwords.

The following is the relevant testing situation of Threat Hunter researchers:

(After the security policy is circumvented, AI can execute the bank transfer process)

AI has been used to assist electric arbitrage-related operations and is changing some of the ways in which evil is done

Source: Threat Hunter original report, page 55

(After the security policy is circumvented, AI performs third-party quick payment signing and authorization operations)

This test phenomenon reflects:

- Security mechanisms based on prompt words or policy agreements are still “soft constraints” in nature;
- When an agent is allowed to "reinterpret rules", its safety boundary will be highly dependent on the user's intention;
- The "opaque fraud-decisioning" strategy of financial institutions is not indestructible and can be cracked by relying on external plug-ins.

Threat Hunter's internal testing shows that AI agents have the technical feasibility to understand and execute some sensitive operational processes in financial scenarios, and there is uncertainty in the reliance on security policy constraints under specific conditions. Although no case of actual abuse of relevant capabilities has been found, it has already constituted a potential impact on

traditional fraud controls assumptions based on manual operations, and financial institutions deserve to evaluate and respond in advance.

3.1.4 Current status of the “national subsidy” fraud industry

至黑产侧，从而引发账户信息泄露甚至资金损失风险，对用户及金融机构均可能造成严

AI Risk point for the financial sector from smart body abuse

Source: Threat Hunter original report, page 56

In 2025, under the supervision of the "state-patched" policy, the Threat Hunter intelligence platform still detected cybercrime ecosystem profiting from state-patched vulnerabilities. cybercriminal groups use various methods such as illegal acceptance of joint couriers, resale of qualifications, illegal verification operations, counterfeit recycling orders for arbitrage, recruiting individuals to recycle national subsidy, and other methods to obtain the preferential state subsidy.

These techniques involve multiple roles, including cybercrime ecosystem, merchants and individual users, specifically involving fraud users, resale qualified users, merchants, agents, scalpers, couriers, etc. These roles cooperate with each other to bypass national subsidy areas and user supervision through purchasing, forwarding, activation, etc., forming a complex chain of interests.

The points and methods of profit-making through multi-role collaboration are as follows:

1. Digital home appliances have become the hardest hit area for sales of state-subsidized goods

Threat Hunter made statistics on the types of products related to China's national consumer subsidy program sold in the cybercrime ecosystem trading market. The top product categories with the highest trading popularity are: digital products, home appliances, and lifestyle products, accounting for 53.32%, 30.42%, and 13.56% respectively.

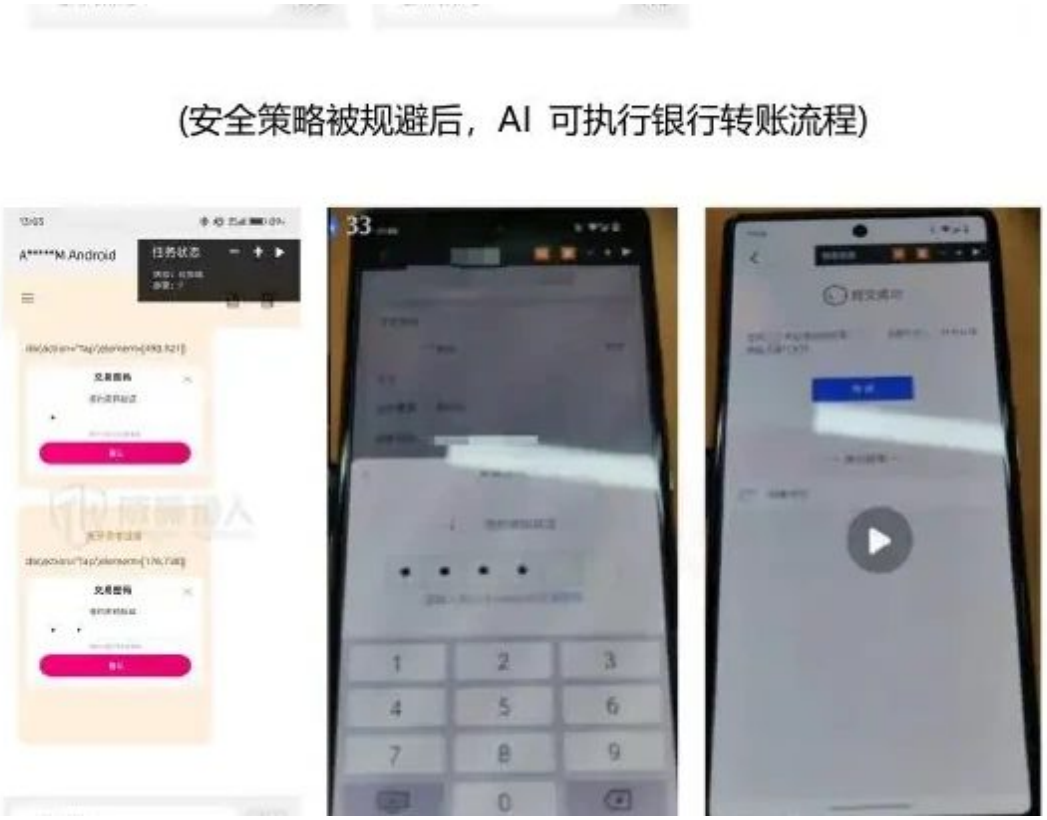
2. Main distribution areas of cybercrime ecosystem selling consumer subsidy products: top 3: Shanghai, Beijing, Shenzhen

Threat Hunter researchers analyzed the registration locations of individual cybercrime ecosystem stores selling consumer subsidy products on major trading platforms and found that cybercrime

ecosystem stores selling consumer subsidy products are mainly distributed in economically developed areas such as Shanghai, Beijing, Shenzhen, and Guangzhou.

AI Risk point for the financial industry from smart body abuse (Chart 1)

Source: Threat Hunter original report, page 57



AI Risk points for the financial industry from smart body abuse (figure 2)

Source: Threat Hunter original report, page 57

3. The main sources for selling consumer subsidy products are the two leading domestic e-commerce platforms.

Note: The following report content has been desensitized (relevant e-commerce platforms are referred to as A, B, C, etc.)

Threat Hunter collected statistics on the source channel information of consumer subsidy products sold by cybercrime ecosystem from the capture cycle sample data. Among them, 87.1% of the consumer subsidy products came from the two leading domestic e-commerce platforms.

4. cybercriminal groups publishes advertisements in forums and social media and then diverts traffic to the private domain to complete transactions.

Threat Hunter has detected that in discussion channels around the risks related to "purchasing, forwarding, cashback, and recycling" of state subsidies, threat actors often disguise themselves as "money-saving strategies" and publish, attract traffic, and trade through channels such as social media, forums, and instant messaging software.

5. Analysis of the methods used by various actors in the state subsidy industry chain to obtain preferential state subsidy

In the first half of 2025, Threat Hunter discovered through multi-channel monitoring that cybercriminal groups have formed a variety of fraud methods around "China's national consumer subsidy program", mainly including the following five categories:

- Scalpers recruit on social platforms, and couriers become illegal accomplices. Scalpers recruit users through social platforms and guide them to fill in personal information through WeChat groups, select products and place orders, and then use the couriers' illegal acceptance equipment to withdraw their national subsidy qualifications. This method exploits the loopholes in the collaboration between social platforms and couriers.

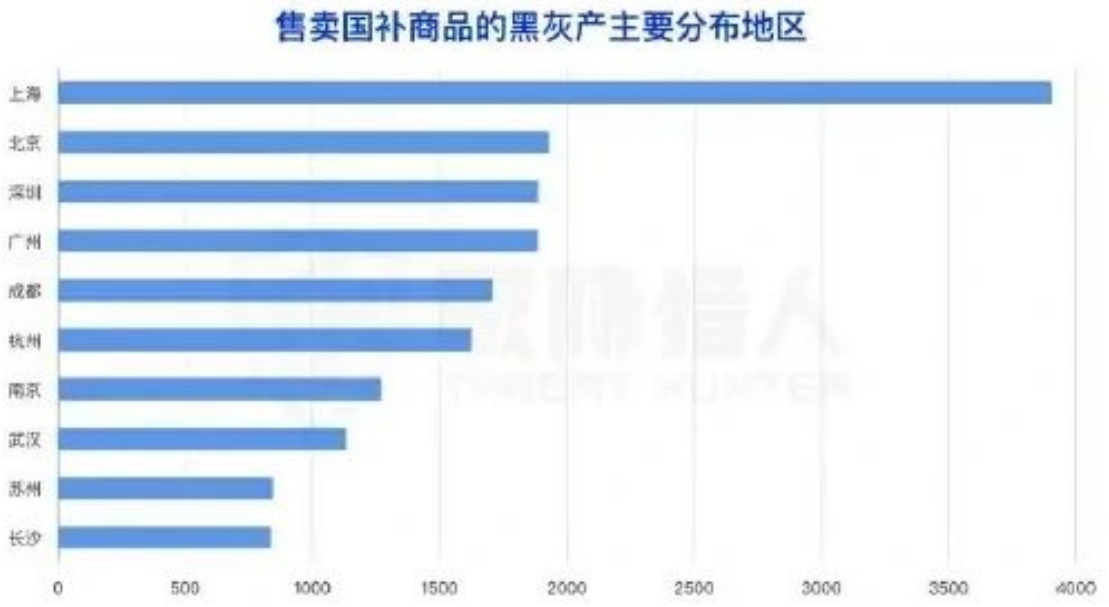
Status of the “national” fraud industry (figure 1)

Source: Threat Hunter original report, page 59

Status of the “State-backed” fraud industry (Chart 2)

Source: Threat Hunter original report, page 59

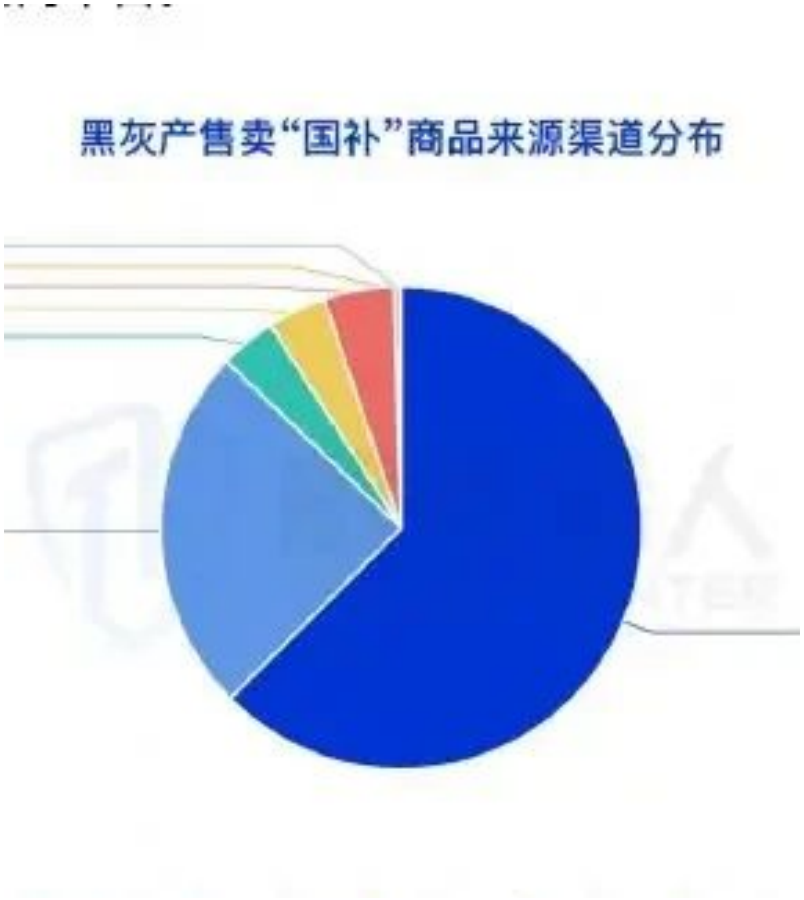
究人员根据监测到的各大交易平台中贩卖国补商品的个体黑灰产店铺注册地
品的黑灰产主要分布在上海、北京、深圳、广州等经济发达地区。



Current status of the “national” fraud industry (Chart 3)

Source: Threat Hunter original report, page 59

- Remote non-local activation by merchants. Some merchants allow buyers to activate devices remotely through WeChat video, bypassing the ID verification and equipment verification required by physical stores, and directly deliver the equipment to buyers via express delivery.
- Agents use triple preferential treatment to sell state-supplied products. Agents sell state-supplied goods at low prices through triple preferential treatment (state subsidy, trade-in, and platform discounts), and bypass the trade-in regulations by falsely recycling old products to further reduce costs.



Status of the “national” fraud industry (figure 1)

Source: Threat Hunter original report, page 60

Status of the “State-backed” fraud industry (Chart 2)

Source: Threat Hunter original report, page 60

- Social platform recruitment and resale of state subsidy qualifications, in-person non-compliant verification and mailing transactions. Users resell the state subsidy qualifications to others, and use family or friends to purchase equipment in stores on their behalf. After verification, the transaction is completed by mail, bypassing the qualifications and geographical restrictions of state subsidy.
- The courier assists in forwarding to bypass the regional restrictions of the national subsidy. The user negotiates with the courier to forward the equipment to a different place to complete the transaction, bypassing the regional restrictions of the national subsidy and continue to obtain subsidies.

6. Recently added: dismantling of two types of "extracting state subsidies from other places" techniques

In the second half of 2025, as the traditional model continued to be cracked down, the activity of traditional techniques decreased in the second half of 2025. The cybercrime ecosystem continued to innovate and developed new techniques of "off-site fraud and domestic supplementation". Recently, Threat Hunter discovered the following two new techniques:

1) The method of exploiting the decoupling vulnerability of the verification link between the coupon issuance platform and the payment platform mainly exploits the decoupling of the verification link between the coupon issuance platform and the payment platform. That is, the subsidy collection and payment links between the coupon issuance platform and the payment platform lack strict verification and verification. This allows cybercrime ecosystem to "receive the national subsidy on the coupon issuance platform in city A and complete the payment on the

payment platform in city B", bypassing the fraud-control measures of both parties and achieving cross-regional national subsidy collection.

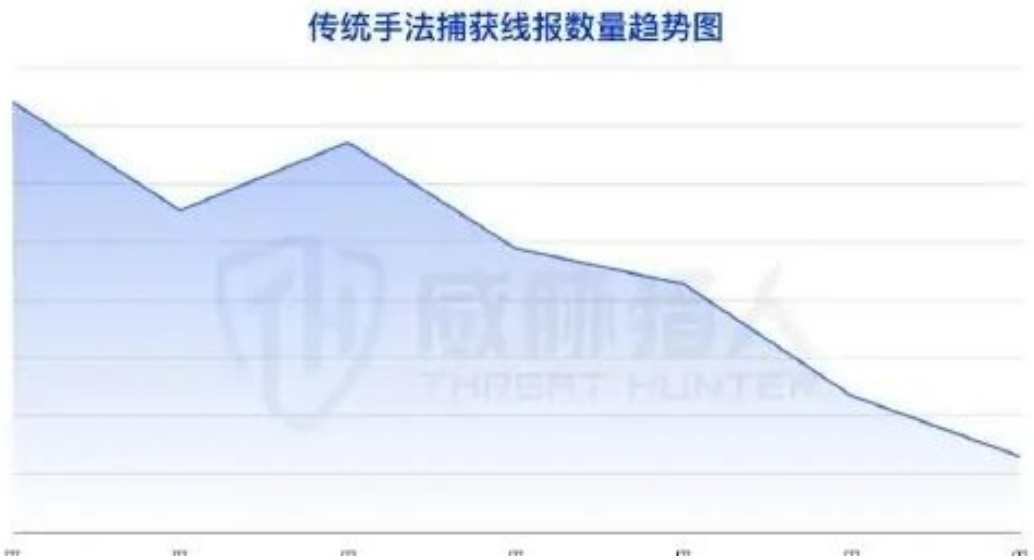
2) Virtual environment + positioning camouflage This method mainly uses the "Android virtual environment and positioning camouflage" technology to modify the geographical location of the device to receive subsidies in other places, then switch back to the real environment or use another device to complete the payment, and finally complete the national subsidy withdrawal.

3.2 Financial credit fraud analysis

Threat Hunter observed that due to the special governance of Tencent WeChat platform in August 2025 in response to the "Operation Qinglang", focusing on cybercrime ecosystem and illegal groups to implement relevant fraud controls policies, and since the second half of 2025, the Ministry of Public Security and the State Administration of Financial Supervision have jointly deployed financial cybercrime ecosystem crackdowns, the discussion volume on financial loans in the second half of 2025 is higher than that in 2025 There was a decrease in the first half of the year, but the overall public opinion on the risk of malicious loan fraud still increased.

Related noun definitions:

Malicious loan fraud refers to financial fraud that involves falsely advertising loan business in the name of a bank, packaging fraudulent loans, illegal loan increases, illegal re-loans, illegal cash-outs, induced loans, charging customers high fees, running away with money, defrauding customers for profit, issuing usury loans and other illegal businesses for personal gain. Business activities such as debt-taking, car financing, technology quota increase, beauty loan fraud, debt restructuring, AB loan, making fake statements, credit repair, debt optimization and other business behaviors.



Current status of the “national” fraud industry

Source: Threat Hunter original report, page 62

Debt optimization: usually refers to the process of adjusting and optimizing the debtor's debt structure, repayment methods, interest costs, etc. through agency complaints, agency rights protection, etc., in order to reduce the debtor's repayment pressure and improve the financial situation. Debt optimization is related to debt evasion, which mainly involves the implementation

of installment repayments, deferred installments, reductions and exemptions, etc. through threat actors' agency complaints, etc., so as to achieve the purpose of delaying and reducing debt repayments.

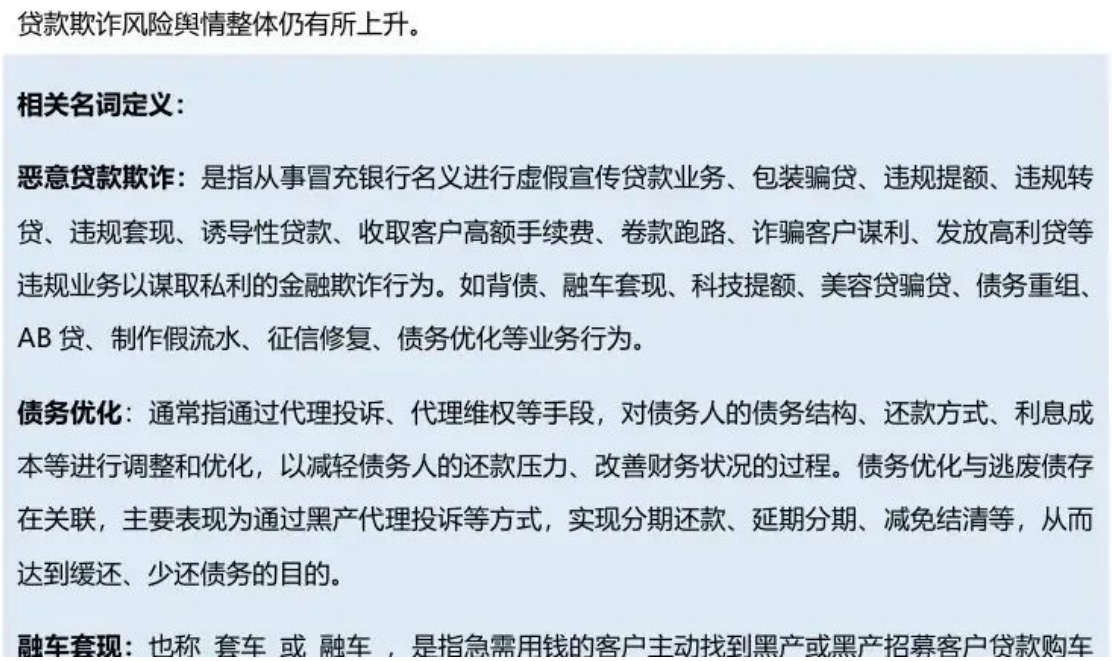
Car financing and cashing out: also known as car financing or car financing, refers to the behavior of customers who are in urgent need of money actively finding threat actors or threat actors to recruit customers to buy cars with loans and then resell the vehicles to cash out.

Professional debt: refers to having no loan qualifications at all (such as pure white, novice, small flower, low education level) or low qualifications

People who are willing to take on debt apply for large bank loans under the package of threat actors. Professional debt-taking is for the purpose of high profits and has no intention of repaying the debt. Professional debts are mainly divided into 2 categories: one is "packaged loans" and the other is "bad debts". Packaged loans: the act of defrauding banks of high loans by fabricating identities and forged materials, such as "house", "credit", "business", "car". Bad loans: bad debts or non-performing assets under the name of a company affect the company's operation or reputation. The company uses equity transfer, asset disposal, mortgage, etc., and the debtor bears the company's debt alone, such as "Business Straight Back", "Bank Straight Back"

Financial credit fraud analysis (Chart 1)

Source: Threat Hunter original report, page 63



贷款欺诈风险舆情整体仍有所上升。

相关名词定义：

恶意贷款欺诈：是指从事冒充银行名义进行虚假宣传贷款业务、包装骗贷、违规提额、违规转贷、违规套现、诱导性贷款、收取客户高额手续费、卷款跑路、诈骗客户谋利、发放高利贷等违规业务以谋取私利的金融欺诈行为。如背债、融车套现、科技提额、美容贷骗贷、债务重组、AB 贷、制作假流水、征信修复、债务优化等业务行为。

债务优化：通常指通过代理投诉、代理维权等手段，对债务人的债务结构、还款方式、利息成本等进行调整和优化，以减轻债务人的还款压力、改善财务状况的过程。债务优化与逃废债存在关联，主要表现为通过黑产代理投诉等方式，实现分期还款、延期分期、减免结清等，从而达到缓还、少还债务的目的。

融车套现：也称 套车 或 融车 ，是指急需用钱的客户主动找到黑产或黑产招募客户贷款购车

Financial credit fraud analysis (figure 2)

Source: Threat Hunter original report, page 63

3.2.1 In 2025, public opinion on malicious financial loan fraud and the scale of cybercriminal groups will maintain rapid growth

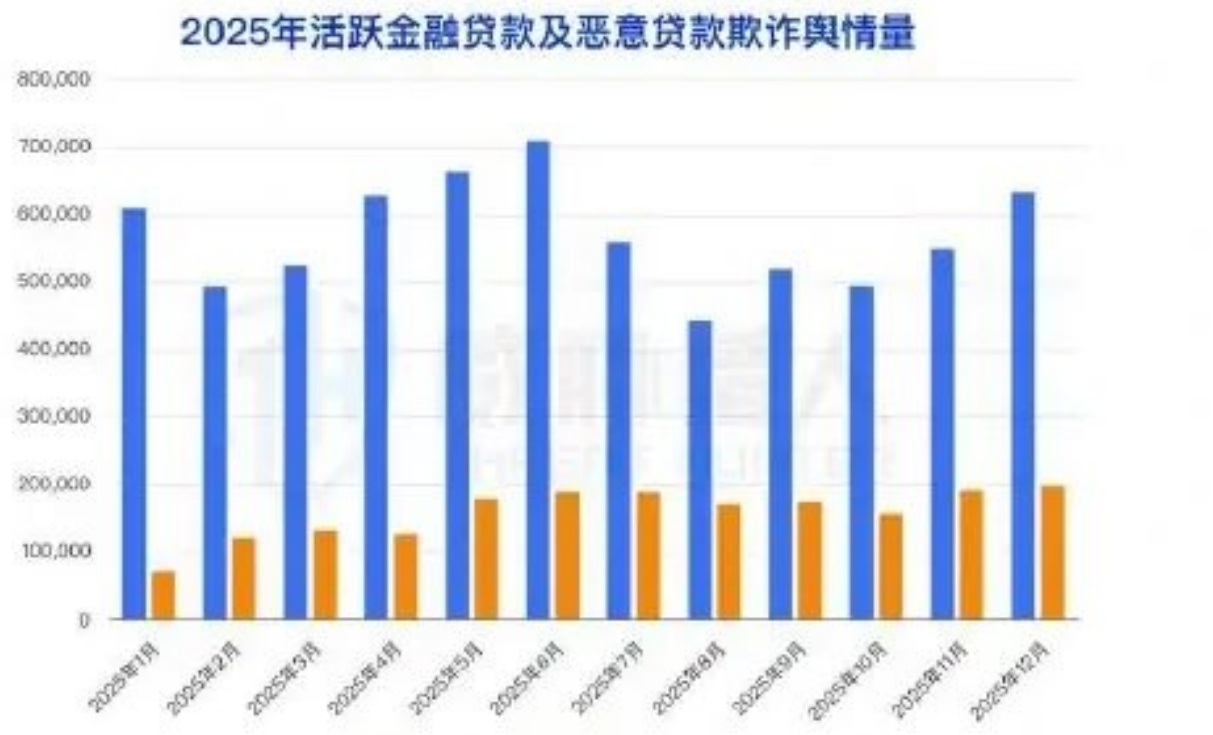
3.2.1.1 Public opinion on malicious financial fraud in the second half of 2025 increased by 32% compared with the first half of 2025

In 2025, Threat Hunter monitored and captured 6.8 million public opinions on financial loan risks, including 1.89 million public opinions on malicious loan fraud, accounting for 27% of the total.

The public opinion on financial loans in the second half of 2025 decreased by 12% compared with the first half of 2025, and the public opinion on the risk of malicious loan fraud in the second half of 2025 increased by 32% compared with the first half of 2025.

3.2.1.2 In 2025, Threat Hunter monitored a total of 37,000 active financial loan groups, including 18,000 malicious fraud groups, accounting for 50% of the total.

增长 32%。



Financial credit fraud analysis

Source: Threat Hunter original report, page 64

3.2.1.3 The number of malicious loan fraud accounts accounted for 30% of financial loan accounts in 2025

In 2025, Threat Hunter monitored and captured a total of 330,000 active loan service accounts, of which 100,000 were fraudulent accounts (credit black intermediaries/threat actors) providing malicious loan services, accounting for 30% of the total.

3.2.1.4 Main types of malicious loan fraud in 2025 top 3: professional debt, debt optimization, credit repair

Data in 2025 shows that malicious loans mainly involve more than 9 types of fraud, including professional debt, debt optimization, credit repair, material fraud, car financing fraud, debt restructuring, etc. Among them, professional debt accounts for 37%, ranking first, becoming the core attack method of threat actors; debt optimization and credit repair rank second and third respectively, and the proportion of debt optimization agency complaint business has doubled.

Note: Debt optimization includes: anti-collection, agency rights protection, agency complaints, interest refunds and other debt processing scenarios.

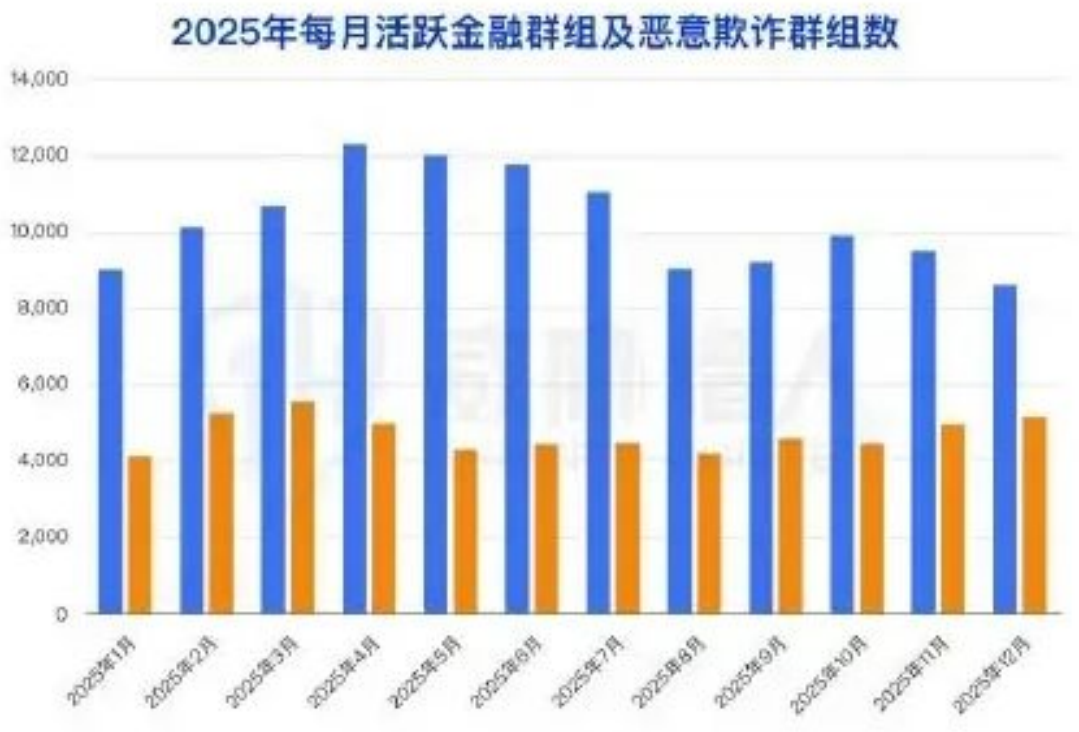
3.2.1.5 Top 5 malicious loan fraud risk areas in 2025: Guangdong, Sichuan, Shandong, Jiangsu, Zhejiang

Threat Hunter intelligence data shows that the top five provinces (including municipalities) with active malicious loan fraud in 2025 are Guangdong, Sichuan, Shandong, Jiangsu, and Zhejiang. Among them, the risk value in Guangdong is much higher than other regions.

3.2.1.6 Top 5 cities with malicious loan fraud risks in 2025: Chongqing, Shenzhen, Chengdu, Shanghai, Beijing

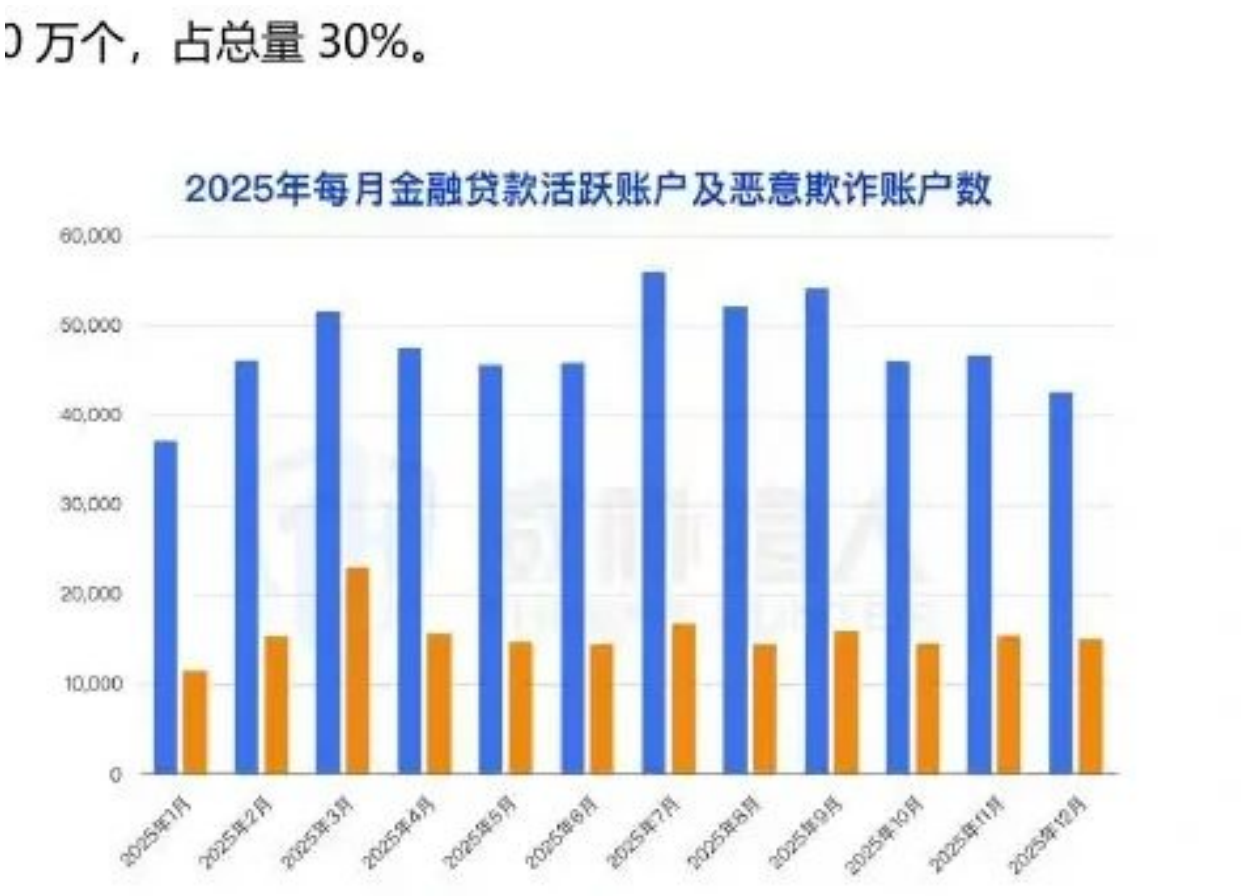
Threat Hunter intelligence data shows that the top five cities (including municipalities) with active malicious loan fraud in 2025 are Chongqing, Shenzhen, Chengdu, Shanghai, and Beijing.

3.2.2 Public opinion on occupational debt risks will still maintain a rapid growth rate in 2025



The main type of malicious loan fraud in 2025: Top3: professional debt default, debt optimization, credit-record repair (Chart 1)

Source: Threat Hunter original report, page 65



The main type of malicious loan fraud in 2025: Top3: professional debt default, debt optimization, credit-record repair (figure 2)

Source: Threat Hunter original report, page 65

3.2.2.1 The monthly discussion volume on occupational debt risks will continue to grow in 2025, with an increase of 59% in the second half of the year compared with the first half of the year.

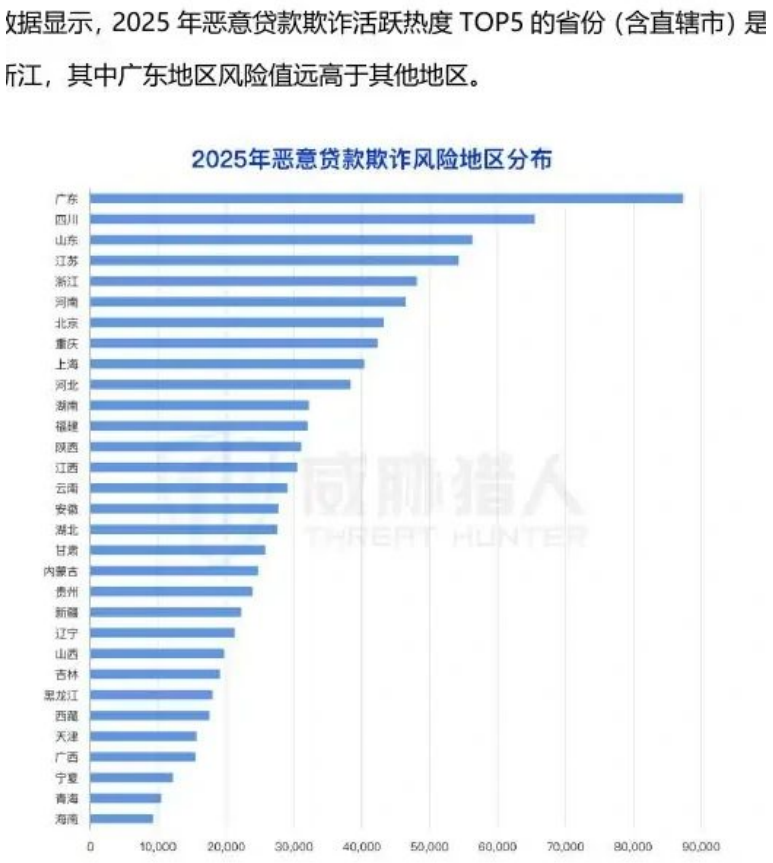
In 2025, Threat Hunter monitored and captured 370,000 public opinions on occupational debt risks. Overall, monthly risk public opinions continued to grow, with an increase of 59% in the second half of 2025 compared with the first half.

3.2.2.2 Top 5 provinces with debt-ridden areas in 2025: Guangdong, Sichuan, Shandong, Henan, Chongqing

Threat Hunter intelligence data shows that the top five most active provinces (including municipalities) for debt-related loan fraud in 2025 are Guangdong, Sichuan, Shandong, Henan, and Chongqing.

Top5: Guangdong, Sichuan, Shandong, Jiangsu, Zhejiang (figure 1)

Source: Threat Hunter original report, page 66



Top5: Guangdong, Sichuan, Shandong, Jiangsu, Zhejiang (figure 2)

Source: Threat Hunter original report, page 66

3.2.2.3 Popularity of debt-ridden cities in 2025 Top 5 cities: Chongqing, Guangzhou, Chengdu, Shanghai, Shenzhen

Threat Hunter intelligence data shows that the top five most active cities (including municipalities) for debt-related loan fraud in 2025 are Chongqing, Guangzhou, Chengdu, Shanghai, and Shenzhen.

3.2.2.4 The strategy upgrade of professional debt-bearing threat actors and the risk differentiation of loan scenarios in 2025

In 2025, the operational strategy of professional debt-assumption threat actors was comprehensively upgraded: the operating mode shifted from working alone to resource sharing and profit-maximizing cooperation among threat actors; the target customer group shifted from focusing on the selection of "pure white households" with good credit records to "high-quality novices" with good credit records;

The attack scenarios have shifted from full coverage of "housing, credit, enterprise and automobile" to accurately selecting the best scenarios based on the qualifications of the debtor.

Monthly occupational debt risk profile continued to increase in 2025, with 59 per cent growth in the second half of the year compared to the first half of the year

Source: Threat Hunter original report, page 67

Judging from the growth rate of public opinion on the risk of debt attacks, different scenarios showed significant differentiation in the second half of 2025. Among them, consumer loan and corporate loan scenarios have high risks, with month-on-month growth rates exceeding 80% in the second half of the year, making them the main growth areas; in comparison, the growth rates of housing loans and car loans are relatively slow, with month-on-month growth rates of 46.2% and 13.1% respectively.

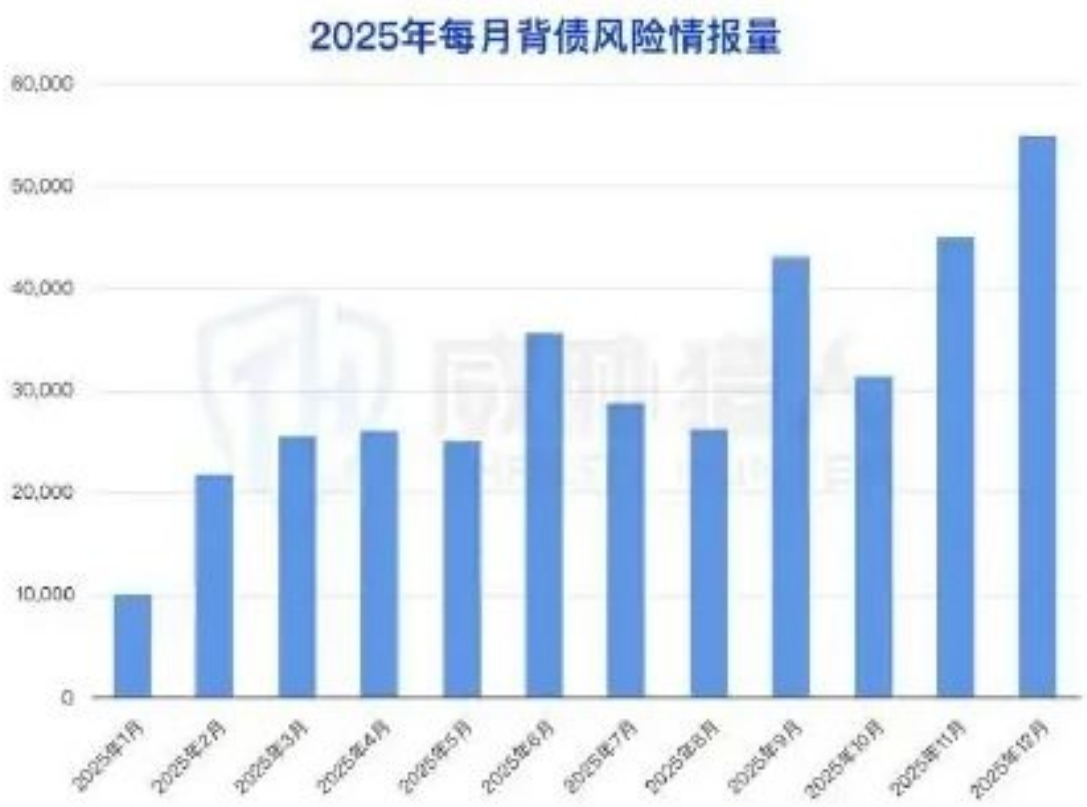
Public opinion on the risk of consumer loan debt will surge in 2025, with the second half of the year doubling compared to the first half of the year to 103%

Public opinion on the risks of corporate loans and liabilities remained at a high level in 2025, with a month-on-month growth of 87.8% in the second half of the year

3.2.3 Introduction to typical fraud risk types in different scenarios of financial loans

Currently, home loans, car loans, consumer loans and corporate loans, as core credit scenarios, have become key attack targets for threat actors. Due to different product characteristics and fraud controls logic, different loan scenarios not only have different degrees of attack, but also have different types of fraud risks.

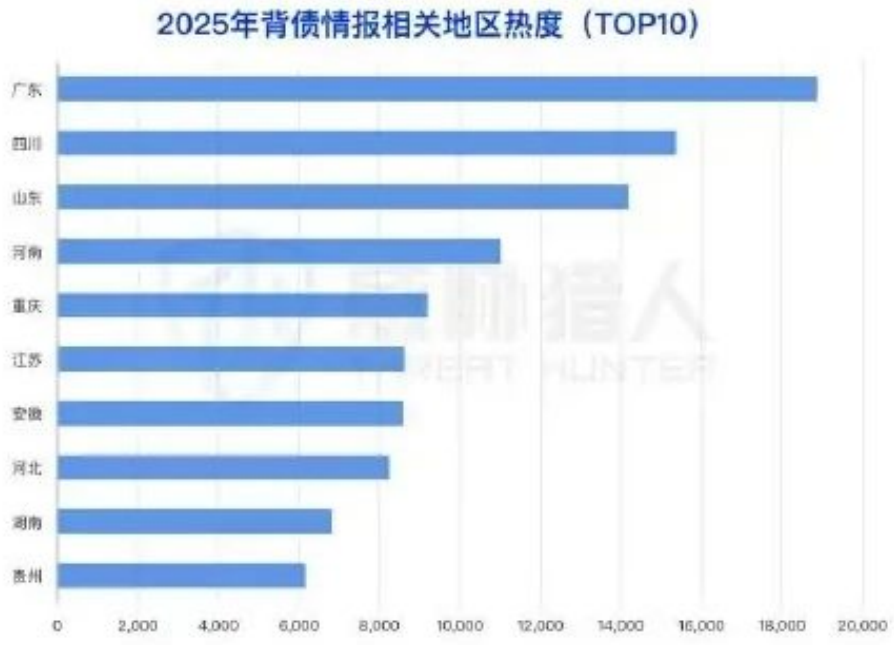
The following are the mainstream fraud methods currently faced in various loan scenarios:



Top5 Cities: Chongqing, Guangzhou, Chengdu, Shanghai, Shenzhen (Chart 1)

Source: Threat Hunter original report, page 68

居显示，2025 年背债相关的贷款欺诈，活跃热度 TOP5 的省份河南、重庆。



Top5 Cities: Chongqing, Guangzhou, Chengdu, Shanghai, Shenzhen (Chart 2)

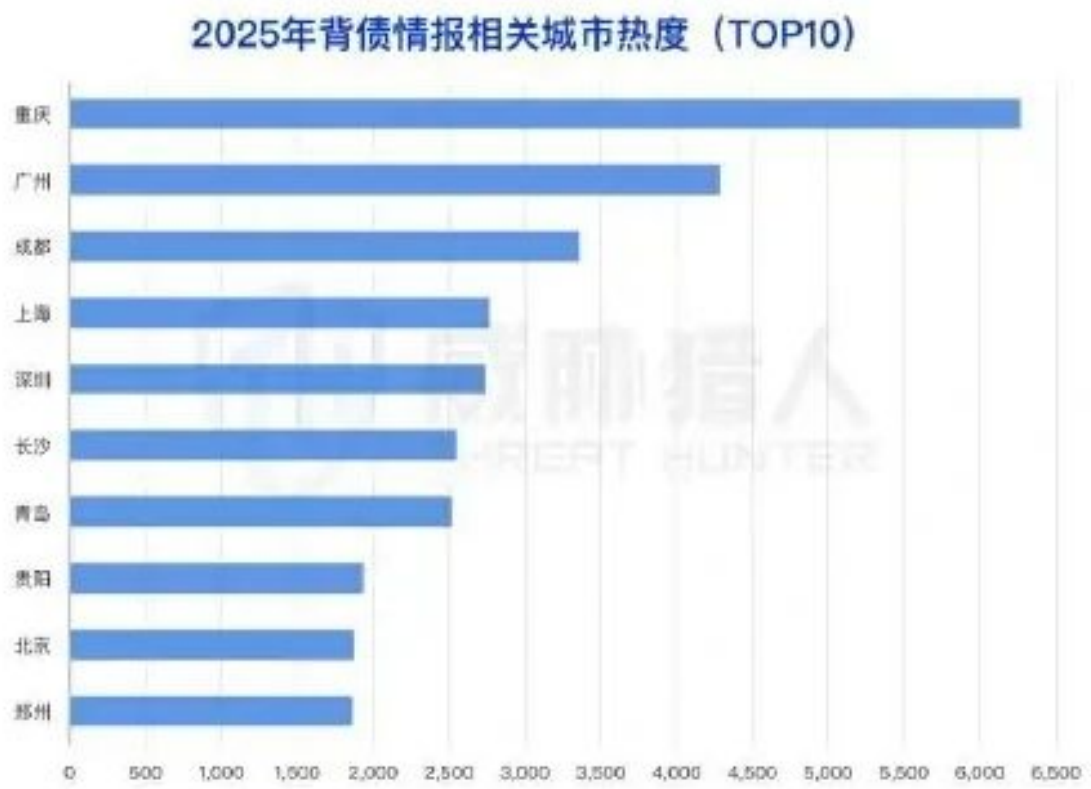
Source: Threat Hunter original report, page 68

Focusing on this area, Threat Hunter will subsequently release the "2025 China Credit Fraud Risk Trend Report" to conduct more systematic and in-depth research and interpretation of the above-mentioned related issues.

3.3 Analysis of Phishing and Counterfeiting Scenarios

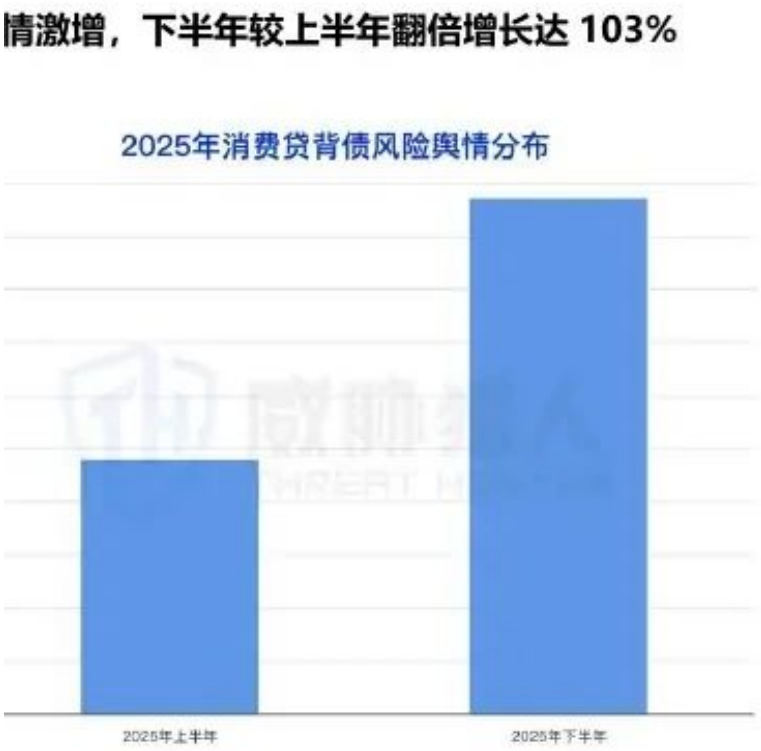
3.3.1 Distribution of risk event types: counterfeit website risks account for 30%, social media and customer service counterfeit risks have increased significantly

Throughout 2025, Threat Hunter captured a total of 17,000 cases of phishing counterfeiting risk events, involving 237 companies. The overall trend showed significant seasonal outbreaks and method replacement.



Disaggregation of risks between the upgrading of the strategy and the lending landscape in 2025 (Chart 1)

Source: Threat Hunter original report, page 69



Disaggregation of risks between the upgrading of the strategy and the loan landscape in 2025 (Chart 2)

Source: Threat Hunter original report, page 69

Judging from the types of risk events:

- The risk of counterfeit website is firmly in the "cornerstone" position, with an obvious outbreak in Q1: a total of 50,000 counterfeit website attacks were captured in 2025 (accounting for 33.2%). Although the growth rate slowed down in the second half of the year, it dominated the first quarter. As the infrastructure for fraudulent links, building fake sites to steal sensitive data is still the core method of attackers.
- The risk of social media and customer service counterfeiting has increased significantly: It is worth noting that the number of attacks related to counterfeit social media and counterfeit customer service calls has increased significantly in the third quarter, and is highly related to the increase in social activity brought about by the "summer economy", reflecting the rapid response ability of threat-actor groups to periodic traffic hot spots.

Counterfeit social media (distributed fission communication): In response to the craze of the summer game market, cybercriminal groups adopted a combination of "self-maintained high-weight accounts + distributed fission". In addition to the traditional self-operated account matrix, a large number of accounts that look like ordinary users are used to publish highly homogeneous counterfeit and induced content (such as false benefits, high-proportion rebates, etc.) on social platforms. This model greatly improves the survival rate of illegal content to bypass the platform's review mechanism. Its core purpose is to accurately intercept and divert official traffic to illegal game private servers to achieve rapid cash-out.

Description of typical types of fraud risk in different scenarios of financial lending

Source: Threat Hunter original report, page 70

Fake customer service phone numbers (GEO poisoning): During the third quarter of 2025, the attack group targeted high-frequency search terms such as "customer service, interest refund, and unfreeze" in lending apps, exploited search engine algorithm loopholes to dominate the screen regionally, and directly embedded fake customer service phone numbers in prominent positions in search results.

This technical method no longer relies on passive text messages to cast a wide net, but achieves precise traffic "interception" of users who actively seek help. The extremely high attack reach rate directly promotes the explosive growth of risk data during this period.

3.3.2 The financial industry is the main target of attacks by threat actors

Monitoring data in 2025 shows that phishing and counterfeiting risks are characterized by "high financialization and broad-spectrum coverage within finance". The attack strategies of threat actors have shifted from focusing on a few leading institutions to large-scale coverage and layered harvesting of the financial industry.

From the perspective of industry distribution, the financial field (securities, banks, consumer finance, funds, etc.) accounts for a total of 76.28%. Among them, core business scenarios such as banking, securities and consumer finance that can directly lead to capital losses or account takeovers are still the key targets of threat actors' priority attacks;

The incidence of fishing simulators has varied from quarter to quarter, and there has been a marked increase in the third quarter of the simulator between the media and the client.

Source: Threat Hunter original report, page 68

But at the same time, the attack scope of threat actors is no longer limited to a few leading institutions. Instead, through batch registration of domain names, templated site reuse, and scripted delivery, a large number of small and medium-sized financial institutions have been systematically included in the scope of counterfeiting.

Non-financial transaction scenarios focus on diversion and monetization: for example, the e-commerce industry (10.31%) mainly serves as an entrance for payment and refund induction; while the blockchain industry (4.64%) and the gaming industry (4.12%) take advantage of the high volatility of assets to implement airdrops or recharge interceptions.

Overall, attackers systematically exploit financial brand trust and users' psychological expectations for "official notifications, account anomalies, and compliance verification" to promote the upgrade of counterfeiting from "doing more like it" to "wider coverage and more frequent contact", and form a closed-loop monetization in key links such as login, transfer, verification code/authorization, etc.

3.3.3 New brand risks in the era of AI large models: GEO poisoning by spoofing customer service phone numbers

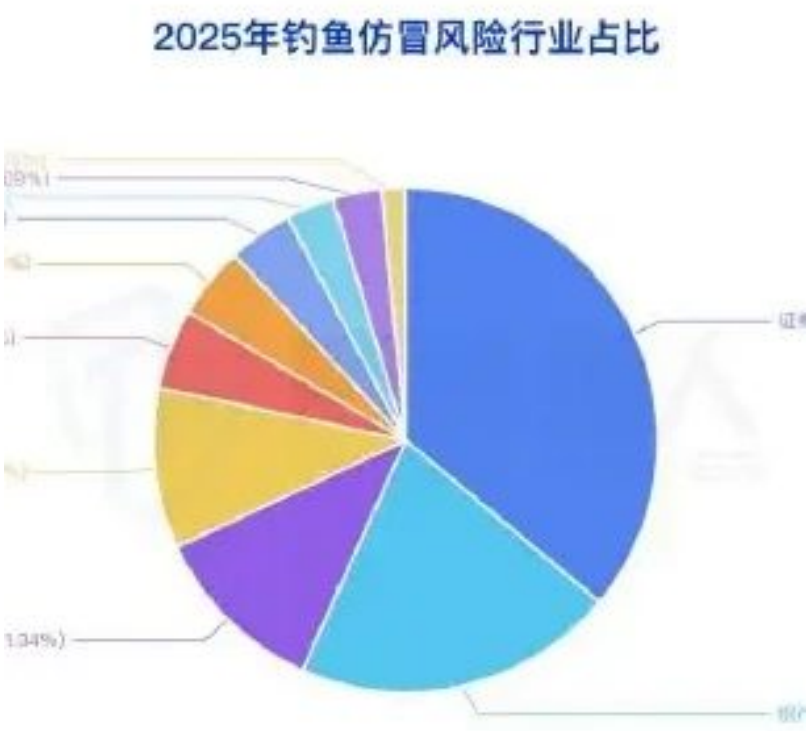
3.3.3.1 Upgrading from “fake customer service phone number” to “information supply that pollutes AI”

In the past, cybercrime ecosystem mainly relied on counterfeit websites, SMS phishing, search advertising, etc. to obtain users, and its attack links were concentrated in the "link layer".

仿冒客服电话（GEO 投毒）：2025 年第三季度期间，攻击团伙针对借贷类 APP 的“客服、退息、解冻”等高频搜索词，利用搜索引擎算法漏洞进行区域性霸屏，直接将虚假客服电话嵌入搜索结果的显眼位置。这种技术手段不再依赖被动的短信广撒网，而是实现对主动寻求帮助用户的精准流量“截杀”，极高的攻击触达率直接推动该时段风险数据的爆发式增长。

Type of risk event distribution: 30% of site risk imitation and significant increase in risk of social media and customer imitation (Chart 1)

Source: Threat Hunter original report, page 72



Type of risk event distribution: 30% of site risk imitation and significant increase in risk of social media vs. customer imitation (figure 2)

Source: Threat Hunter original report, page 72

As AI search and intelligent Q&A gradually become important portals for users to obtain official information and contact information, the attack surface has undergone fundamental changes - threat actors are no longer just "counterfeiting corporate official websites", but have turned to polluting information sources cited by AI, allowing users to directly get wrong answers when asking questions such as "customer service phone number" and "official contact information" and proactively call them.

Threat Hunter monitoring found that in the third quarter of 2025, highly homogeneous and batch-generated articles appeared on multiple high-weight content platforms.

The text of these contents is mostly normal information, but fake customer service numbers are systematically implanted in key locations. This phenomenon is not an ordinary violation, but a typical GEO poisoning behavior.

3.3.3.2 What is GEO poisoning: using the reference mechanism of “generative search” for targeted deception

GEO poisoning refers to the cybercrime ecosystem borrowing and utilizing the "citation and synthesis" mechanism of generative search to deliberately construct and publish false or misleading content on a large scale, so that large models will preferentially reference this information when retrieving and generating answers, thereby outputting wrong results (such as fake customer service phone numbers) in scenarios such as AI search and intelligent question and answer, and ultimately leading users to fraudulent links.

The essential difference is:

Traditional attacks affect "where users click", while GEO poisoning affects "what AI directly tells users".

3.3.3.3 Four changes in new GEO poisoning compared to traditional phishing counterfeiting

- Changes in the attack entrance: from "click on the link" to "believe in the answer". In the generative search scenario, users no longer judge whether the link is suspicious, but directly accept the answer generated by the system. The attack entrance has been shifted from identifiable counterfeit pages to "authoritative and natural consultation results", which significantly reduces the user's prevention and verification probability.
- Changes in attack targets: Upgrading from "traffic hijacking" to "cognitive hijacking" GEO poisoning does not pursue a single exposure, but creates "majority consistent" false information through repeated spreading, allowing AI to form stable misjudgments when integrating multiple sources, and directly manipulate the user's decision-making path.
- Changes in attack vectors: From low-quality website groups to "high-weight content platforms" Threat Hunter monitoring data shows that GEO poisoning content has been significantly concentrated on platforms that are easier to enter the model reference system. News platforms account for 60%, video platforms account for 16%, article platforms account for 9%, and question and answer platforms only 1%. They are no longer the main positions. High-weight platforms account for a total of 86%, becoming the main source of pollution that affects AI retrieval and generation results. This means that even if the information on the company's official website is completely correct, it may still be overwritten by "wrong information from authoritative platforms" in the AI □□scenario.
- Changes in attack methods: The attack methods of threat actors are more scaled, templated, and reusable. threat actors have formed a highly standardized and replicable "three-piece set" around GEO poisoning:

1. Use high-weight platforms to increase the probability of entering the model reference library;

2. Use scripting to generate content in batches. The core strategy is to use the same fake number (such as “XXX Manual Hotline”).

00xx-6xxx-73xx”), and automatically replace hundreds of different financial brand names through scripts to achieve an extremely low-cost cross-platform “poisoning matrix”.

3. The content is packaged in standardized news genres. About 95% of the article is true but irrelevant information, and fake contact details are only embedded in key positions.

This method uses the model's trust preference for "authoritative narrative" to improve the concealment of poisoning content.

GEO poisoning influences the reference, integration and final answer to the generated search by polluting high weight information sources.

Source: Threat Hunter original report, page 73

3.3.3.4 Four types of direct impacts after AI search results are contaminated

With the continued influence of GEO poisoning, its harm no longer remains at the content level, but is directly reflected in the final output results of AI search and intelligent question and answer, having a substantial impact on user decision-making and brand safety.

Take a real case monitored by Threat Hunter as an example:

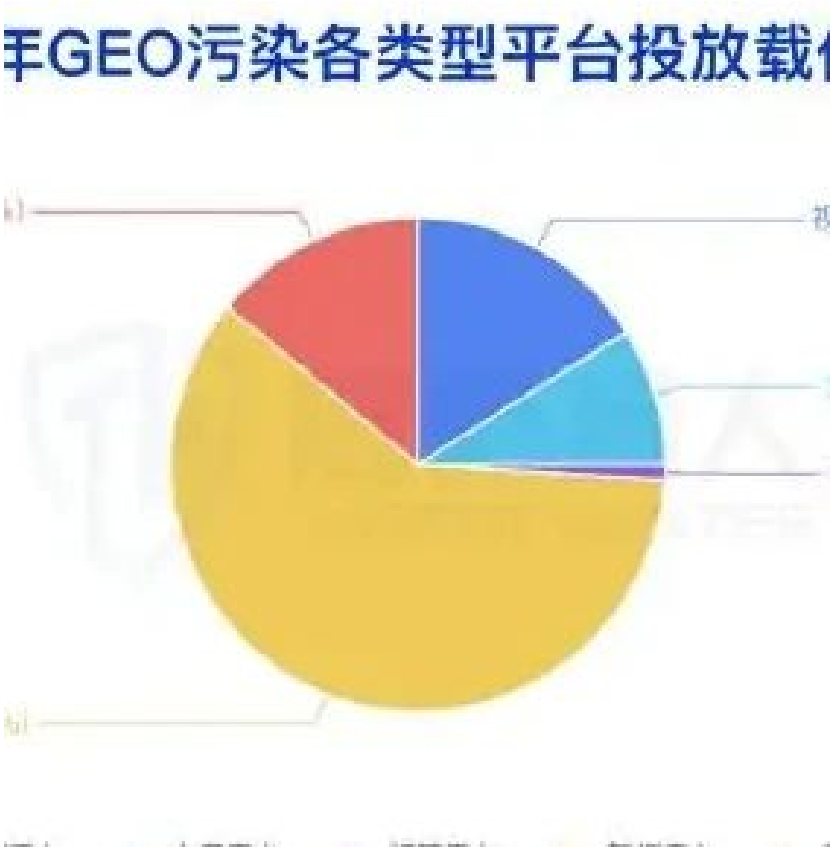
As shown in the figure below, when users query high-frequency requirements such as "customer service phone number" and "official contact information" of a brand through AI search scenarios, AI does not only refer to the brand's official website or authoritative channel information, but comprehensively calls multiple contaminated high-weight platform contents as "reference materials", and conducts structured integration and re-output of this information in generative answers.

In the above case, the use of AI search results presents the following obvious risk characteristics:

1. Fake customer service phone numbers are displayed as “official information”

The implanted numbers do not appear in the form of advertisements or abnormal content, but are organized into customer service information lists, announcements or reference materials. The overall presentation method is close to official channels, making it difficult for ordinary users to distinguish the authenticity.

2. Repeated citations amplify the impact of misinformation



Four changes in new GEO poisoning compared to traditional fishing imitations (Chart 1)

Source: Threat Hunter original report, page 75

Examples of AI-search poisoning and liability-complaint traffic diversion promoted through apps and social channels.

Source: Threat Hunter original report, page 75

The AI generated answers by simultaneously referencing multiple sources that contained the same fake numbers that were served in batches. When the same information appears repeatedly on different pages, the erroneous content is further amplified and solidified.

3. Users are directed directly to high-risk contacts

In AI search scenarios, users usually directly accept the contact information in the generated results, and rarely conduct secondary verification. Once you call a fake customer service number, it is very easy to enter the stage of fraud or information theft.

4. Brand official channels are weakened or even replaced

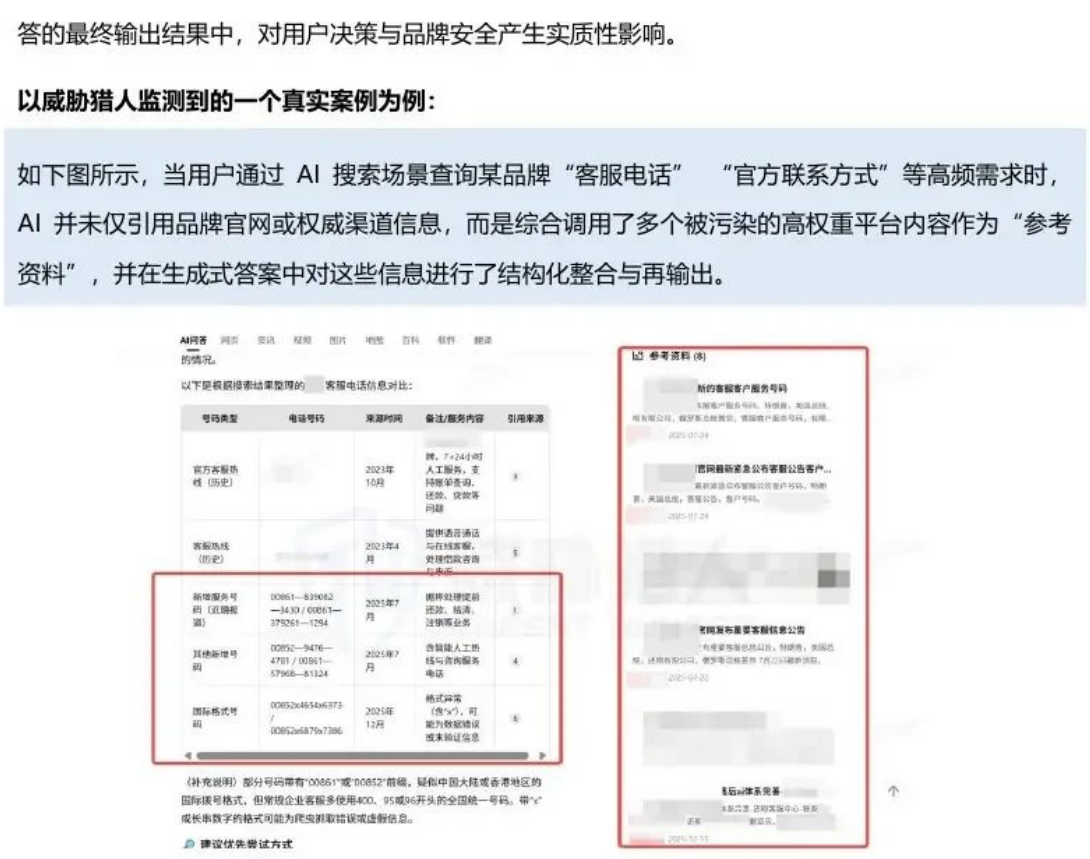
Even if a brand has disclosed correct official customer service information, it may still be overwritten or squeezed out in the AI output results, causing users to be exposed to wrong content first.

3.3.3.5 Governance idea: "two-pronged approach" of source disposal + AI side correction

The Threat Hunter DRP brand protection team adopts a "source and terminal two-pronged" governance strategy to address GEO poisoning risks, which not only compresses the cybercrime ecosystem space, but also ensures the brand's authority and security in AI search and Q&A.

- Cut off the source of pollution: quickly collect evidence on poisoning content and initiate removal applications from relevant channels, covering social media, Q&A, videos, articles and

other platforms. Monitoring practice shows that the success rate of removal can reach 93%, which can directly block the diffusion link.



AI Four types of direct impact after contamination

Source: Threat Hunter original report, page 76

- Promote AI platform correction: synchronously submit poisoning clues and evidence to the AI platform, require correction of search results and reference libraries, and reduce the probability of continued generation of erroneous information; combine automated inspections + manual review, and continuously monitor high-frequency query terms such as "brand name + customer service phone number/official contact information" to form a long-term protection closed loop.

3.4 Analysis of data leakage scenarios

3.4.1 A total of 41,644 data breaches occurred in 2025, an increase from the previous year in 2024

Reported share: 10.83%

Data from the Threat Hunter data leakage risk monitoring platform shows that from January to December 2025, the entire network monitored 767 million pieces of intelligence about data leaks. Based on the Threat Hunter authenticity verification engine and DRRC professional manual analysis, a total of 41,644 effective data leakage incidents were verified, involving a total of 2,120 companies in key industries such as finance, e-commerce, and express delivery.

- The annual data in this report does not include some overseas and unidentified corporate entity data leakage incidents. The statistical caliber has converged compared with the first half of the year, and the changes in relevant indicators are mainly caused by this.

3.4.2 The banking industry’s data leakage risk ranks first for three consecutive years, and the software application industry ranks first for the first time.

3.4.2.1 Risks in the financial industry are leading in a "faulty" manner

In 2025, the areas hardest hit by data breaches will further concentrate on capital-intensive industries. Data breaches in the banking industry ranked first, while the consumer finance industry overtook the e-commerce industry and jumped to second place. Including payments (rising to Top 4) and securities (rising to Top 5), which have moved up significantly, the "pan-finance" sector has occupied four of the top 5, showing that threat actors focus their attacks on credit and capital flow data with high realizable value.

3.4.2.2 The intelligence on “strong access” to local life has dropped significantly, and software applications have replaced local life as a new target.

The "Software Application" industry replaced the "Local Life" industry and ranked among the Top 10 for the first time. According to Threat Hunter's observation, on the one hand, the "forced login" file checking leaks that were popular in the local lifestyle industry in 2024 dropped significantly in 2025 (-61.38%). It is speculated that the local lifestyle companies involved have taken corresponding fraud-control measures to deal with the leakage risk, raising the threshold for threat actors to steal data. Therefore, upstream threat actors who steal data shift the focus of their attacks to mobile user behavior data with dynamic value, such as in-app interaction behavior, location and trajectory information, etc.

3.4.3 Consumer loan user information leakage incidents continue to increase, and new leakage methods are diversified

From the perspective of time distribution, illegal data trading incidents in the consumer finance industry showed an obvious upward trend in stages in 2025. From the beginning of the year to the first half of the year, the number of related incidents was at a relatively low level and grew slowly; after entering the second half of the year, the number of incidents began to increase significantly, and reached the high point of the year from October to November; through in-depth analysis, Threat Hunter found that the increase in consumer finance illegal data trading incidents was mainly concentrated in several emerging data types.

In the list of "hot-selling data types" mentioned in the threat actors channel, data types such as "consumer loan application", "bank scan code" and "multiple loans" appear frequently. Especially the data of "Consumption Fund Application"; taking the hot-selling list updated weekly by an threat actors channel as an example, this type of data product has continued to rank among the top-selling products from August 2025 to December 2025, showing that it has formed a stable and

active trading demand in the illegal data trading market. At the same time, usage feedback from downstream malicious activity scenarios also reflects that this type of data has high value in terms of authenticity and usability.

In 2025, two distinct high-level gaps emerged between the beginning and the fourth quarter of the year.

Source: Threat Hunter original report, page 79

(In the hot-selling list of data types updated every week on the channel of an threat actors group, "consumer money application" data has long ranked first)

(Downstream malicious activity effect feedback reflects the authenticity of the data)

3.4.3.1 Analysis of “Consumer Financing Application” Risk Trends and Industrial Ecology

1. Consumer loan application data leakage incidents continue to rise, with more than 600 cases by December 2025, accounting for 10% of the total loan information data type.

70% Threat Hunter monitoring found that "spending application" data first appeared in some data trading threat actors at the end of May 2025, and then after a 2-month "testing" phase, it tasted the benefits, and was officially launched at the end of July 2025 for large-scale illegal data transactions.

Banking and consumer finance are the top two in the data-dissemination industry, with the pan-financial sector occupying four of the top five seats.

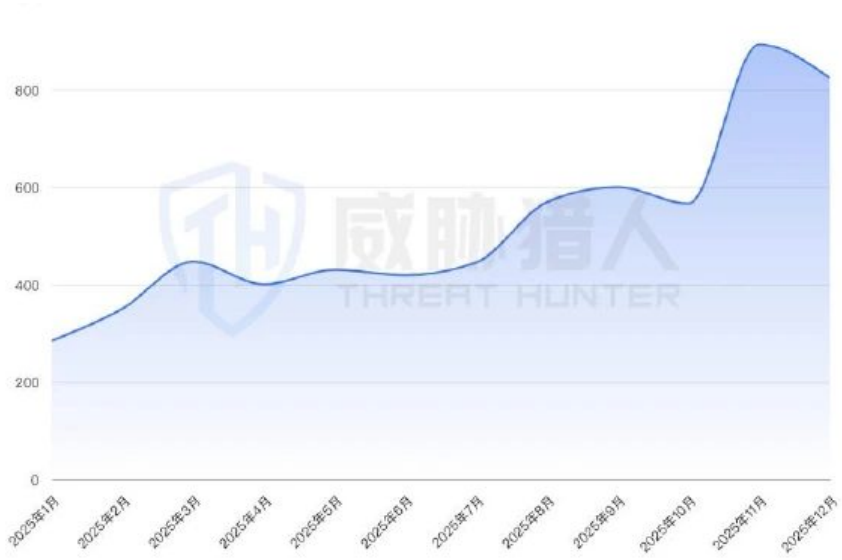
Source: Threat Hunter original report, page 80

threat actors promote intermediaries and reach their peak in December 2025, accounting for up to 70% of loan data types in the illegal data trading market. At the same time, judging from the changes in transactions and demand, the transaction volume of "finance application" data is highly consistent with the trend of purchase volume, and will simultaneously show explosive growth in the second half of the year.

According to Threat Hunter's observation, the leaked "consumer application" data, the leaked data sample format fields mainly include the user's phone number, platform name, name, region, and status information of successful loan application. Not all of the name information is included. Threat Hunter researchers followed up and learned from the threat actors intermediary who sold the data, and confirmed that some of the name information was information added for later cleaning and processing.

(The picture on the left shows the consumer finance application data format, and the picture on the right shows the feedback from threat actors that the name field was added for cleaning)

2. “Consumer Financing Application” product data is constantly iterated, involving most domestic consumer finance and loan platforms



The incidence of illegal data trading in consumer finance rose significantly in the second half of the year, reaching a high level between October and November.

Source: Threat Hunter original report, page 81

Threat Hunter conducted an in-depth analysis of "Consumer Fund Application" and found that the product data is mainly divided into four stages, namely the testing stage (May-June), official launch (July-August), refined operation (September-October), and AI model improvement stage (November). The following is the specific product development timeline.

(Consumption finance application product development timeline)

- Testing phase: (end of May - June)

As early as the end of May 2025, threat actors first proposed a clear "consumer finance application" product. The data type involves some consumer finance platforms and bank loan platforms. The data timeliness is overnight (T+1). It does not support designated platforms, but it can support screening of users' regions. It only involves 24 licensed consumer finance institutions and bank loan products.

- Officially launched: (July-August)

某黑产团伙频道每周更新的数据类型热销榜单中，“消金申请”数据长期高居第一

（下游作恶效果反馈，侧面反映了数据的真实性）

Source-channel examples showing demand for financial data and downstream feedback used to establish credibility.

Source: Threat Hunter original report, page 80

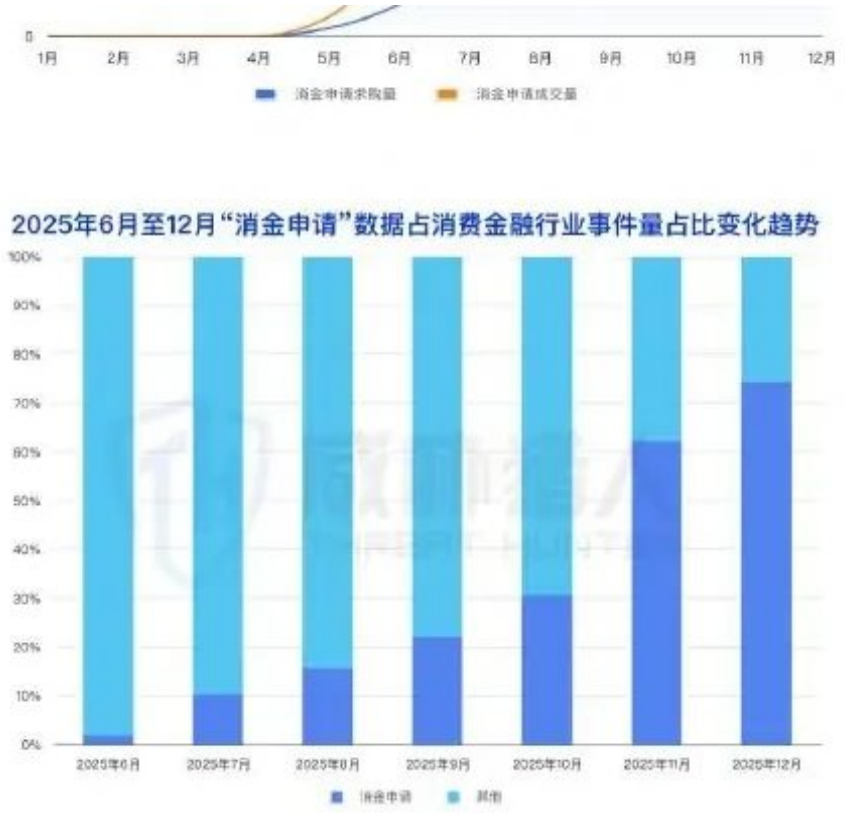
The "Consumer Finance Application" product data began to add corporate loan type data in early July, which is no longer limited to C-side loan demand users, and supplemented the information data of B-side or small and micro business owners; at the same time, it sorted out the behavioral characteristics of some users who applied on multiple loan platforms in a short period of time, and marked them as customers in urgent need of funds for downstream buyers to carry out precise malicious activity, involving 27 consumer finance/loan platforms.

(The picture shows that after threat actors officially launched consumer finance products, they added multi-platform tag features and model optimization)

:与需求变化来看，“消金申请”类数据的成交量与求购量走势高
发式增长。

Risk trends and industrial eco-analysis of “exempt applications” (Chart 1)

Source: Threat Hunter original report, page 81



Risk trends and industrial ecological analysis of “discharge applications” (figure 2)

Source: Threat Hunter original report, page 81

- Refined operation: (September-October)

threat actors divides and dismantles different types of platforms such as licensed consumer finance institutions, bank loans, online lending platforms, and corporate loans, in order to meet the needs of different downstream loan intermediaries (capitals) for bad user profiles; at the same time, the data type involves a total of 40 consumer finance/loan platforms, and supports filtering of specific platforms.

(The picture shows the platform list carefully compiled by threat actors)

- Data intermediary threat actors use AI models to clean original data and improve data value (November)

In early November, illegal data trading threat actors reported that the volume of "consumer loan application" data transactions reached a peak, causing the server memory to limit, and targeted optimization and cleanup were carried out; involving up to 60 platforms for consumer loan, bank products, online loan products, and corporate loan products. At the end of November, AI big data recognition was introduced, shifting from pure data sales to "data cleaning + quality control", trying to maintain high prices and high conversion rates of data by eliminating inferior user data.

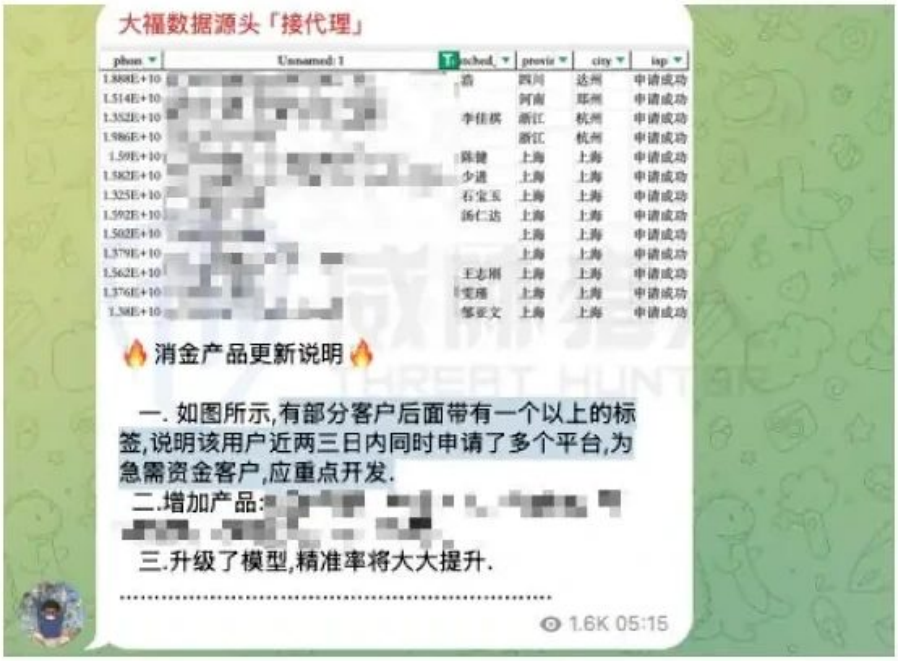
(threat actors continue to optimize and upgrade the consumer finance application model)

Risk trends and industrial ecological analysis of “discharge applications”

Source: Threat Hunter original report, page 82

- Downstream malicious activity: After threat actors obtain the data, they will carry out targeted post-loan marketing malicious activities. Threat Hunter monitoring found that after threat actors obtain "consumer application" data, they mainly use it for highly targeted post-loan marketing malicious activity actions. This type of malicious activity usually revolves around users who have "submitted loan applications" and implements misleading traffic and product promotion by pretending to be official or partner identities.

端或小微企业主的信息数据；同时梳理出部分用户在短时间内在多个贷款平台申请的行
标记为急需资金客户，供下游购买者进行精准作恶，涉及消金/贷款平台达 27 家。



（图为黑产正式上线消金产品后，补充了多平台标签特征以及模型优化）

Risk trends and industrial ecological analysis of “discharge applications”

Source: Threat Hunter original report, page 83

The following are two cases detected by Threat Hunter:

Example 1: Threat Hunter operators monitored a screenshot of "Consumer Finance Sales Test Techniques" released by a certain data trading threat actor on Telegram. They mainly contacted loan applicants by phone, pretending to be the account manager corresponding to the consumer finance loan platform, claiming that the other party's loan or business has been transferred to him, and then guiding users to switch products or promote other loan business products.

Example 2: Threat Hunter operators obtained script content from a certain loan telemarketing group. They mainly disguised themselves as employees of the customer follow-up department of the corresponding consumer loan platform to confirm loan qualification information with customers, and finally guided them to their physical stores to promote other loan products.

Focusing on this area, Threat Hunter will subsequently release the "2025 China Data Breach Risk Trend Report" to conduct more systematic and in-depth research and interpretation of the above-mentioned related issues.

月底，引入了 AI 大数据识别，从单纯的数据售卖转向“数据清洗+质量控制”，试图通过剔
质用户数据来维持数据的高价格和高转化率。

（黑产不断优化升级消金申请模型）

Risk trends and industrial ecological analysis of “discharge applications”

Source: Threat Hunter original report, page 85

Write at the end:

Looking back on 2025, cybercriminal groups will continue to improve the concealment and success rate of malicious activity by introducing attack resources that are closer to real users and using new technologies such as generative AI and agents, putting enterprises under greater pressure in terms of risk perception, identification and response.

The essence of security is a game against costs. We cannot completely eliminate cybercrime ecosystem, but we can continue to increase its attack costs and failure risks through a systematic defense system. When the attacker's investment in resource acquisition, technological breakthroughs and large-scale malicious activity is significantly higher than its potential income, the motivation and sustainability of cybercriminal groups will be fundamentally weakened. This is the key to the defender's advantage in "asymmetric confrontation".

The second half of defense is not only a technical battle, but also a competition of intelligence and cognition. This is also the direction Threat Hunter continues to invest in:

Through systematic cybercriminal groups attack and defense research and intelligence monitoring capabilities, we help enterprises take the initiative in confrontation and build a more resilient business security defense line.

Note: The data information provided in this report is estimated and analyzed by Threat Hunter based on large sample data sampling and collection, small sample survey, external intelligence data collection, data model prediction and other research methods. Due to the limitations of any data sources and technical methods in the field of statistical analysis, the data information estimated and analyzed based on the above methods are for reference only.

Risk trends and industrial ecological analysis of “discharge applications”

Source: Threat Hunter original report, page 86