THREAT HUNTER RESEARCH

H1 2025 Cybercrime Ecosystem Trends Report

A half-year view of changing attack resources, AI and payment abuse, and six fraud scenarios affecting digital businesses.

Original publication: 2025-07-22
Research team: Threat Hunter Research Team
Source report: 99 pages

Original report text

This text version is reconstructed based on the 99-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 first half of 2025, cybercriminal attacks on the Internet continued to evolve, showing a trend of becoming more covert, smarter, and more industrialized. The number of cybercrime operators continues to grow, and attack resources, technologies, and crime scenarios have been comprehensively upgraded. Overall, several major events in the cybercrime ecosystem in the first half of 2025 have always confirmed the core law of the cybercrime ecosystem market - threat actors never sleep. When the main trading platform is attacked, threat actors and their malicious activity needs will quickly migrate to existing or emerging alternative channels.

Summary of key points in the report:

In terms of attack resources, Threat Hunter captured an average of 13.82 million daily active risk IPs, an increase of 15.02% month-on-month. "Hijacking shared agent" IP attacks have become more rampant and the billing models have become more diverse; illicit SIM-card channels have shrunk significantly after regulatory crackdowns. At the same time, new "link code" methods have emerged to improve attack concealment; money laundering bank cards increased by 28.60% month-on-month, of which gambling-related cards accounted for 70.25%, a month-on-month increase. 141%, which is related to the new recharge method of the gambling platform "pending order recharge"; money laundering corporate accounts dropped by 40% month-on-month, and the targets of threat actors gradually shifted from the six major banks to city commercial banks and rural credit cooperatives; the number of merchants laundering money increased, and the industry was concentrated in terminal retail, wholesale and retail, and catering industries.

In terms of attack technology, AI capabilities have been deeply abused by threat actors. Minute-level AI face-changing and voice cloning have been widely used in electronic fraud and authentication bypass scenarios, significantly improving attack efficiency and deception. At the

same time, money laundering technical tools such as "code pulling tools" flow into the transaction chain of threat actors, which can directly transfer black money to the formal platform transaction path for laundering.

In terms of attack scenarios, typical scenarios such as marketing fraud, financial fraud, telecommunications fraud, phishing and counterfeiting, data leaks, and API attacks are still common, and the attack model has evolved from single-point operations to chain collaboration. Overall, cybercriminal groups have penetrated into the business chains of various industries, crime patterns are constantly being renovated, threats continue to expand, and the defense system is in urgent need of systematic upgrades.

In the face of the evolving cybercrime ecosystem threats, Threat Hunter released the "Internet cybercrime ecosystem research report for the first half of 2025". 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.

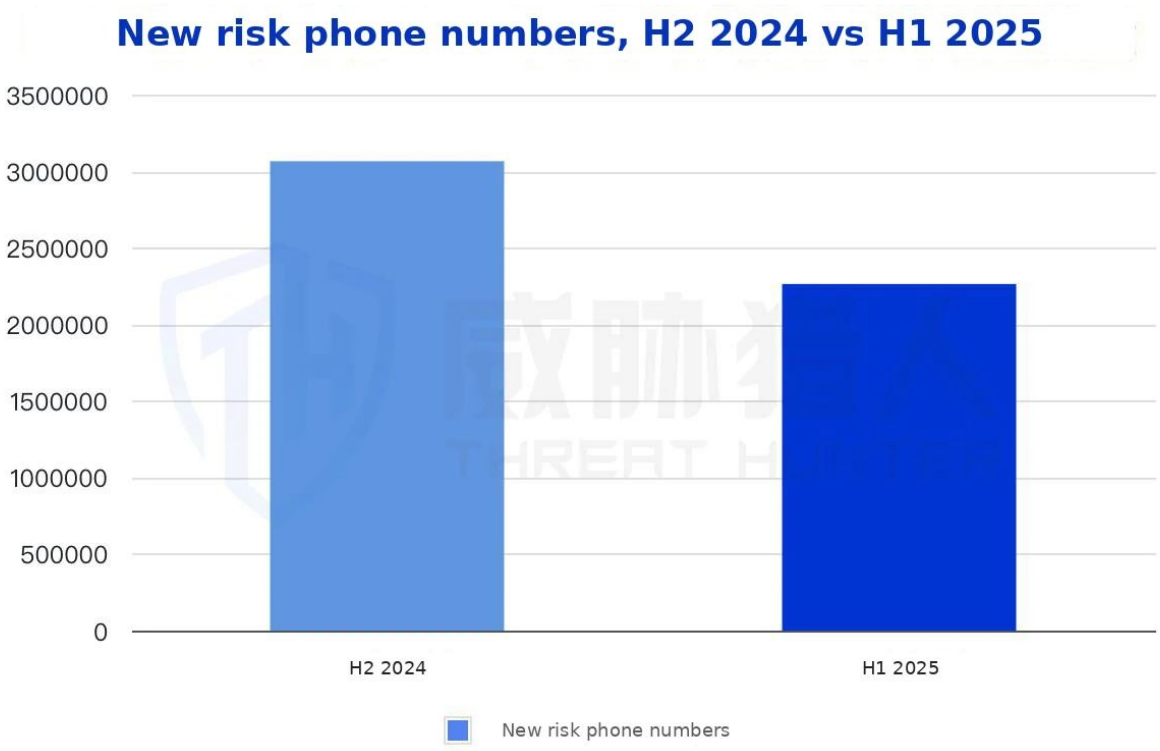
Analysis of attack resources used by threat actors in the first half of 2025

1. Analysis of attack resources used by threat actors in the first half of 2025

1.1 Analysis of malicious mobile-number resources in the first half of 2025

1.1.1 The total number of new domestic risky phone numbers in the first half of 2025 was lower than that in the second half of 2024

In the first half of 2025, Threat Hunter found that the total number of new domestic risky phone numbers showed a downward trend, with the number of new ones reaching 2.26 million, a 26.16% decrease from the second half of 2024.



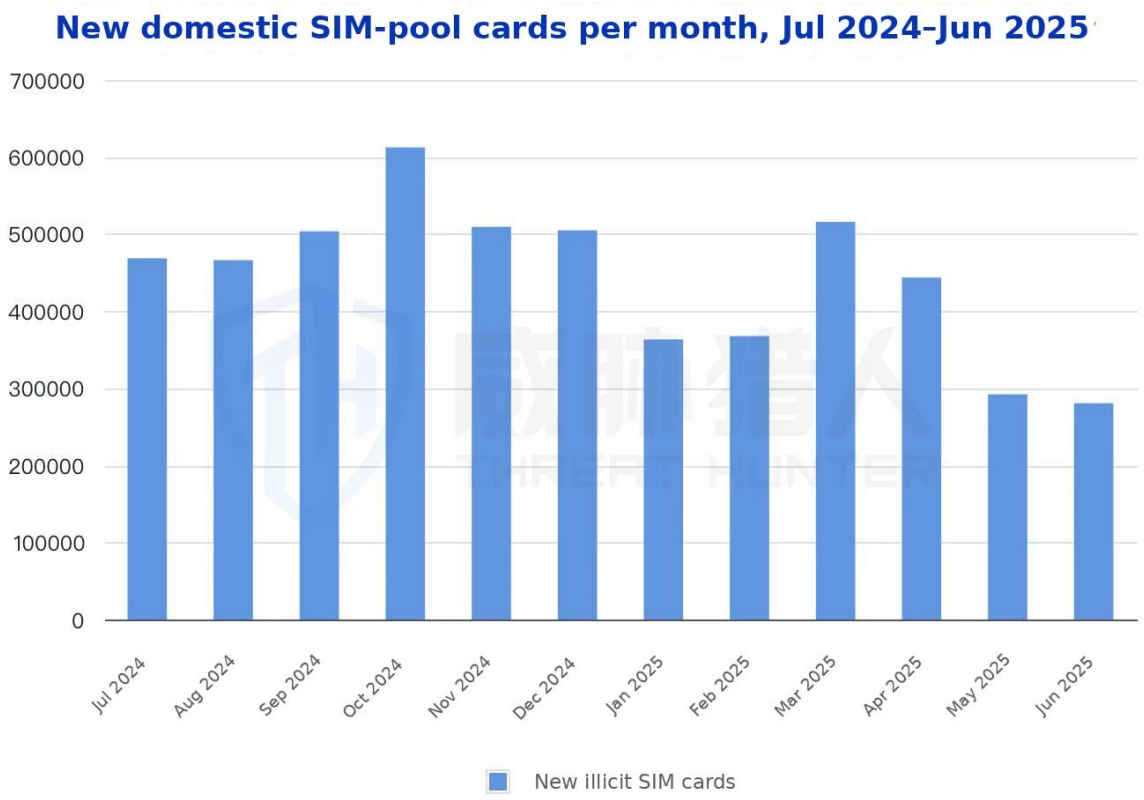
New risk phone numbers, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 6. Original figure with Chinese text replaced by English.

1.1.2 Change trend of SIM pool cards resources in the first half of 2025

(1) The number of domestic SIM pool cards in the first half of 2025 decreased by 26.16% compared with the second half of 2024. According to data from the Threat Hunter intelligence platform, 2.26 million new SIM pool cards were captured in the first half of 2025, a 26.16% decrease from the second half of 2024.

SIM pool cards: refers to the mobile phone SIM card in the "SIM pool" device of threat actors, which can be batch-controlled to achieve functions such as sending and receiving text messages. It is often used by criminals for illegal activities.



New domestic SIM-pool cards per month, Jul 2024–Jun 2025

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

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

1. In January and February, due to the slowdown of transactions by threat actors during the Lunar New Year, the activity of downstream perpetrators decreased, resulting in a significant decline in supply.

The steady upward trend has been restored; this phenomenon is the annual cyclical law of the cybercrime ecosystem.

2. In the first half of 2025, the number of SIM pool cards showed a downward trend from May to June, mainly due to the contraction of the supply of upstream illicit SIM-card dealers.

Since the end of April 2025, card supply sources have been subject to regulatory crackdowns, and card vendors have stopped supplying cards, resulting in a decline in the overall data volume in the first half of 2025. See 2.1.3 for details.

(2) The three provinces with the most new SIM pool cards in the first half of 2025 are: Shanghai, Chongqing, and Guangdong. Threat Hunter conducted a statistical analysis of the new domestic SIM pool cards in the first half of 2025 and found that Shanghai, Chongqing, and Guangdong (including municipalities directly under the Central Government) are the three provinces with the most SIM pool cards.



Top 10 provinces for SIM-pool cards, H1 2025

Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.

Province	Rank by new SIM-pool cards, H1 2025	Year-on-year trend
Shanghai	1st	No change
Chongqing	2nd	Up 8
Guangdong	3rd	Up 3
Hunan	4th	New entry
Shandong	5th	Down 1
Hubei	6th	Up 2
Liaoning	7th	Down 4
Fujian	8th	Up 1
Zhejiang	9th	New entry
Jiangsu	10th	Down 3

Province ranking for new SIM-pool cards, H1 2025

Source: Threat Hunter original report, page 8. Table re-typeset in English from the original.

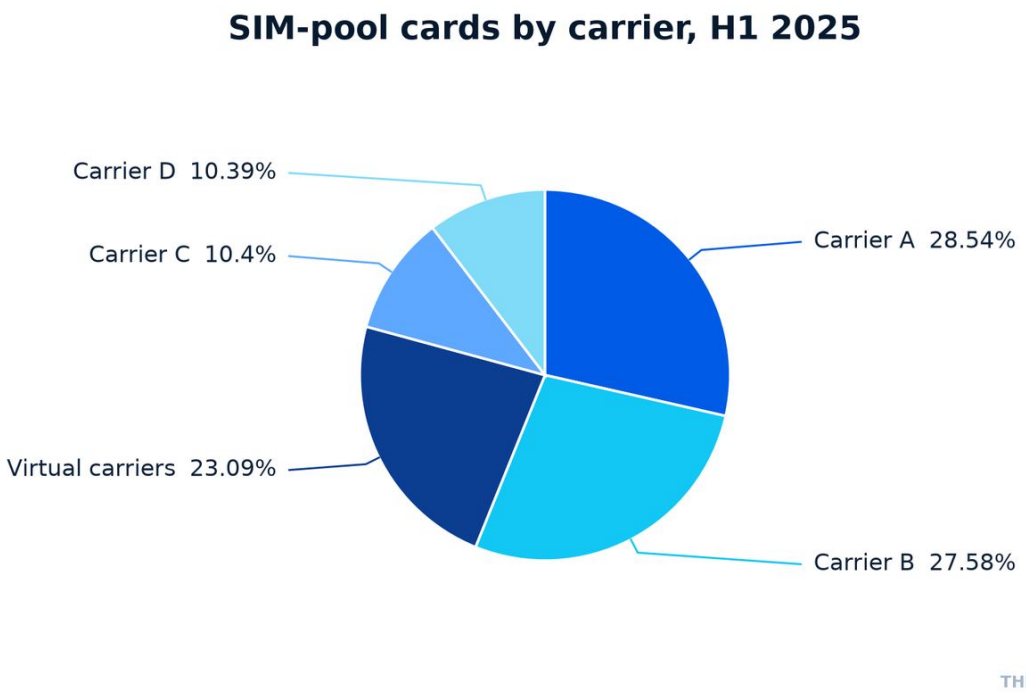
(3) The three cities with the most new SIM pool cards in the first half of 2025 are: Shanghai, Chongqing, and Changsha. Threat Hunter conducted a statistical analysis of the new domestic SIM pool cards in the first half of 2025 and found that Shanghai, Chongqing, and Changsha are the three cities with the most SIM pool cards.



Top 10 cities for SIM-pool cards, H1 2025

Source: Threat Hunter original report, page 8. Original figure with Chinese text replaced by English.

(4) Among the new SIM pool cards captured in the first half of 2025, 66.51% were owned by the three major domestic operators. Threat Hunter intelligence data shows that 2.26 million new SIM pool cards were detected in the first half of 2025, of which 66.51% were owned by the three major domestic operators.



SIM-pool cards by carrier, H1 2025

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

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

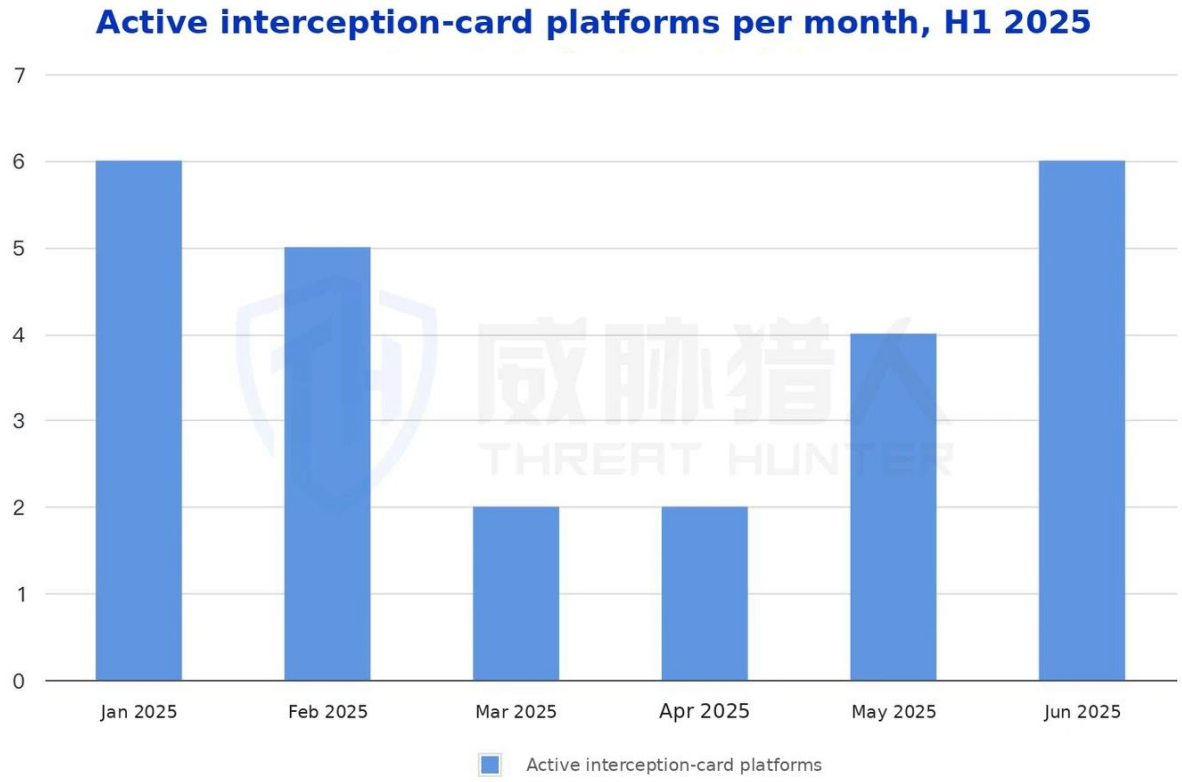
Interception card: threat actors use virus Trojans to hijack the permission to send and receive text messages on mobile phones, thereby controlling the phone number. The owner of the number is a normal user.

(1) Domestic interception cards in the first half of 2025 decreased by 83.51% compared with the second half of 2024. According to data from the Threat Hunter intelligence platform, in the first half of 2025, Threat Hunter captured 155,000 new interception cards, a decrease of 83.51% compared with the second half of 2024. Further analysis of the supply of cybercrime ecosystem interception cards shows:

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, of the six originally active card interception platforms (card supply channels), only two remained in a semi-stagnant state;
- In late May, monitoring found that 4 new card supply channels were added. The 2 card supply channels that were previously in a semi-stagnant state became active after threat actors changed their domain names and verification-code reception tools.

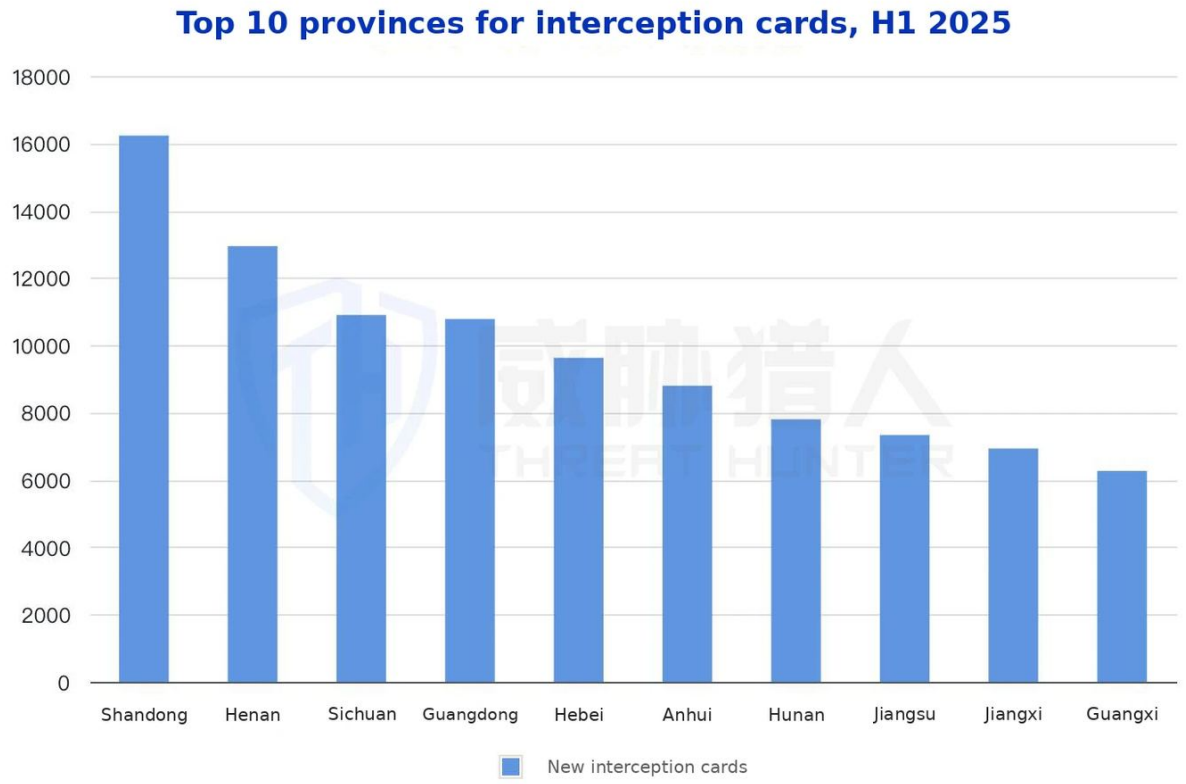
As of the first half of 2025, there are currently 6 active card supply channels, but the magnitude and quality of number supply on the above platforms are unstable and fluctuating.



Active interception-card platforms per month, H1 2025

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

(2) The three provinces with the most interception cards in the first half of 2025 are: Shandong, Henan, and Sichuan. A statistical analysis of domestic interception cards captured in the first half of 2025 found that Shandong, Henan, and Sichuan are the three provinces with the most interception cards.



Top 10 provinces for interception cards, H1 2025

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

Province	Rank by new interception cards, H1 2025	Year-on-year trend
Shandong	1st	Up 1
Henan	2nd	Up 2
Sichuan	3rd	No change
Guangdong	4th	Down 3
Hebei	5th	Up 3
Anhui	6th	No change
Hunan	7th	Down 2
Jiangsu	8th	Up 1
Jiangxi	9th	Up 1
Guangxi	10th	Down 1

Province ranking for new interception cards, H1 2025

Source: Threat Hunter original report, page 11. Table re-typeset in English from the original.

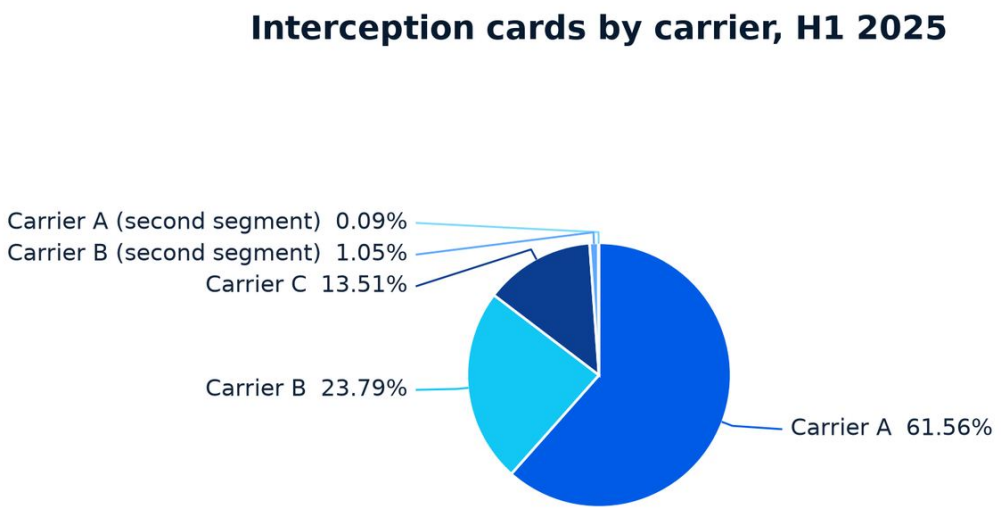
(3) The three cities with the most new interception cards in the first half of 2025 are: Chongqing, Heze, and Linyi. Threat Hunter conducted a statistical analysis of the new domestic interception cards in the first half of 2025 and found that Chongqing, Heze, and Linyi are the three cities with the most interception cards.



Top 10 cities for interception cards, H1 2025

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

(4) Among the new interception cards captured in the first half of 2025, 98.86% belong to the three major domestic operators. In the first half of 2025, the Threat Hunter intelligence operation platform captured 155,000 new interception cards, and the interception cards belonging to the three major domestic operators accounted for 98.86%.



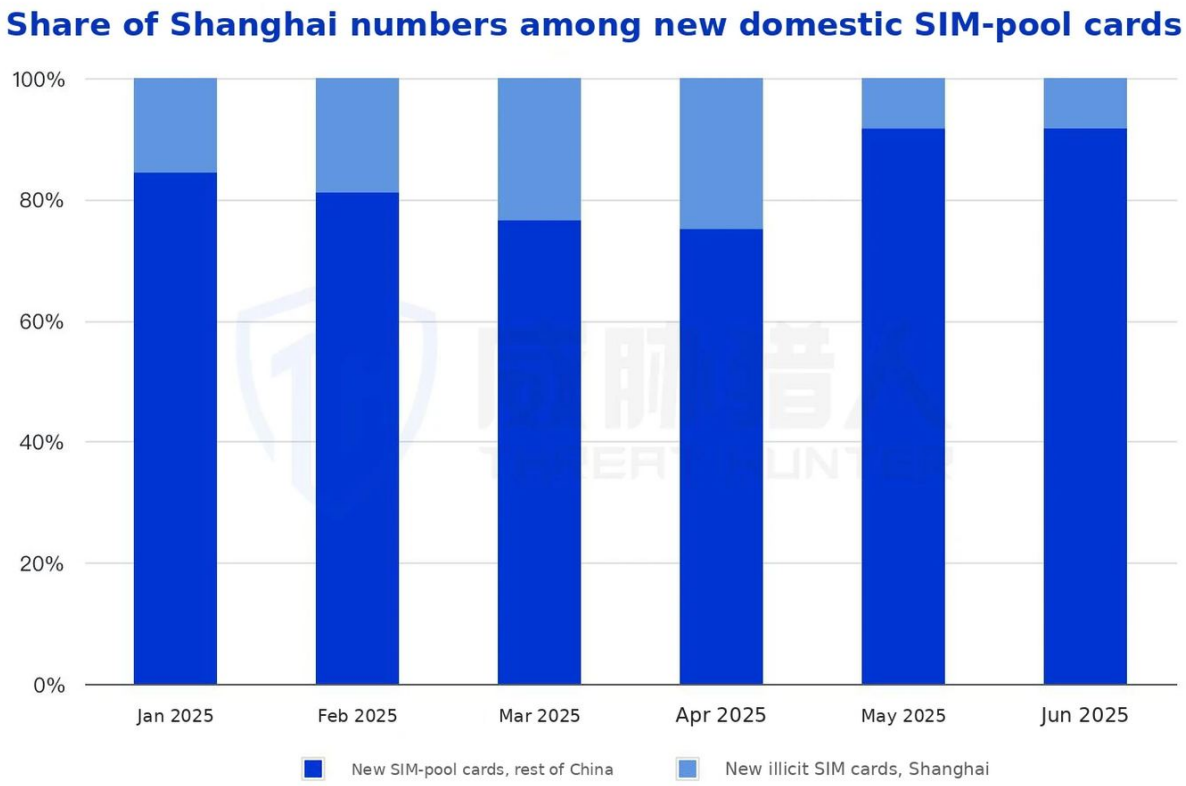
Interception cards by carrier, H1 2025

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

1.1.4 Supervision to crack down on card supply sources: Fluctuations in upstream card supply sources affect the entire chain of threat actors conducting malicious activity acts

(1) Supervision of Shanghai card dealers, the leading card supply source, has been severely affected. Domestic SIM pool cards have dropped sharply in the first half of the year. According to Threat Hunter monitoring data analysis, Shanghai card dealers have become the leading card supply source for SIM pool cards in recent years. Since 2024, SIM pool cards dealers that provide numbers belonging to Shanghai have continued to be highly active. The new Shanghai SIM pool cards in 2024 accounted for 11.77% of the total new additions throughout the year;

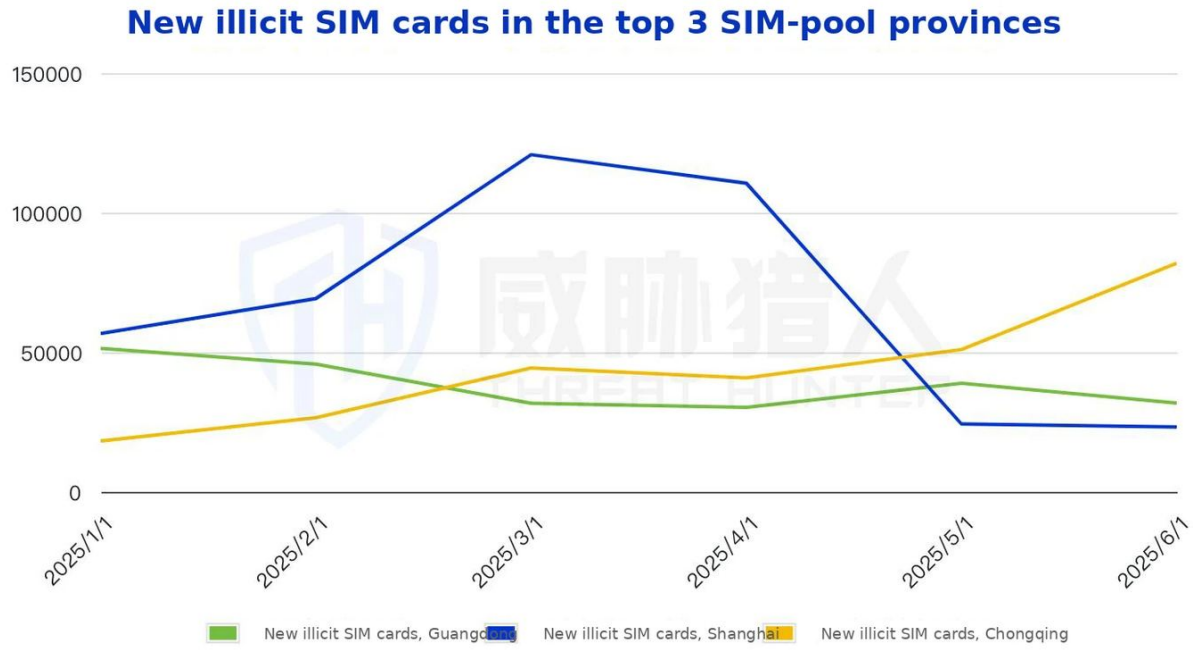
The upward trend will still remain from January to April 2025, reaching a peak in April. 24.93% of the new domestic SIM pool cards that month came from Shanghai. In the regulatory crackdown in May 2025, Shanghai card merchants were the first to be hit. The proportion of new card sources in the country in May quickly fell to an average monthly share of 8.29%. This is also the main reason for the sharp decline in domestic SIM pool cards in the first half of the year.



Share of Shanghai numbers among new domestic SIM-pool cards

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

The number of new illicit SIM cards in Shanghai dropped sharply during the regulatory crackdown, leading to a decline in the overall number of SIM pool cards nationwide. As can be seen in the figure below, the number of new illicit SIM cards in Shanghai dropped sharply in May and was lower than illicit SIM cards in Guangdong and Chongqing for the first time this year. This pattern is still maintained.



New illicit SIM cards in the top 3 SIM-pool provinces

Source: Threat Hunter original report, page 13. Original figure with Chinese text replaced by English.

The timeline for regulatory crackdowns on the illicit SIM-card supply chain in the first half of 2025 is as follows. Upstream card dealers in Shanghai and Chongqing have been hit one after another.



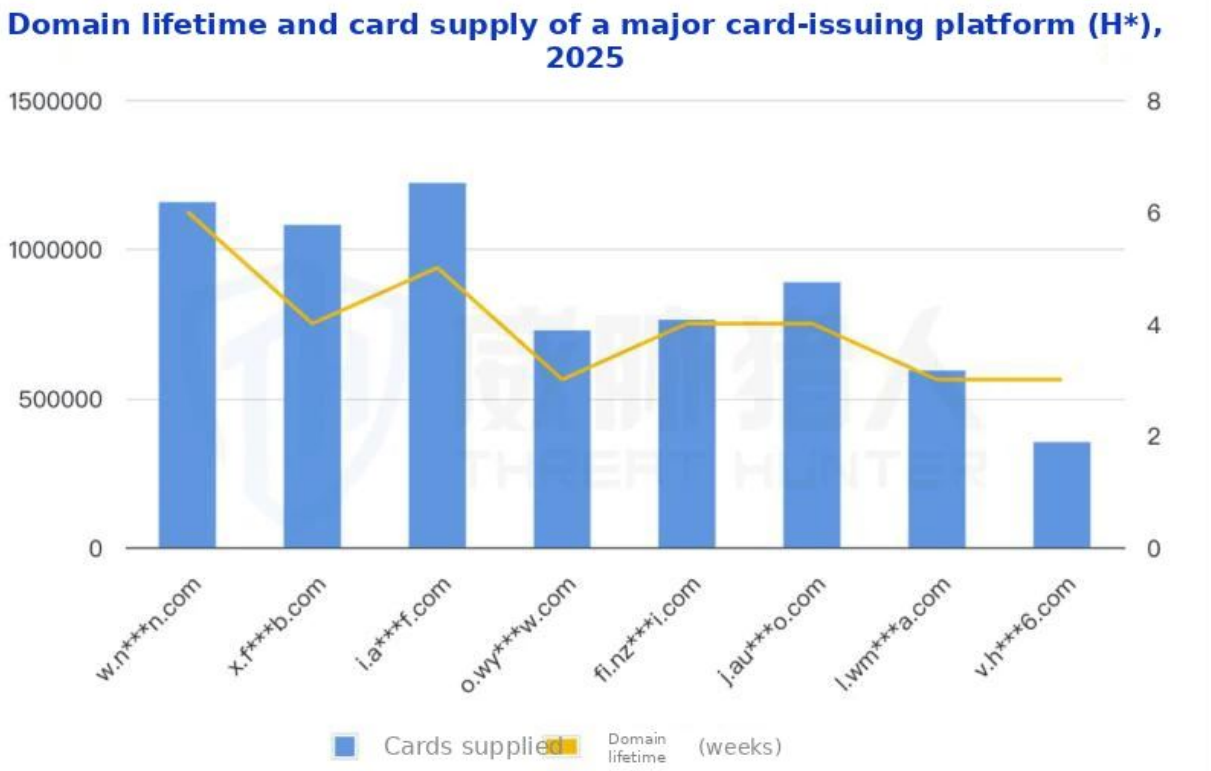
Enforcement against the illicit SIM card supply chain, H1 2025

Source: Threat Hunter original report, page 13. Original figure with Chinese text replaced by English.

(2) Fluctuations in the upstream card supply source are transmitted to the midstream link of threat actors. As the card issuance platform and SMS verification-code receiving service of the midstream link of threat actors, frequent relocations, shutdowns for maintenance, or cancellations occurred from May to June 2025, which further blocked the downstream illicit SIM-card supply chain.

Taking Group A, a mainstream card-issuing platform group of threat actors that has been monitored for a long time, as an example, the domain name it used frequently changed more than

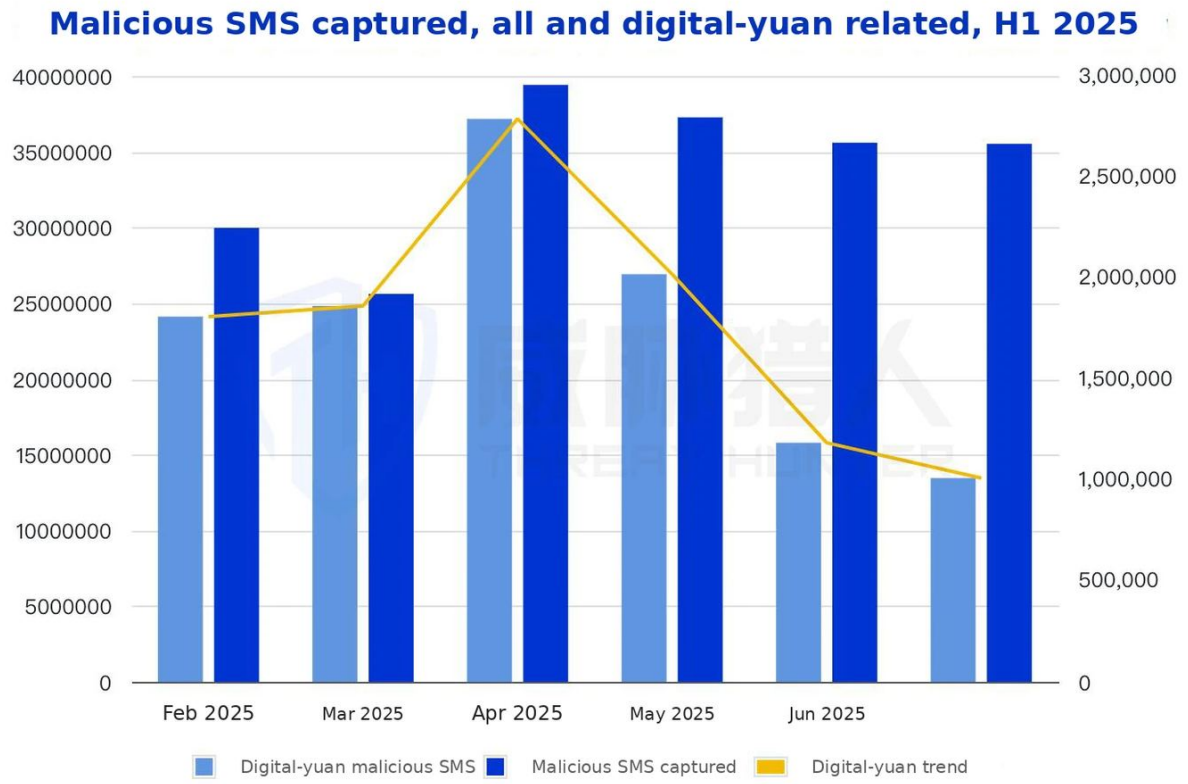
8 times in a short period of time, and the domain name survival period was shortened to 15 to 21 days. The number of cards supplied also showed a downward trend, from 1.15 million to 350,000 at the end of June.



Domain lifetime and card supply of a major card-issuing platform, 2025

Source: Threat Hunter original report, page 14. Original figure with Chinese text replaced by English.

As one of the main malicious activity channels of cybercrime ecosystem, the group verification-code reception channel has observed a downward trend in captured verification-code reception text message records - the number of captured text message records from May to June 2025 dropped by 5.56 million compared with March to April of the same year, a month-on-month decrease of approximately 7.26%. Taking the "Digital RMB" code reception, a key target of threat actors' malicious activity, as an example, the changing trend in the number of malicious activity text messages is a typical example of this impact.

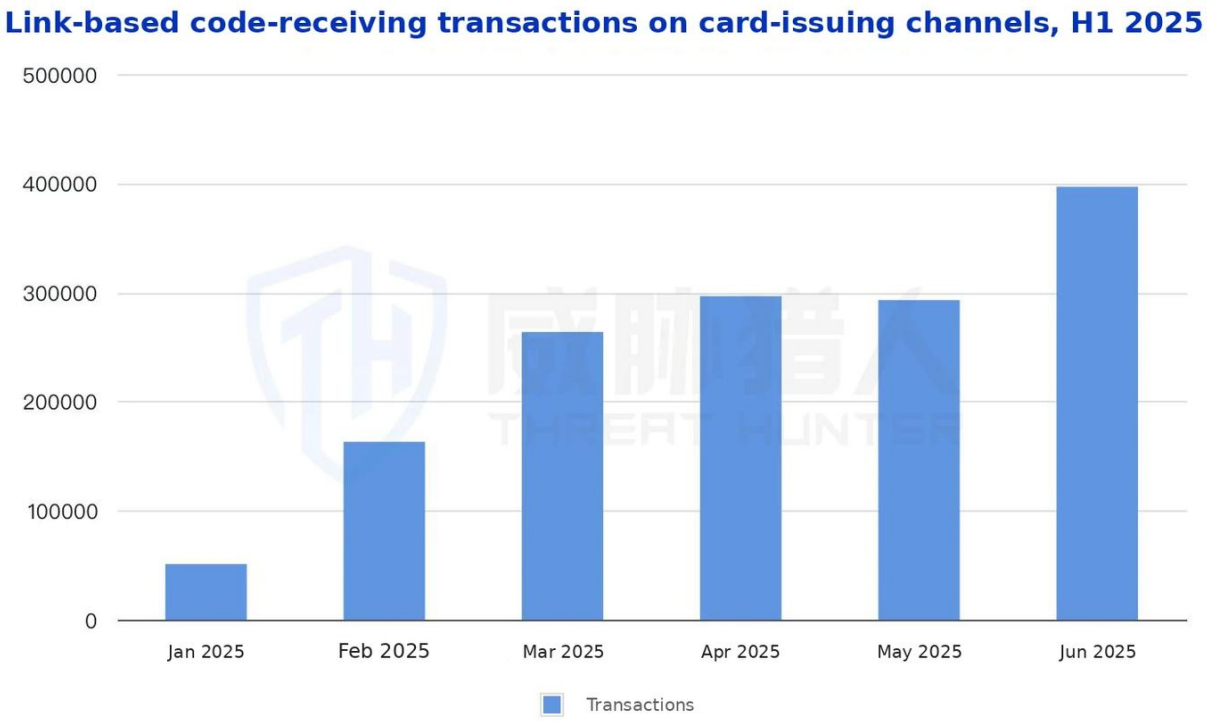


Malicious SMS captured, all and digital-yuan related, H1 2025

Source: Threat Hunter original report, page 14. Original figure with Chinese text replaced by English.

1.1.5 Link connection code: The rise of new code connection method cybercrime ecosystem

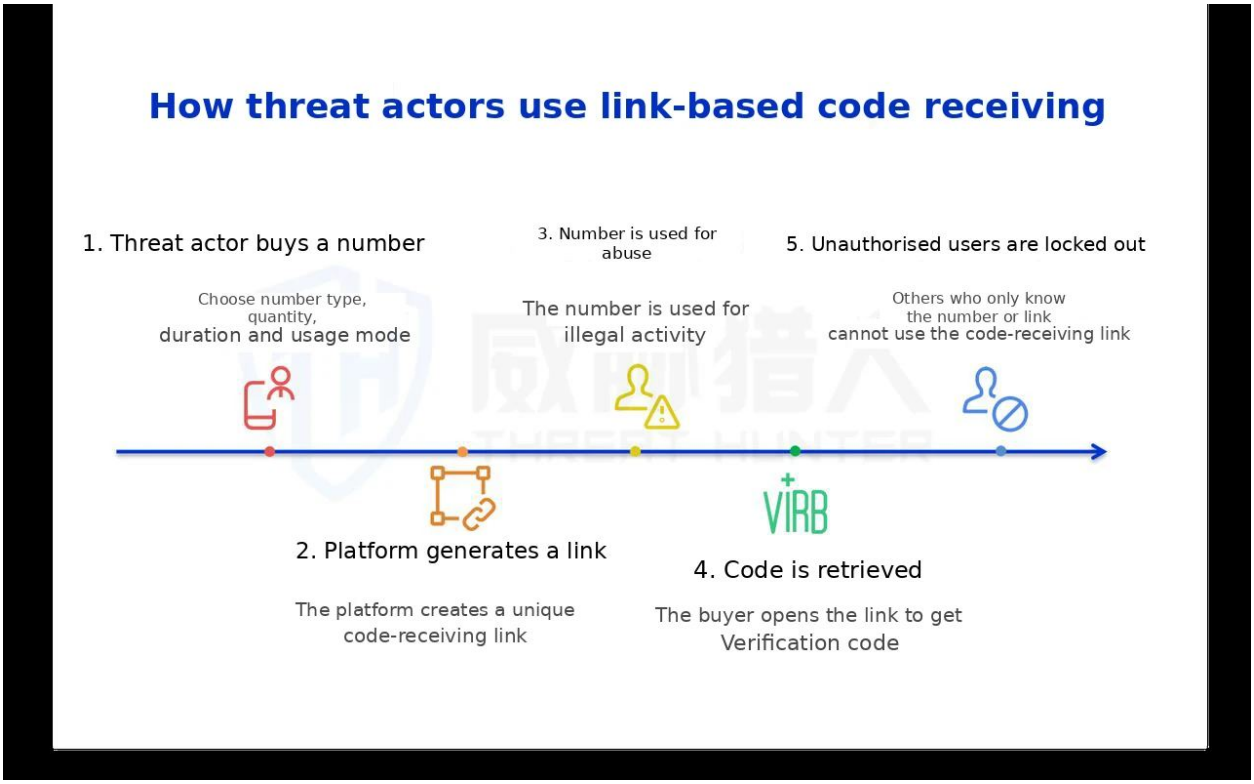
In the first half of 2025, a new code-receiving method called "link connection code" emerged in card issuance channels. threat actors are currently mainly used for code-receiving services in North America and Hong Kong, China. As of June, more than 1.46 million transaction records have been monitored, involving 140 domain names related to link codes, and approximately 8 independent domain names of distributors are added every week.



Link-based code-receiving transactions on card-issuing channels, H1 2025

Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

The distinguishing feature of "link access code" is the "one-to-one" model. Specifically, after the downstream threat actors purchase a project, they will be assigned a dedicated code access phone number and receive the SMS verification code for the project through an exclusive link. Each malicious phone number only serves a single project, and each link only displays the verification code of the corresponding project. The link code process is as follows:



How threat actors use link-based code receiving

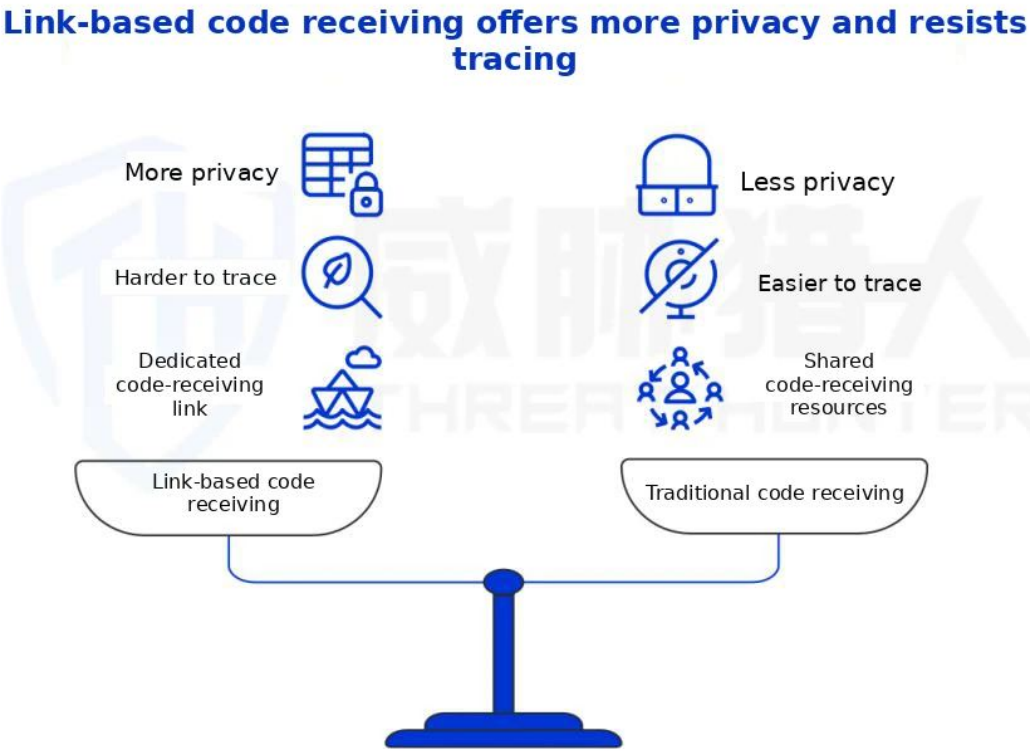
Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

Compared with the traditional code connection method, the link connection code has higher privacy and anti-tracing capabilities, and it effectively avoids the three common types of risks in traditional code connection:

The first is that the results of account maintenance are stolen - traditional code connection usually shares the connection code or transcoding room, resulting in the clear text or mask of the number being read by other threat actors, and the malicious accounts that have been developed are hijacked;

The second is the problem of resource conflict - the same number is reused in multiple threat actors projects, causing data pollution and requiring additional filtering processes.

The third is regulatory traceability and tracking - 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 threat-actor platform.



Link-based versus traditional code receiving

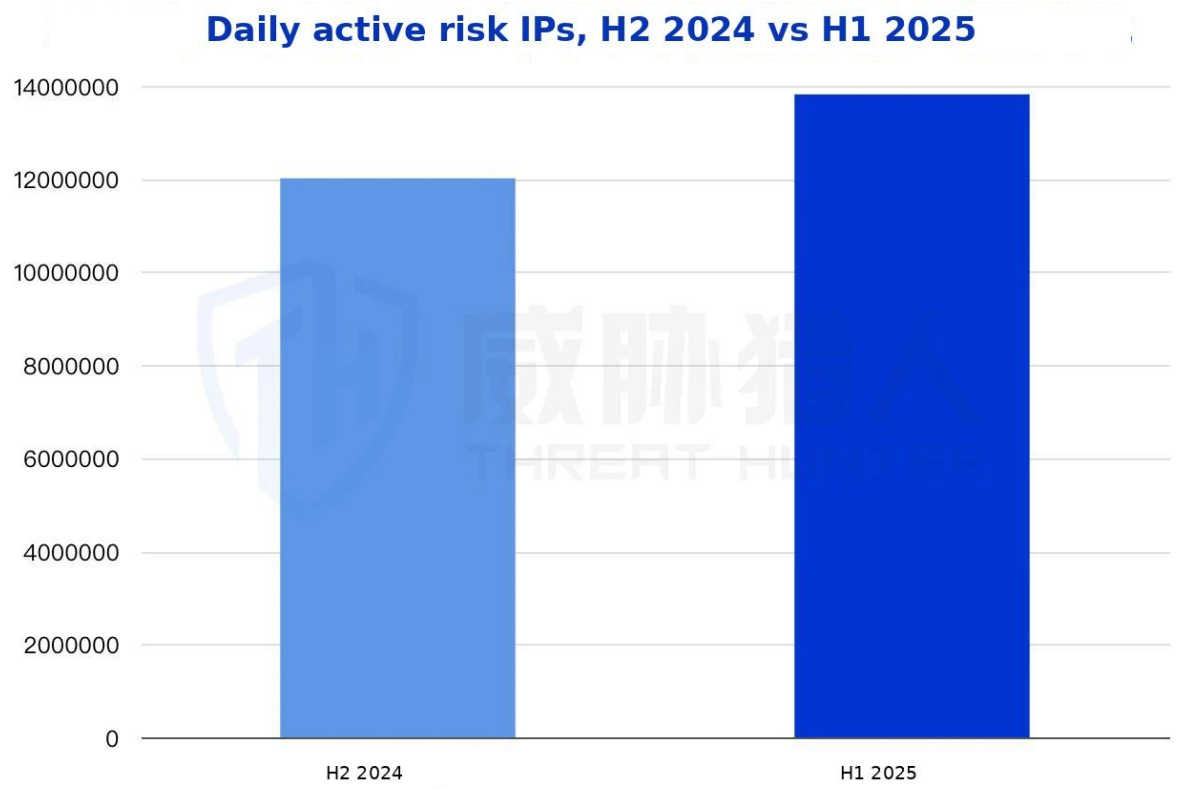
Source: Threat Hunter original report, page 16. Original figure with Chinese text replaced by English.

1.2 Analysis of malicious IPs resources in the first half of 2025

1.2.1 The total daily average active risk IP in the first half of 2025 increased compared with the second half of 2024

Reported share: 15.02%

In the first half of 2025, Threat Hunter monitoring found that the average daily number of active risk IPs continued to rise, with the number of risk IPs reaching 13.82 million, an increase of 15.02% from the second half of 2024.

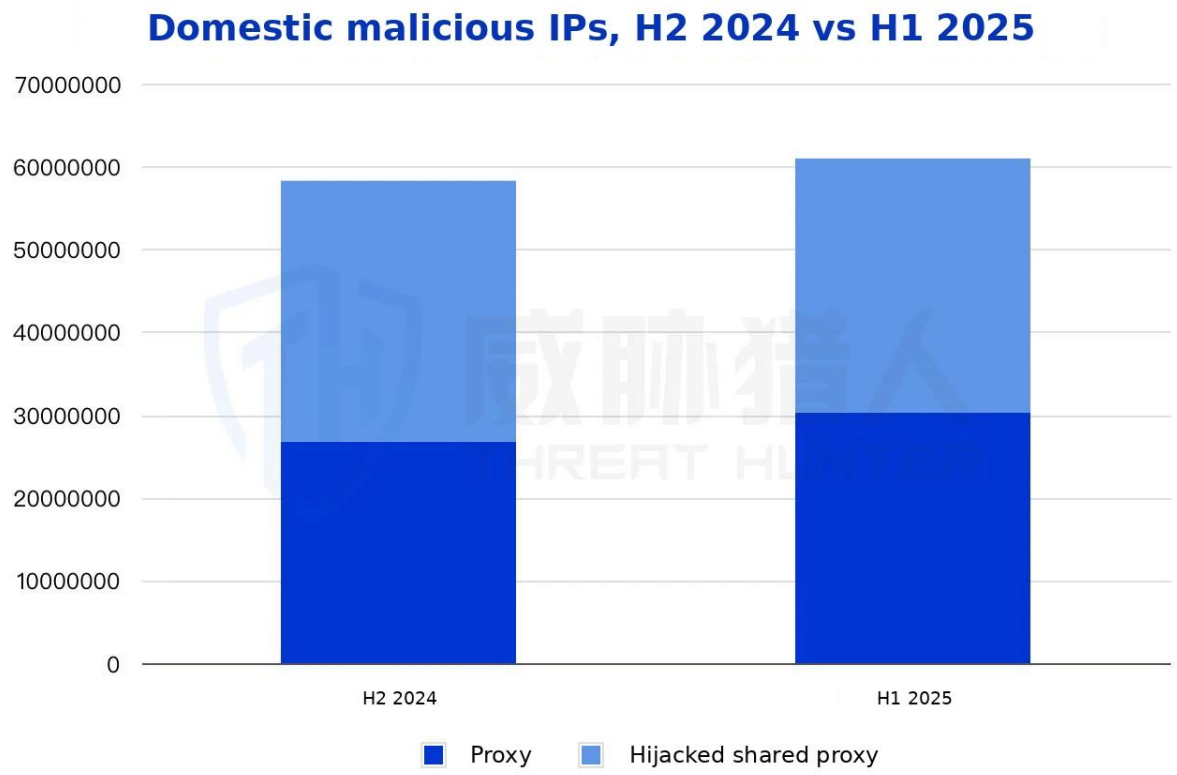


Daily active risk IPs, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 17. Original figure with Chinese text replaced by English.

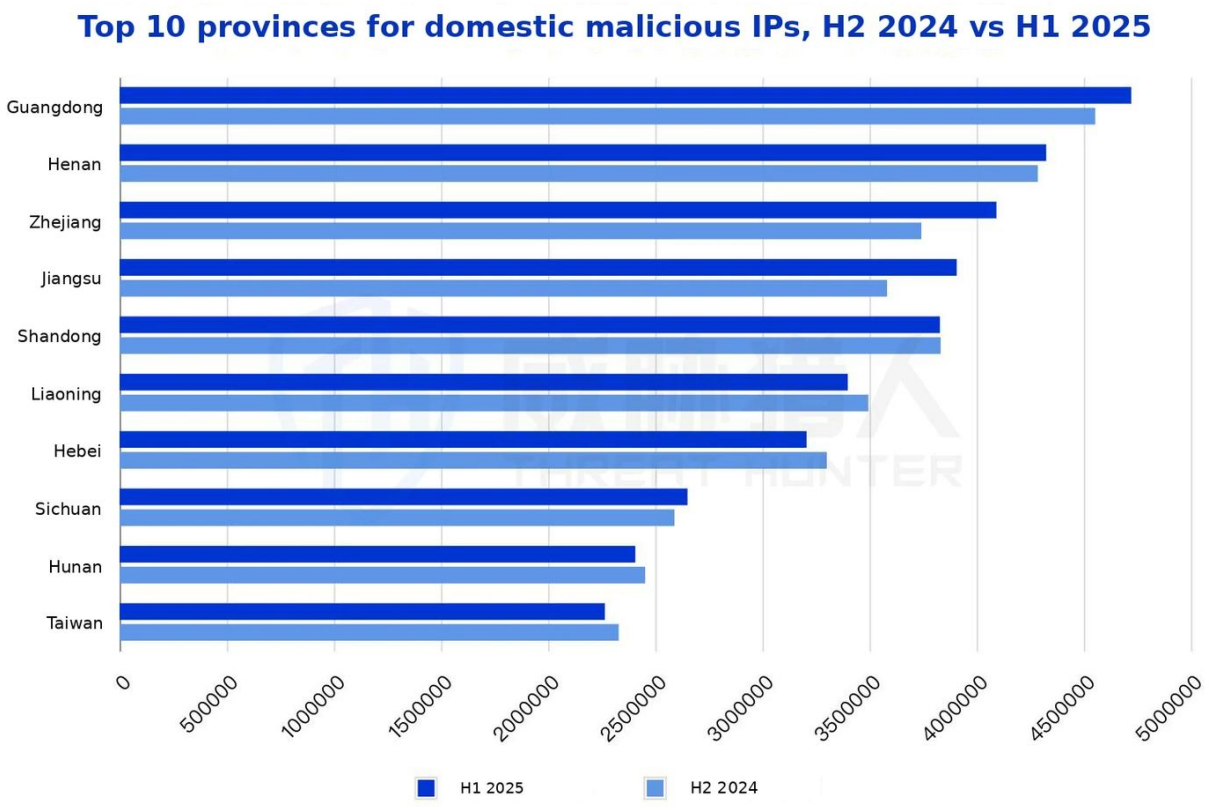
1.2.2 Analysis of domestic malicious IPs resources in the first half of 2025

(1) In the first half of 2025, there were 60.96 million domestic malicious IPs, an increase of 4.61% from the second half of 2024. (2) The provinces where domestic malicious IPs belong to in the first half of 2025 are top 3: Guangdong, Henan, and Zhejiang. Threat Hunter intelligence data statistics show that domestic active malicious IPs in the first half of 2025 The provinces (including municipalities directly under the Central Government) are mainly concentrated in Guangdong Province, Henan Province and Zhejiang Province.



Domestic malicious IPs, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 17. Original figure with Chinese text replaced by English.

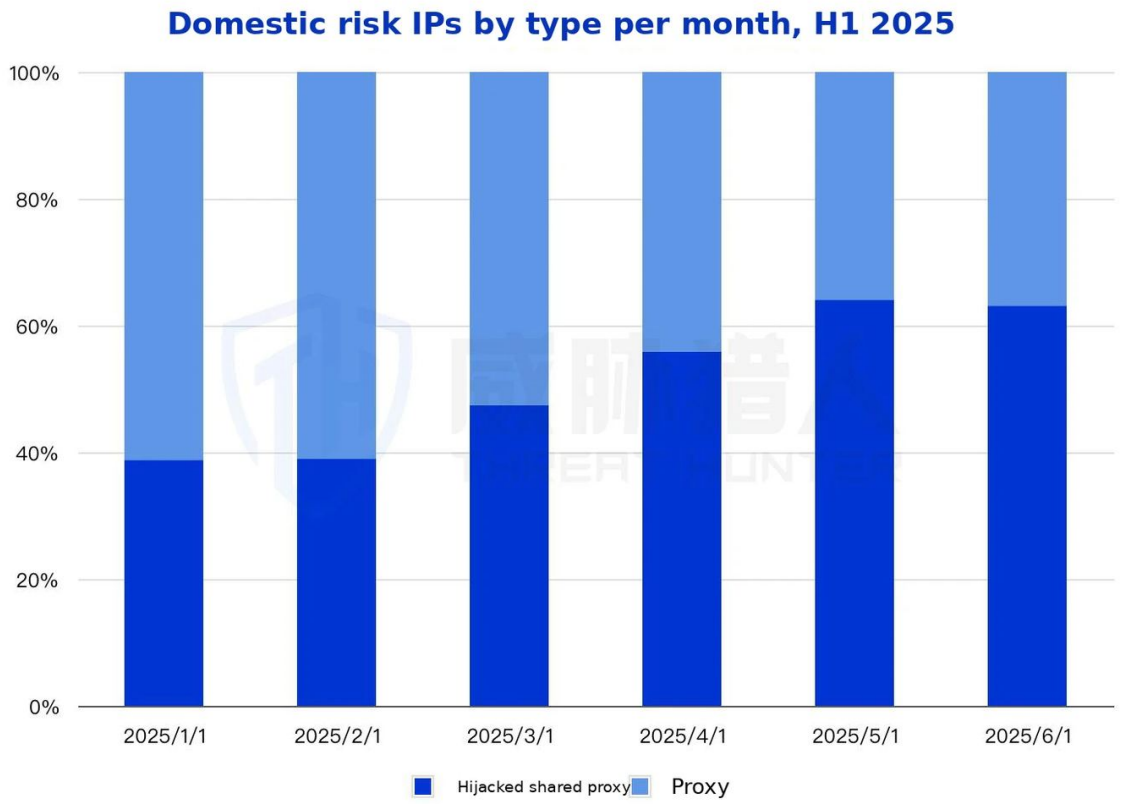


Top 10 provinces for domestic malicious IPs, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

(3) In the first half of 2025, "hijacking shared proxy" IP attacks accounted for 50.37% of the total. IP resource supply is more stable and billing models are more diverse. Threat Hunter continues to monitor the proxy IP platform. Judging from the data captured in the first half of 2025, the average daily number of "hijacked shared proxy" IPs reached 1.2 million. At the same time, judging from the proportion of domestic risk IP types, the proportion of threat actors using hijacked shared IP attacks increased from January The increase from 38.80% to 63.10% in June shows that threat actors have become more rampant in maliciously using normal user IPs by implanting Trojans.

Since this type of IP is used by normal users most of the time, such as clicking, recharging, browsing, etc., it will be hijacked and shared by threat actors for a small amount of time, causing short-term malicious activity behaviors. Therefore, the platform may identify the user as a normal user, and then ignore his short-term malicious activity behaviors, giving threat actors an opportunity to take advantage of.



Domestic risk IPs by type per month, H1 2025

Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

From the rise of hijacking shared agents to stability, in order to meet the needs of threat actors for multiple types of attacks, the charging model has evolved from the previous single IP-based charging model to a charging model adapted to different attack scenarios, and the product has gradually matured.

Proxy IP type	H2 2024	H1 2025
Proxy	Billed per IP Billed by traffic Billed by concurrency Unlimited IP pool	
Hijacked shared proxy	Billed per IP	Billed per IP Billed by traffic Billed by concurrency

Proxy IP billing models, H2 2024 vs H1 2025

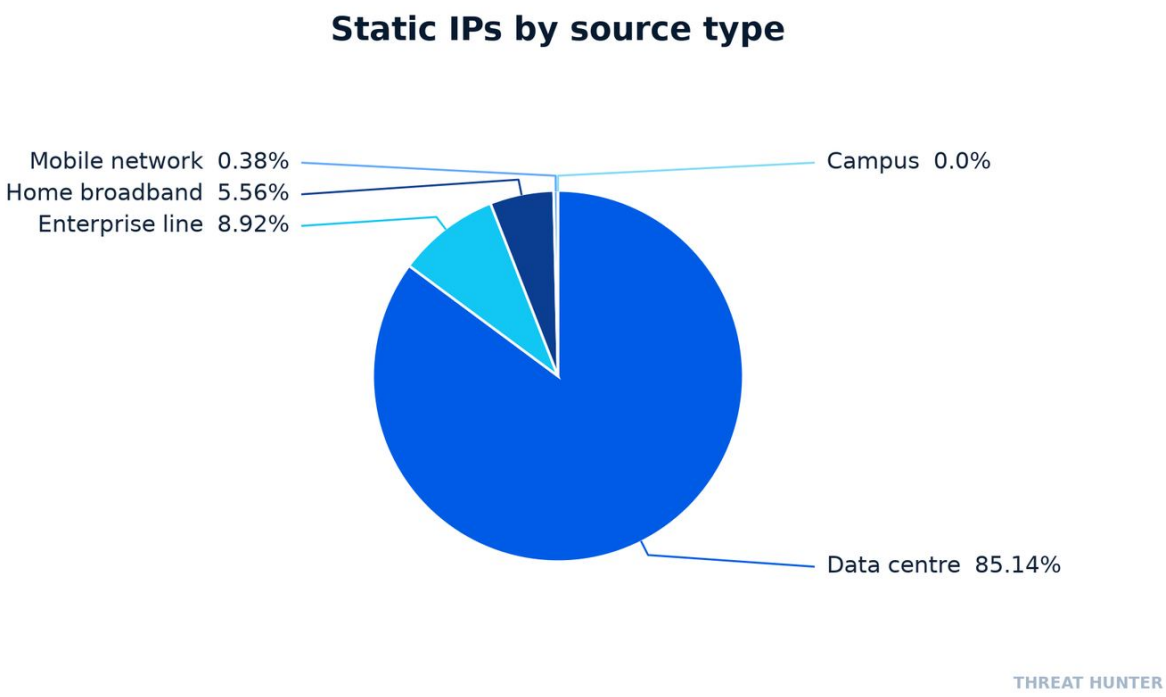
Source: Threat Hunter original report, page 19. Original figure with Chinese text replaced by English.

(4) In the first half of 2025, static IP will still be one of the important malicious resources. Threat Hunter continues to monitor proxy IP. Based on the recent resources used by threat actors, we found that some threat actors will still use static long-lasting proxy IP to conduct malicious activity.

Judging from the capture data in the first half of 2025, the number of “long-lasting static proxy” IP captures reached 1.4 million.

Different from the short-lived dynamic proxy IPs monitored by Threat Hunter in the past, this type of long-lived static IP address remains unchanged for a long time. Its characteristics are relatively fixed and obvious. It is easy to be identified by websites and network security systems and associated with malicious activities. Once the IP is detected and banned by the platform, it cannot continue to be used, making it difficult for threat actors to continue their attacks. However, in some malicious activity scenarios that do not require frequent IP changes, threat actors usually use static IPs, mainly used in the following scenarios:

At the same time, we found that the source type of this type of long-term static proxy IP is mainly from data centers, accounting for 85.14%, while the short-term dynamic proxy IP mainly comes from home broadband.



Static IPs by source type

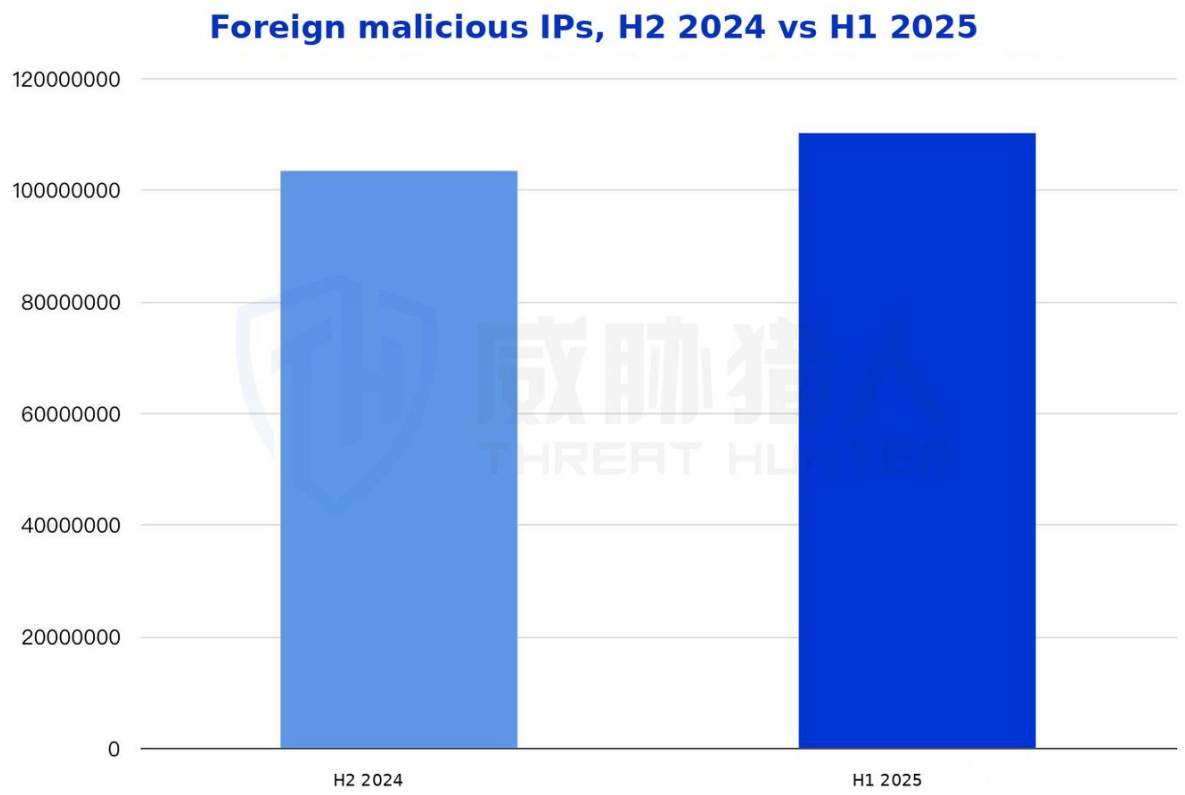
Source: Threat Hunter original report, page 20. Redrawn in English from the original figure.

Social platform account maintenance: Use fake accounts registered with long-lasting static IPs to maintain accounts, and then send a large number of spam private messages, comments, group advertisements, etc. to conduct malicious marketing and promotion, interfere with the social experience of normal users, and divert traffic to other illegal platforms or websites.

Low-frequency crawler: A crawler that uses long-lasting static IP to imitate ordinary users for data crawling. It is closer to ordinary users in terms of User-agent, frequency, timeline and other characteristics, and then crawls information on social media, news websites, forums and other platforms.

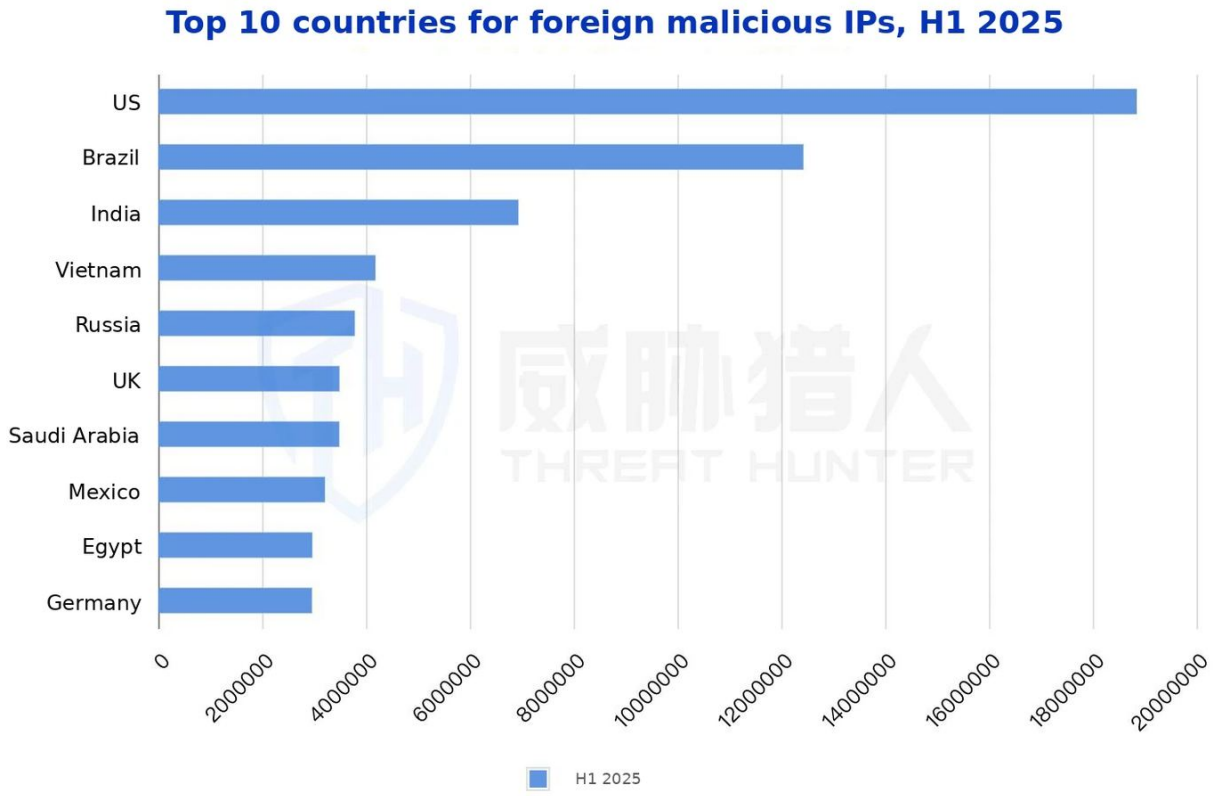
1.2.3 Analysis of foreign malicious IPs resources in the first half of 2025

(1) In the first half of 2025, 110 million foreign malicious IPs were captured, an increase of 6.56% from the second half of 2024. (2) The top 3 countries of foreign malicious IPs in the first half of 2025: the United States, Brazil, and India. Threat Hunter intelligence data statistics show that the countries with active foreign malicious IPs in the first half of 2025 are mainly concentrated in the United States, Brazil, and India.



Foreign malicious IPs, H2 2024 vs H1 2025

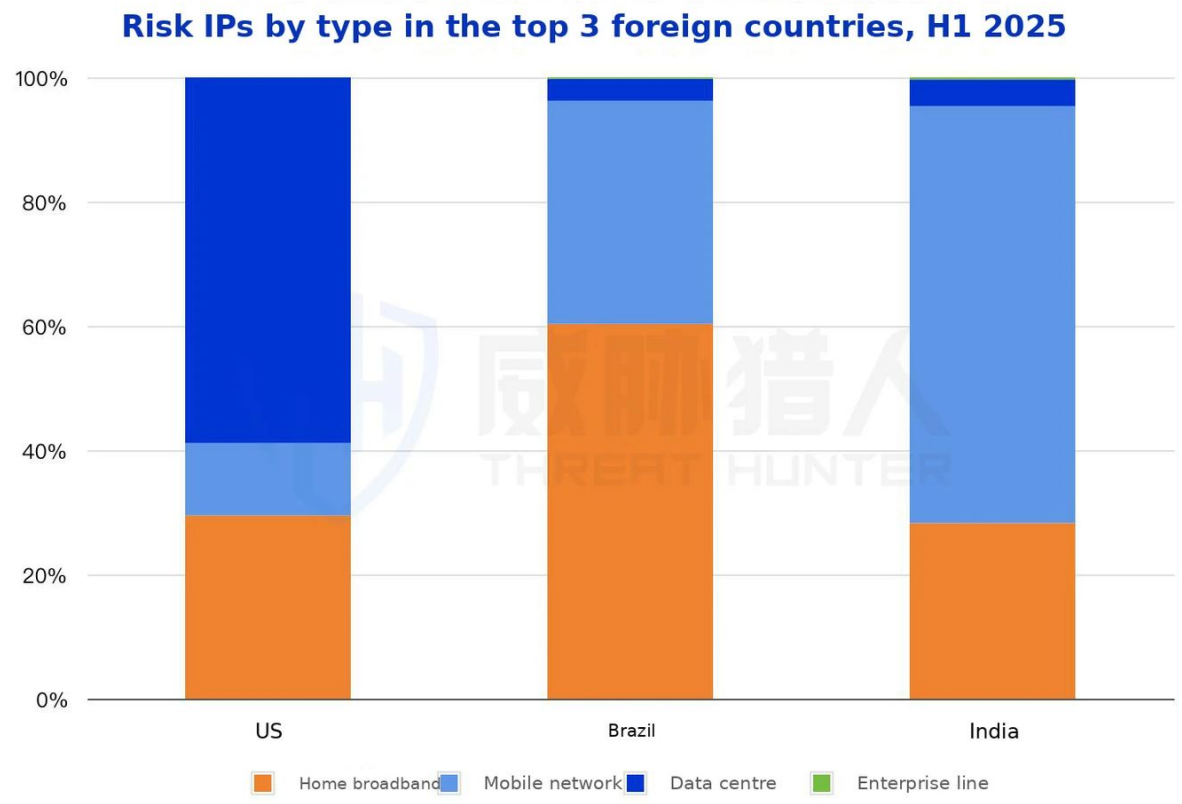
Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.



Top 10 countries for foreign malicious IPs, H1 2025

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

Threat Hunter found that the black IP malicious resources in different countries are also different. The following is the distribution of black IP types in the top 3 foreign countries.



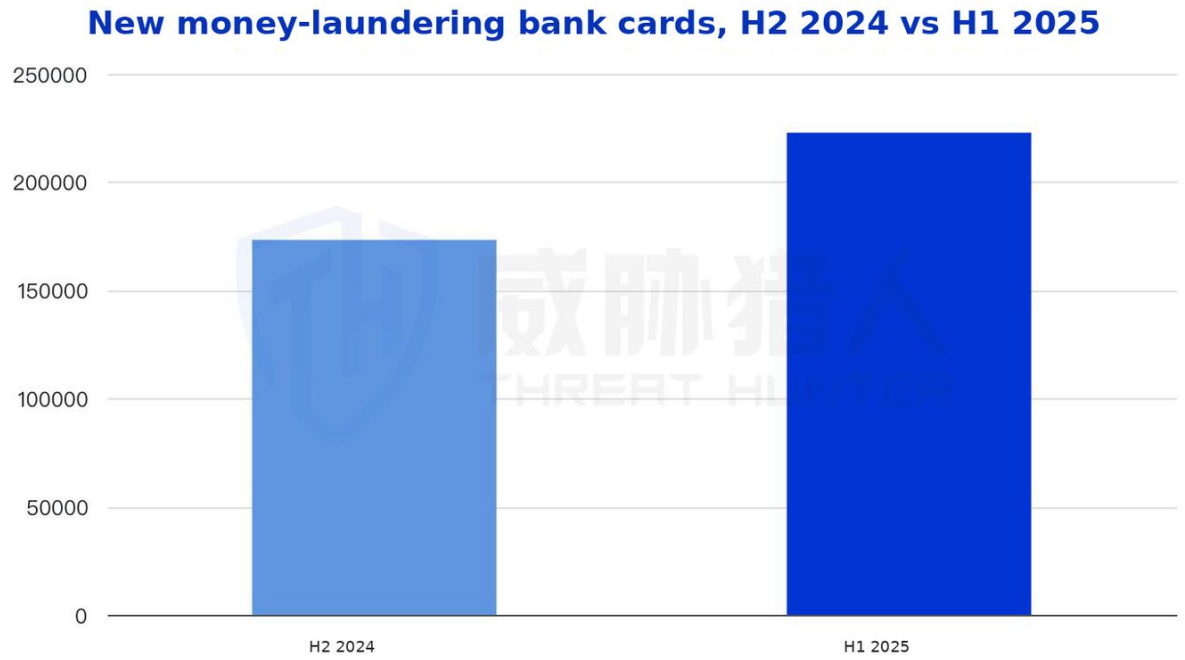
Risk IPs by type in the top 3 foreign countries, H1 2025

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

1.3 Analysis of Internet Money Laundering Resources in 2024

1.3.1 In the first half of 2025, the number of bank cards involved in money laundering increased compared with the second half of 2024.

Reported share: 28.60%



New money-laundering bank cards, H2 2024 vs H1 2025

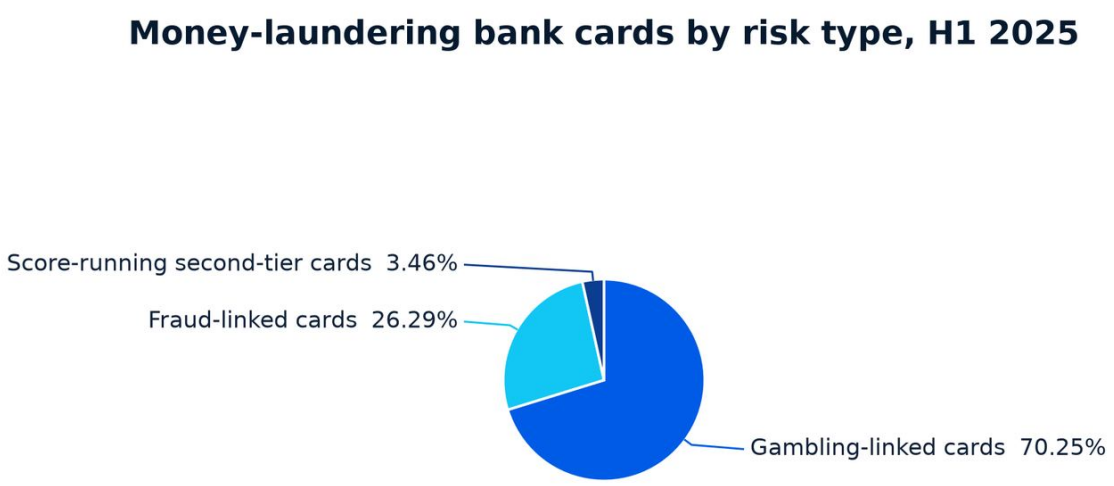
Source: Threat Hunter original report, page 22. Original figure with Chinese text replaced by English.

Gambling-related cards: Bank cards that are active in gambling platforms and are used to collect payments on gambling platforms. They are often used for recharging and collecting payments on gambling platforms. 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.

Second-level bank card for running points: a second-level bank card that is active on the running points platform and is used to collect washed funds. Threat Hunter obtains the bank card account information in the benchmark order from the benchmark platform app through an automated method.



Money-laundering bank cards by risk type, H1 2025

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

(1) Gambling-related cards accounted for 70.25% of money-laundered bank cards in the first half of 2025, a month-on-month increase of 141%. Threat Hunter analyzed 222,800 bank cards involved in money laundering captured in the first half of 2025. They were mainly divided into three types: gambling-related cards, score-level secondary cards and fraud-related cards. Among them, gambling-related cards accounted for the largest proportion, reaching 70.25%.

1 In the first half of 2025, gambling platform orders and recharges gradually became large-scale, and gambling-related cards increased by 141% month-on-month. Threat Hunter observed that the core reason for the significant growth of gambling-related bank cards increased by 141% month-on-month was the discovery and scale monitoring of the new recharge method of gambling platforms - "orders and recharges." Threat Hunter first discovered this type of gambling recharge method on a gambling platform in November 2024. This method uses the peer-to-peer recharge method between recharge gamblers and withdrawal gamblers to conduct money laundering activities.

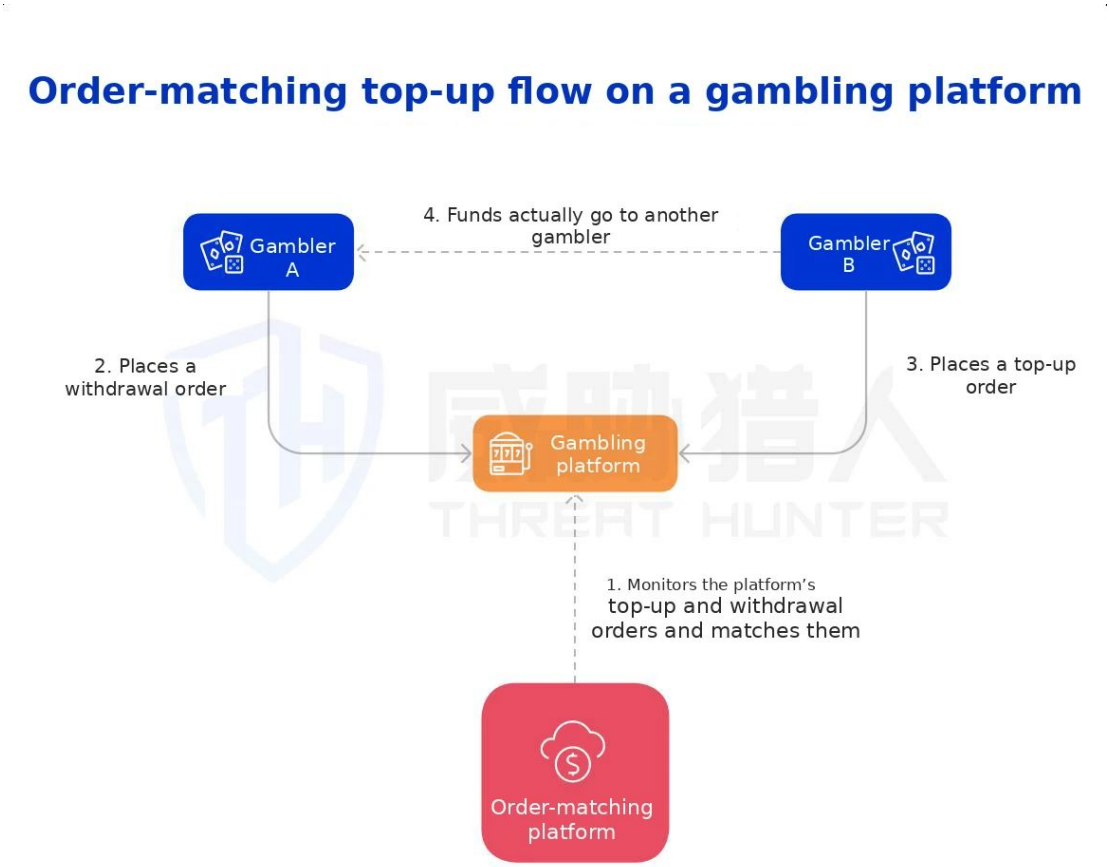
Compared with the early score-running model, "order recharge" does not require the recruitment of professional score-running personnel. It can directly use gamblers' bank cards to obtain a large number of accounts at a low cost and disperse and transfer fraudulent funds. Because the gambler's card does not have obvious money laundering characteristics in the early stage (such as small-amount high-frequency transfers), the concealment of fund transfers is greatly enhanced.



New gambling-linked cards, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 23. Original figure with Chinese text replaced by English.

The gambling platform's order recharge money laundering model is to match the withdrawal demand of gambler A with the recharge demand of gambler B in real time, guiding gambling funds to flow directly point-to-point between gamblers. Allowing gamblers to become money laundering channels without their knowledge and help complete the transfer of stolen money.



Order-matching top-up flow on a gambling platform

Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.

2 In the first half of 2025, the largest threat actor guarantee "Haowang" collapsed, money laundering gangs moved, and fraud-related card data showed a temporary decline in May. Threat Hunter observed that the number of new fraud-related cards dropped significantly in May, but quickly rebounded in June. The reason behind this is that the United States imposed sanctions on Huione Group (Huiwang) in May, which led to the collapse of its cybercrime ecosystem guarantee platform "Haowang" on an encrypted messaging app. The sanctions appeared to curb threat-actor activity, but in fact they only caused a short-term shift of money-laundering gangs. Threat actors quickly migrated to emerging guarantee platforms such as "Tudou", and money-laundering activities were not substantially affected.

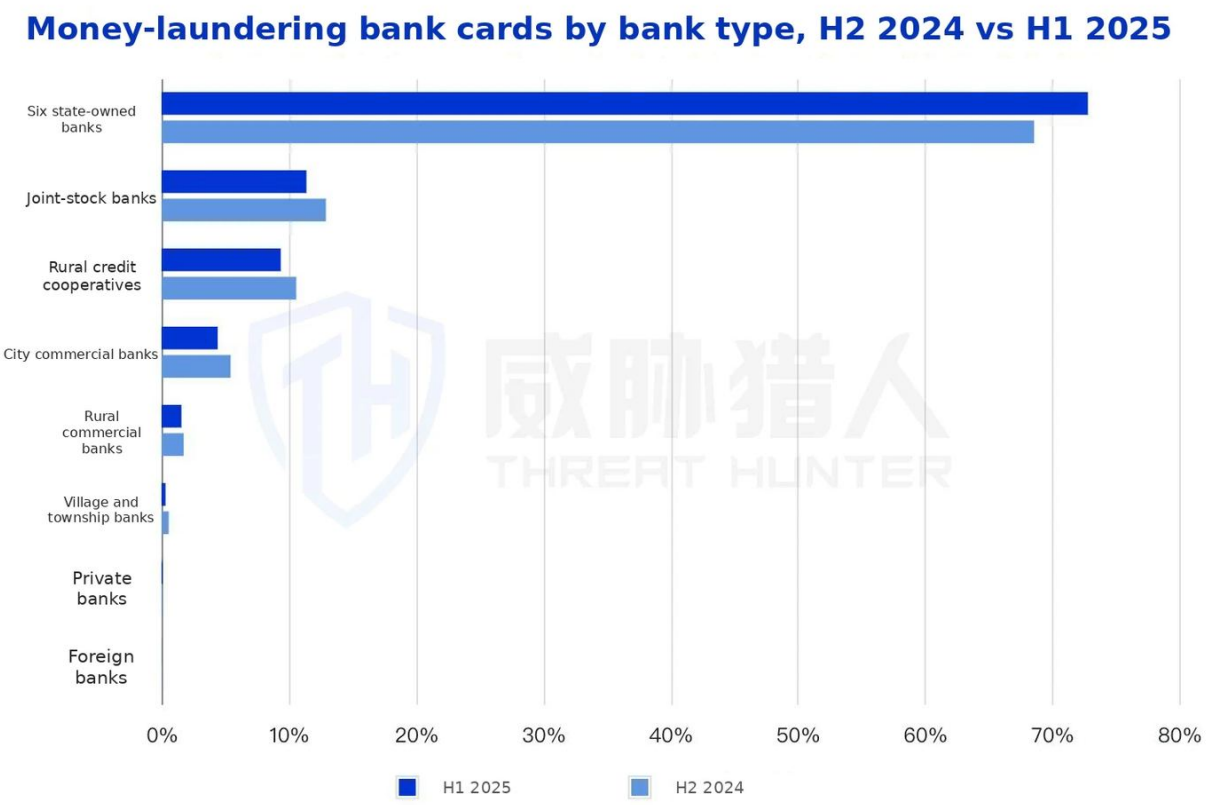
This change clearly reflects that the current crackdown methods have not fundamentally cut off the money laundering chain of threat actors. The threat actors organization has extremely strong adaptability and transfer capabilities. Once a certain platform is restricted, it will quickly turn to other channels to continue operating. Therefore, it is difficult to form a sustained and effective deterrent force by relying solely on sanctions on individual platforms. The money laundering industry chain of threat actors is still evolving and spreading, and the crackdown faces huge challenges.



New fraud-linked cards per month, H1 2025

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

(2) Among the bank cards involved in money laundering in the first half of 2025, the money laundering cards of the six major state-owned banks still account for the largest proportion, reaching 73%. (3) Among the bank cards involved in money laundering in the first half of 2025, the three types of money laundering cards are ranked in the top 1 provinces of Guangdong Province. Threat Hunter research found that in the first half of 2025, the three risk types of money laundering bank cards belong to the top 10 provinces. All cover Guangdong, Jiangsu, and Sichuan, among which the top 1 is Guangdong.

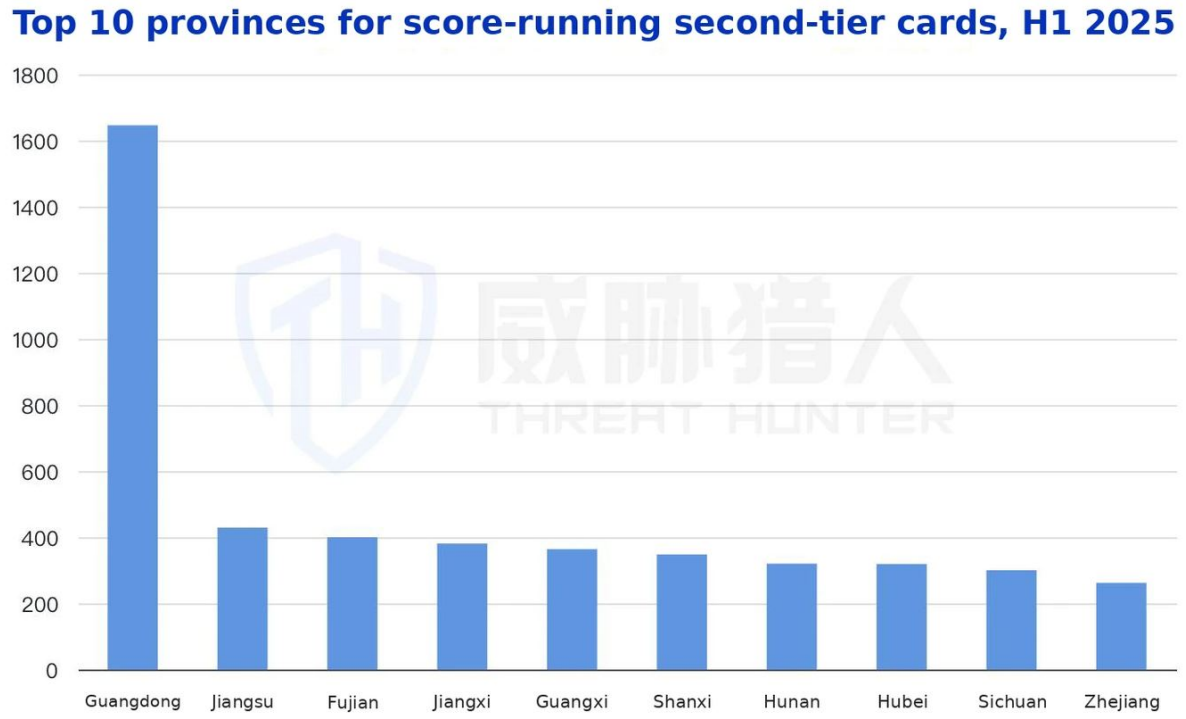


Money-laundering bank cards by bank type, H2 2024 vs H1 2025

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

However, there are differences among the top 10 provinces for different types of money laundering bank cards:

For example, among the top 10 provinces that score second-level cards, Fujian and Jiangxi are unique provinces; and among the top 10 provinces that are involved in fraudulent cards, Shandong is unique.



Top 10 provinces for score-running second-tier cards, H1 2025

Source: Threat Hunter original report, page 26. Original figure with Chinese text replaced by English.



Top 10 provinces for gambling-linked cards, H1 2025

Source: Threat Hunter original report, page 26. Original figure with Chinese text replaced by English.



Top 10 provinces for fraud-linked cards, H1 2025

Source: Threat Hunter original report, page 26. Original figure with Chinese text replaced by English.

(4) Among the bank cards involved in money laundering in the first half of 2025, the top 1 cities for the three types of money laundering cards are all Shenzhen. Threat Hunter research found that the top 10 cities for the three risk types of money laundering cards in the first half of 2025 all include Shenzhen, Guangzhou, Chongqing, Shanghai, Beijing, Dongguan, and Chengdu, among which the top 1 is Shenzhen.

However, there are differences among the top 10 cities for different types of money laundering bank cards:

For example, among the top 10 cities that score second-level cards, Jincheng and Nanjing are unique cities; among the top 10 cities that are involved in gambling cards, Yinchuan is unique; and among the top 10 cities that are involved in fraudulent cards, Zhengzhou and Xi'an are unique cities.



Top 10 cities for score-running second-tier cards, H1 2025

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



Top 10 cities for gambling-linked cards, H1 2025

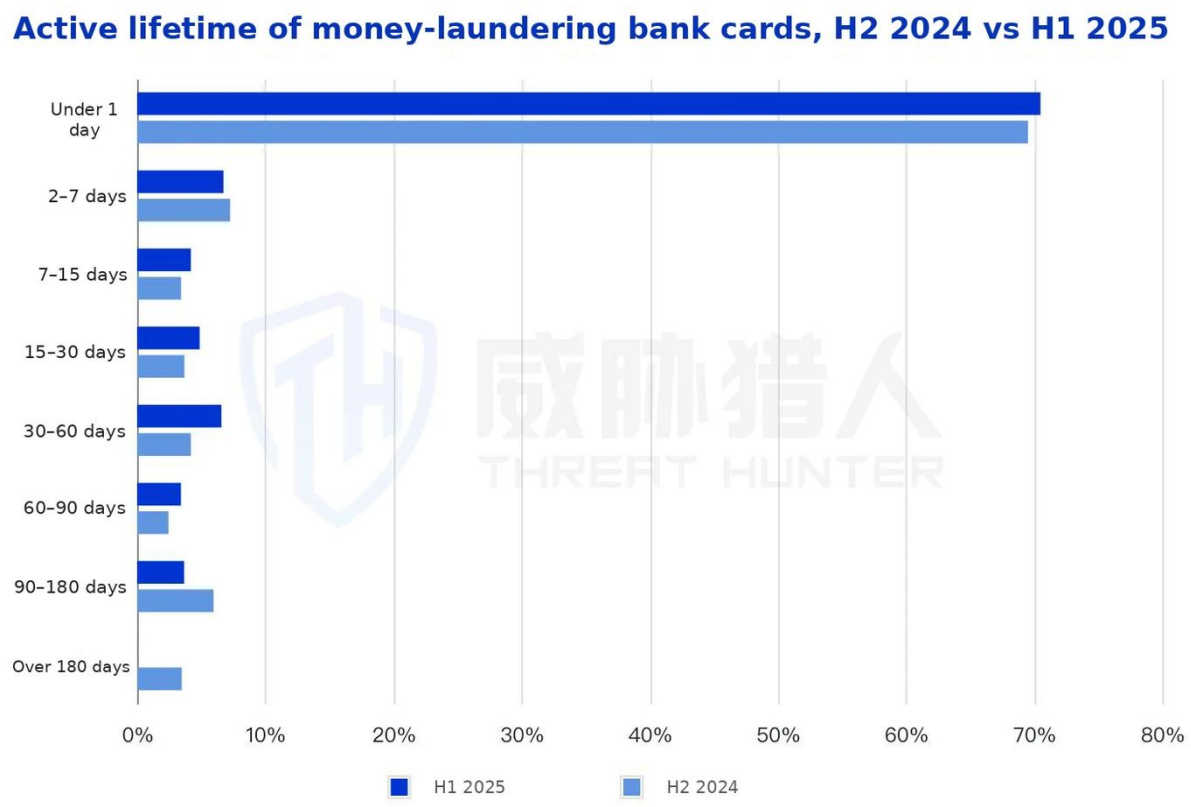
Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.



Top 10 cities for fraud-linked cards, H1 2025

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

(5) Among the bank cards involved in money laundering in the first half of 2025, the proportion of active cycles within "one day" has basically remained at around 70%. Threat Hunter analysis found that the active time of money laundering cards still shows short-term characteristics. In the first half of 2025, single-day active cards accounted for 70%, and long-term active cards (more than 180 days) accounted for less than 1%.



Active lifetime of money-laundering bank cards, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 28. Original figure with Chinese text replaced by English.

1.3.2 Analysis of changes in corporate money laundering account resources in the first half of 2025

Money laundering corporate accounts: Corporate accounts refer to accounts opened in banks in the name of a company. Money laundering corporate accounts refer to bank corporate accounts used by threat actors to launder illegal funds. Because corporate accounts have the characteristics of large collection amounts and high number of transfers, "corporate accounts" often serve as concentration and divergence points for black money transfers.

(1) In the first half of 2025, new money laundering corporate accounts dropped by 40% month-on-month. In the first half of 2025, Threat Hunter monitoring data showed that the number of new money laundering corporate accounts dropped by 40% month-on-month. The analysis found that there are three main factors leading to the decline:

1. The number of money laundering gangs that provide public accounts for money laundering is decreasing. In the first half of 2025, the number of money laundering gangs that provide public accounts decreased.

That's down 18%.

2. The demand for corporate money laundering will drop briefly at the beginning of each year. According to research on underground money laundering actors, it is found that threat actors are approaching

The demand for public money laundering will decrease in the 1-2 months before the Spring Festival, and the number of threat actors providing public accounts will also decrease.

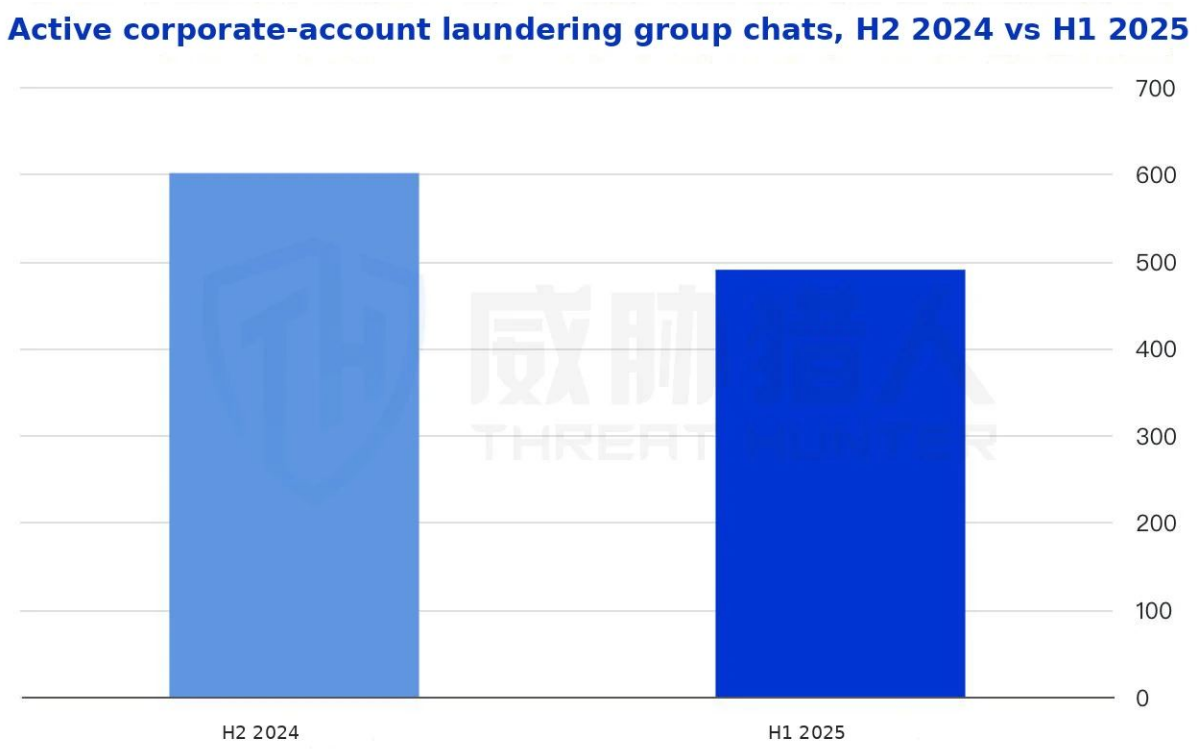
3. In May, the United States imposed sanctions on Huione Group (Huiwang), causing its cybercrime ecosystem guarantee platform "Haowang" on an encrypted messaging app to collapse.

The number of threat actors active in public money laundering on encrypted messaging apps dropped further by 26.25% after May.



New money-laundering corporate accounts, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 29. Original figure with Chinese text replaced by English.



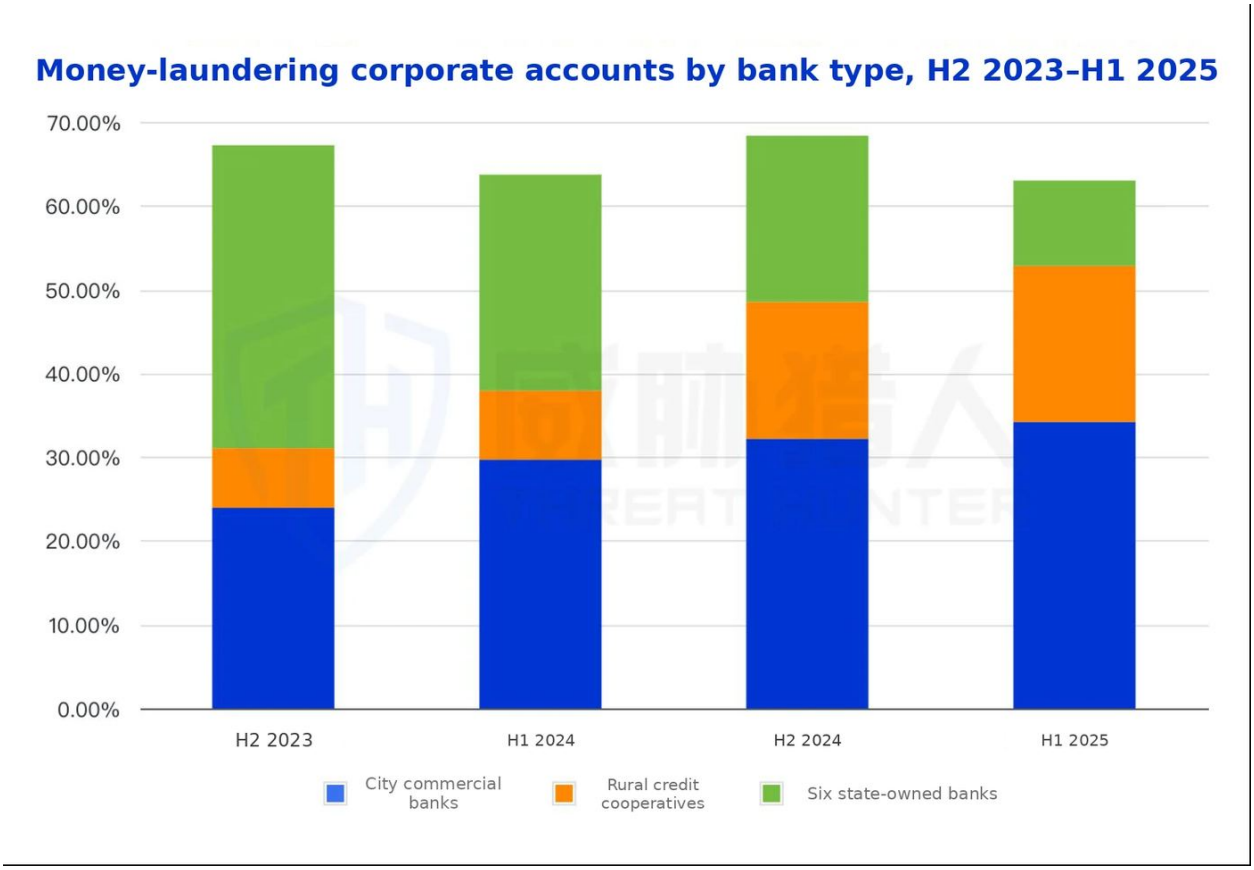
Active corporate-account laundering group chats, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 29. Original figure with Chinese text replaced by English.

(2) In the first half of 2025, among corporate accounts involved in money laundering, the targets of threat actors gradually shifted from the six major banks to city commercial banks and rural credit cooperatives. Threat Hunter data in the past two years shows that the ownership of corporate accounts involved in money laundering has changed significantly. From the second half of 2023 to the first half of 2025, the proportion of money laundering public accounts of the six major state-owned banks dropped from 36% to 20%. At the same time, urban commercial banks and rural agricultural banks

The proportion of rural credit cooperatives has continued to rise, with urban commercial banks increasing from 23% to 34%, and rural credit cooperatives also rising from 7% to 18%.

This phenomenon clearly 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. , (3) Among the public accounts involved in money laundering in the first half of 2025, the top 3 provinces are Guangdong, Shandong, and Jiangsu (4) Among the public accounts involved in money laundering in the first half of 2025, the top 3 cities are Beijing, Guangzhou, and Shenzhen



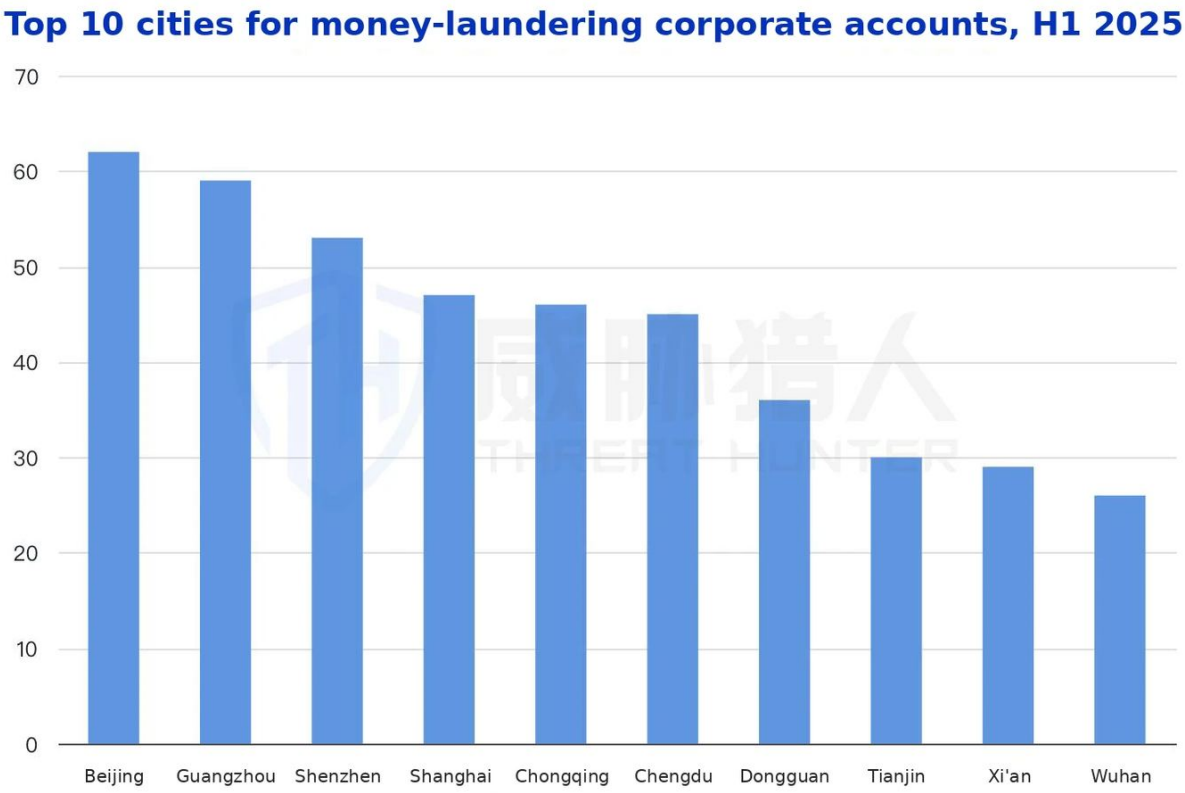
Money-laundering corporate accounts by bank type, H2 2023–H1 2025

Source: Threat Hunter original report, page 30. Original figure with Chinese text replaced by English.



Top 10 provinces for money-laundering corporate accounts, H1 2025

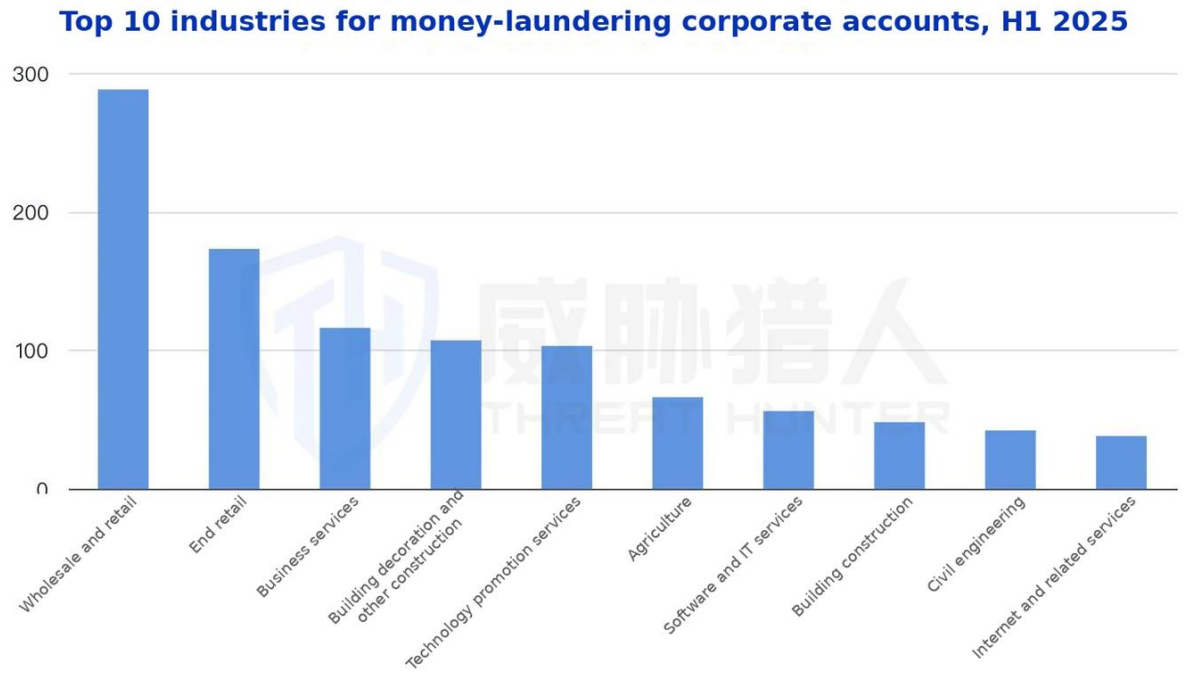
Source: Threat Hunter original report, page 30. Original figure with Chinese text replaced by English.



Top 10 cities for money-laundering corporate accounts, H1 2025

Source: Threat Hunter original report, page 31. Original figure with Chinese text replaced by English.

(5) Among the public accounts involved in money laundering in the first half of 2025, the top 3 industries are wholesale and retail, terminal retail, and business services. Threat Hunter data in the past two years shows that among the public accounts involved in money laundering, the industries of the top 10 have not changed, and the channel wholesale industry has long been at the top. This shows that public accounts in such industries are more likely to be used by threat actors to launder money.



Top 10 industries for money-laundering corporate accounts, H1 2025

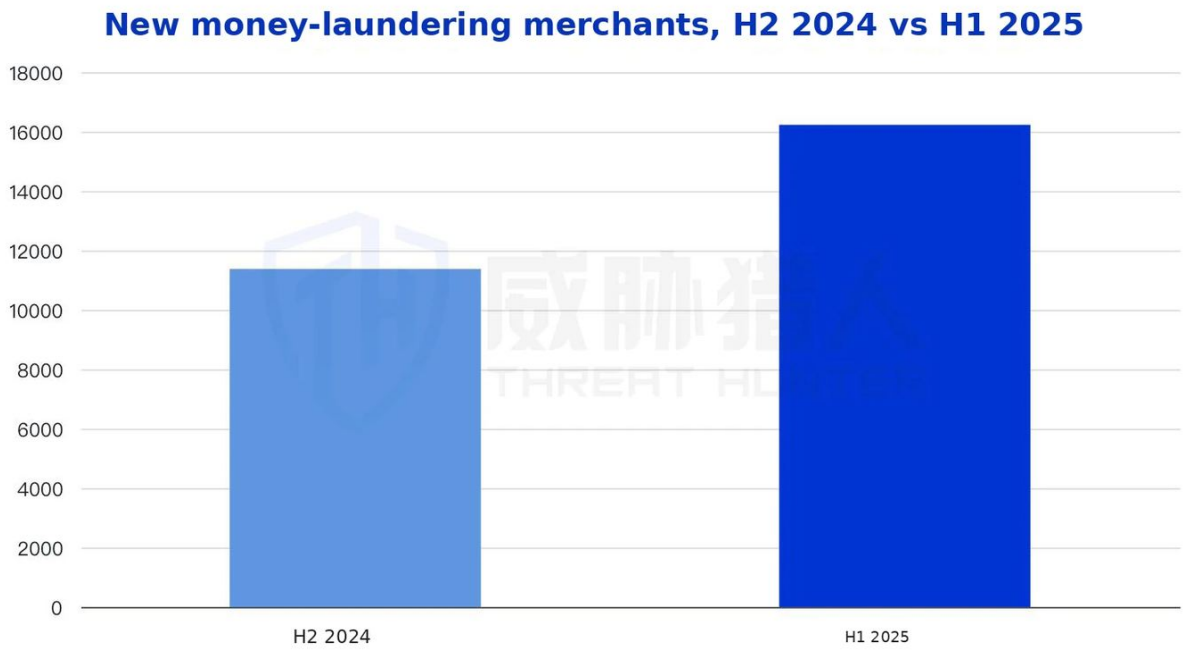
Source: Threat Hunter original report, page 31. Original figure with Chinese text replaced by English.

1.3.3 Analysis of resource changes of merchants involved in money laundering in the first half of 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 Huabei, credit card and other payment methods. Compared with traditional money laundering methods, they are more covert and efficient.

(1) The number of active merchant money laundering gangs continues to rise, and the number of merchants used by threat actors to launder money has increased by 43% month-on-month. In the first half of 2025, the number of merchant accounts used for money laundering has increased by 43% month-on-month, showing a rapid growth trend. The main driving force behind this significant growth is that the cost and threshold for threat actors to acquire merchants are low, and the characteristics of merchant transactions are similar to those of money laundering transactions.

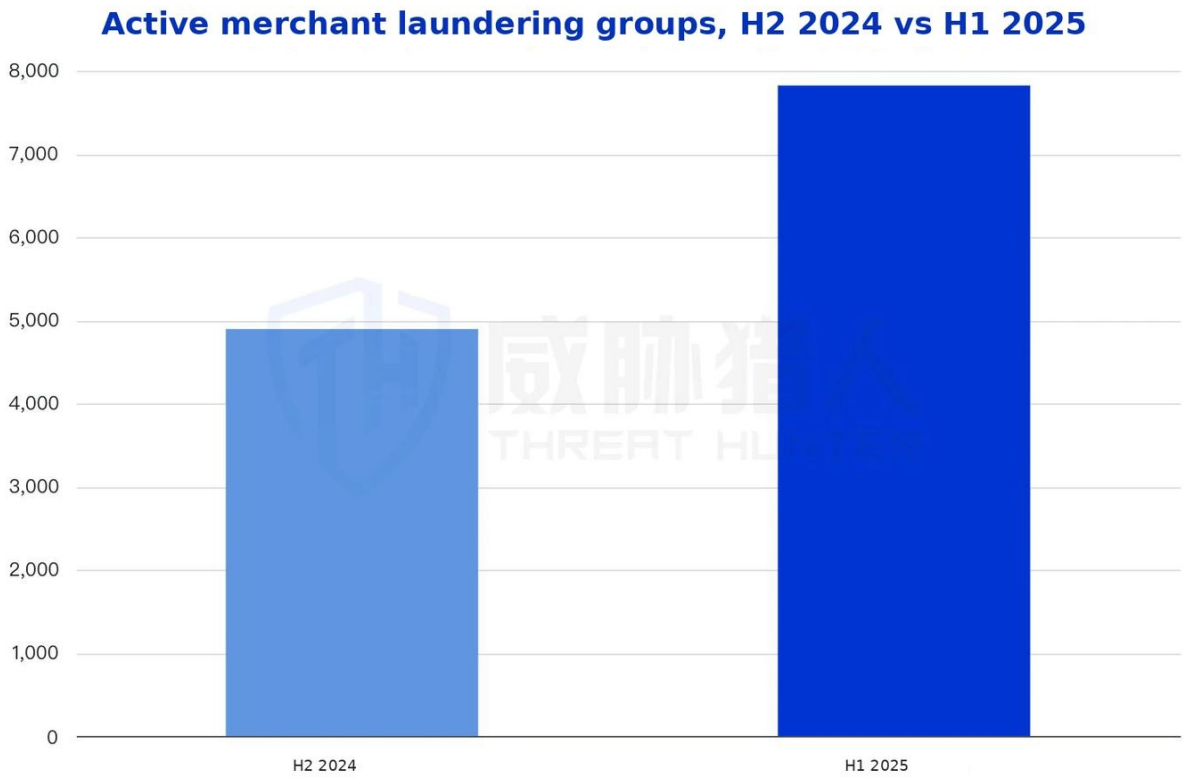
On the one hand, threat actors use illegal means such as forging materials, qualification transactions, and agency account opening to bypass audits at extremely low costs. Once obtained, these accounts will be sold or leased to money laundering gangs in large quantities. On the other hand, merchants themselves have the characteristics of high-frequency transactions, large-amount capital flows, and support for multiple payment methods, which provide a natural channel for the flow and cover of illegal funds. This "easy access and high adaptability" feature makes merchants become important nodes in the money laundering chain of threat actors.



New money-laundering merchants, H2 2024 vs H1 2025

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

Threat Hunter monitoring data shows that in the first half of 2025, the number of active merchant money laundering threat actor groups increased by 60% month-on-month. This data reflects the expansion of merchants' money laundering risks, and the model is evolving towards organization and scale, further demonstrating the challenges that merchants' money laundering models pose to anti-money laundering work.



Active merchant laundering groups, H2 2024 vs H1 2025

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

(2) Among the merchants involved in money laundering in the first half of 2025, the top 3 provinces are Guangdong, Zhejiang, and Hubei (3) Among the merchants involved in money laundering in the first half of 2025, the top 3 cities are Guangzhou, Wuhan, and Kunming (4) Among the merchants involved in money laundering in the first half of 2025, the top 3 industries are terminal retail, wholesale and retail, and catering industries



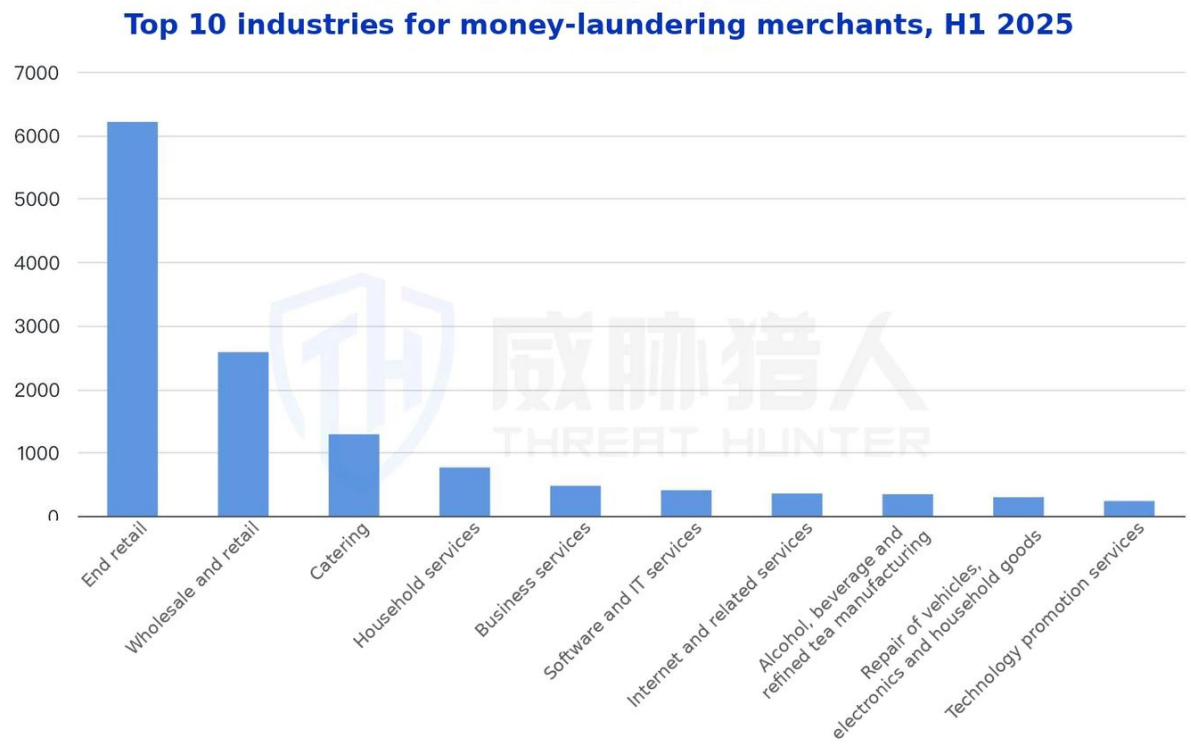
Top 10 provinces for money-laundering merchants, H1 2025

Source: Threat Hunter original report, page 33. Original figure with Chinese text replaced by English.



Top 10 cities for money-laundering merchants, H1 2025

Source: Threat Hunter original report, page 33. Original figure with Chinese text replaced by English.



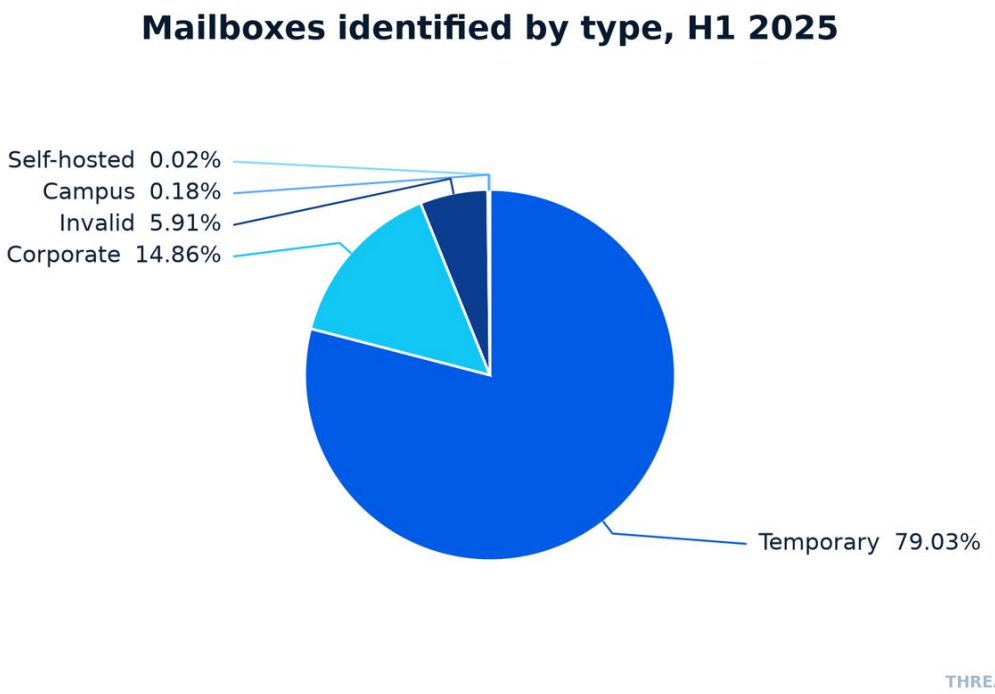
Top 10 industries for money-laundering merchants, H1 2025

Source: Threat Hunter original report, page 33. Original figure with Chinese text replaced by English.

1.4 Analysis of risk mailbox resources in the first half of 2025

In the first half of 2025, Threat Hunter identified 116,800 email domain names, of which high-risk temporary email addresses accounted for the largest proportion, reaching

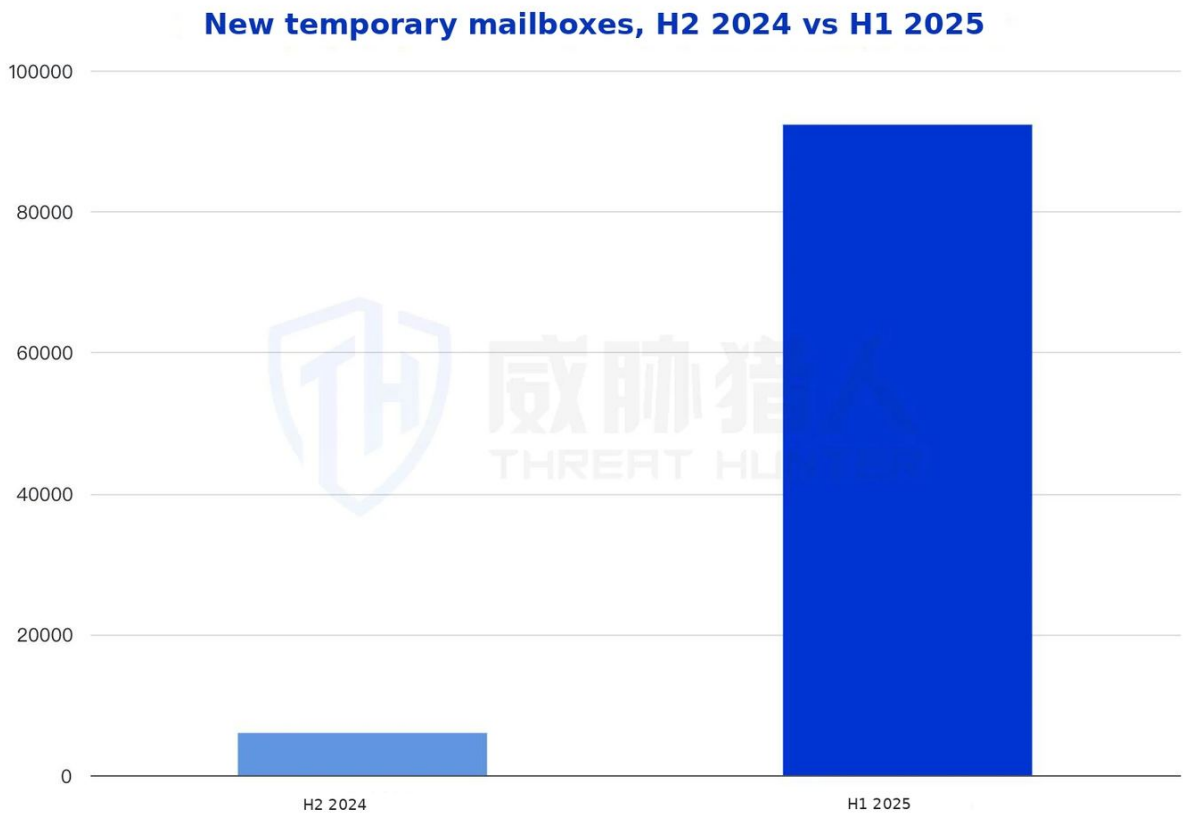
79.03%.



Mailboxes identified by type, H1 2025

Source: Threat Hunter original report, page 34. Redrawn in English from the original figure.

In the first half of 2025, the number of high-risk temporary email domain names increased 14 times month-on-month. Threat Hunter uses mail server anti-inspection technology to strengthen the monitoring capabilities of temporary mailbox domain name groups that share the same mail server, and captures derivative domain names that are not fully covered and belong to the same batch of temporary mailbox service providers, greatly broadening the monitoring scope of risky mailboxes.



New temporary mailboxes, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 34. Original figure with Chinese text replaced by English.

Analysis of common attack techniques by threat actors in the first half of 2025

2. Analysis of common attack technologies by threat actors in the first half of 2025

2.1 AI technology helps threat actors achieve minute-level attacks

"Mom, 8,000 yuan is not enough, please transfer 15,000 yuan to me." A mother was video chatting with her daughter. When her daughter, who was studying out of town, complained coquettishly in the video that "living expenses are not enough," she felt distressed and planned to transfer the money to her child immediately. Just then, the door opened and her "real daughter" walked in. On the other side, the "fake daughter" in the video is still begging her mother to "give her living expenses."

This is an AI anti-fraud video. In the comment area of □□this anti-fraud video, many netizens reported that they had had similar experiences of being deceived, "The scammer called, and his voice and appearance were exactly like those of my family."

In the above example, the fraudsters used real-time face-changing + voice cloning technology to commit fraud. Real-time face-changing technology provides the first convenience for fraudsters to pretend to be relatives of victims, while voice cloning technology provides a second layer of

insurance for fraudsters to gain the trust of relatives of victims, allowing fraudsters to maximize the trust of relatives of victims and thereby commit fraud.

Thanks to the development of AI technology, threat actors are gradually applying AI technology to their attacks. This lowers the attack threshold of threat actors to a certain extent, improves the attack efficiency of threat actors, and improves the quality of attacks by threat actors. This also makes victims vulnerable to attacks from threat actors.

2.1.1 Evolution of AI face-changing technology - realizing minute-level AI face-changing with the help of a small number of pictures

In 2023, Threat Hunter demonstrated cybercriminal groups attack technology of AI face-swapping based on videos; and after two years of technological development, the attack technology of AI real-time face-swapping based on pictures has gradually matured and begun to be used by threat actors in attacks.

(1) Comparison of old and new technologies

By comparing attack techniques in different periods, we can know:

1. New technology has the advantages of lower material requirements and shorter training time;

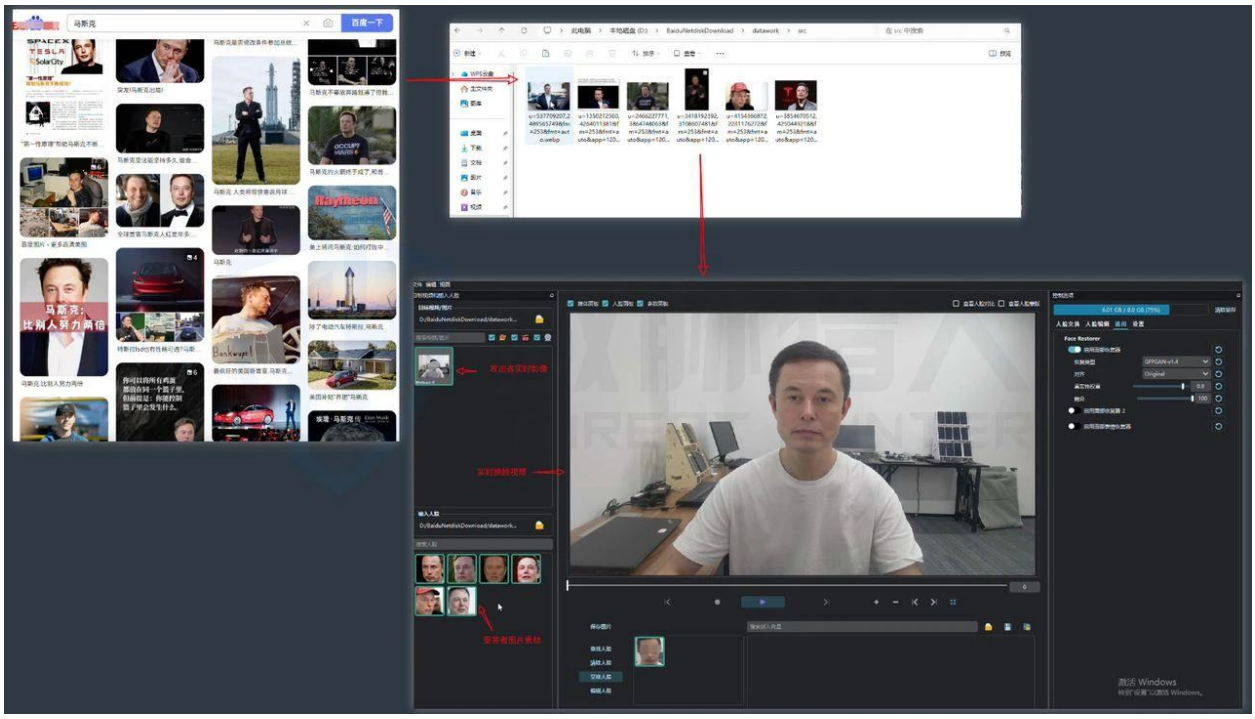
2. There are limited conditions for the face-changing effect. The face shape needs to be similar. The degree of similarity directly affects the success rate.

	Early stage	Middle stage	Now
Result	Offline face swap based on model training	Real-time face swap based on model training	Real-time face swap with no model needed
Material needed	10–20 seconds of the victim’s face on video	10–20 seconds of the victim’s face on video	3–5 photos of the victim’s face
Training time	Hours to days	Hours to days	None: swaps in real time
Swap quality	Good	Good	Depends on how alike the attacker’s and victim’s faces are: the closer, the better
Hardware	30-, 40- or 50-series graphics cards all work	30-, 40- or 50-series graphics cards all work	30-, 40- or 50-series graphics cards all work

How face-swap technology has evolved

Source: Threat Hunter original report, page 37. Table re-typeset in English from the original.

(2) The new technology demonstration process is very simple: first, obtain 2-3 pictures of the target person from public channels; then directly load the pictures using face-changing software to achieve real-time face-changing.



Screenshot of a face-swapped live video call

Source: Threat Hunter original report, page 37. Original image retained.

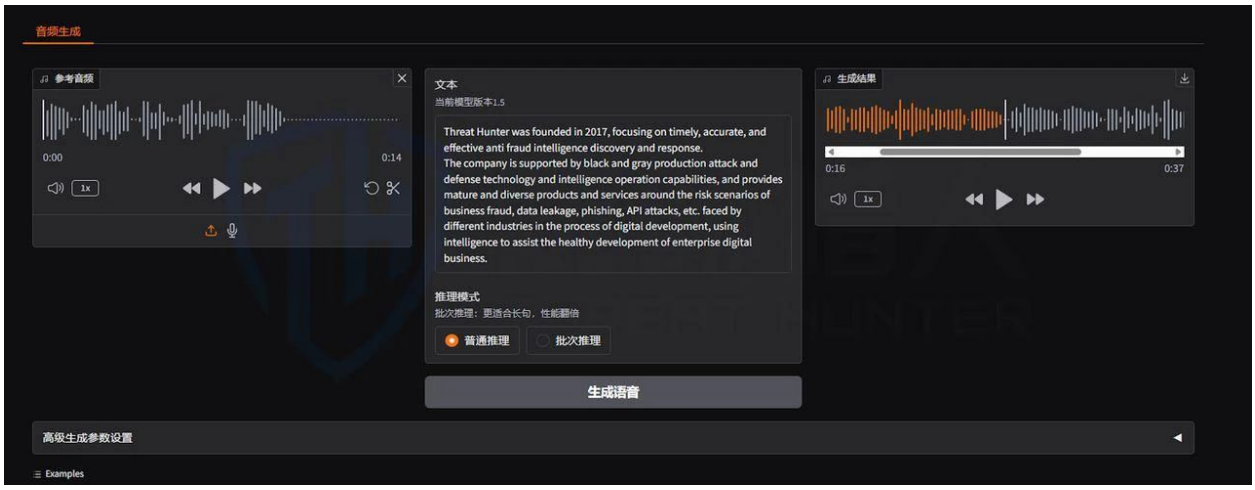
(3)Risk

The development of AI face-changing technology has made the materials needed for attackers to carry out attacks simpler and faster. Take app face authentication bypass scenarios and telecommunications fraud scenarios as examples. This allows attackers to carry out attacks in a shorter period of time, leaving victims with less and less time to think. Often, attackers have already launched attacks before the victim can react, leaving the victim defenseless.

2.1.2 Voice cloning technology-sound cloning based on 10 seconds of audio

Thanks to the development of technology, in addition to the AI face-changing technology mentioned above, voice cloning technology based on a small amount of audio has also become mature and used by threat actors in attacks.

(1) The technical demonstration uses a 10-second audio clip of the victim as a cloning sample. The clone can be completed in just 10 seconds, and any content can be output in the victim's voice.



Screenshot of a voice-cloning tool

Source: Threat Hunter original report, page 38. Original image retained.

(2) Risks Unlike AI face-changing, voice cloning is often used in telecommunications fraud scenarios. Voice cloning technology may be used in common fraud scenarios such as phone fraud and video conferencing fraud. The development of voice cloning technology will inevitably make attackers' attacks more realistic and faster.

2.2 Code pulling tool-grab platform payment order link for money laundering (1) Tool information

Threat Hunter captured a code pulling tool commonly used by threat actors for money laundering in April 2025. The function of this tool is to capture payment order links generated by e-commerce platforms and payment platforms, and convert the links into QR codes for their associates to scan and use.

Information about the tool is as follows:

App name	Huangchao Proxy Pay
App type	Code-pulling tool
Requirements	Root access, VPN proxy
Interface	

Profile of a code-pulling tool

Source: Threat Hunter original report, page 39. Original figure with Chinese text replaced by English.

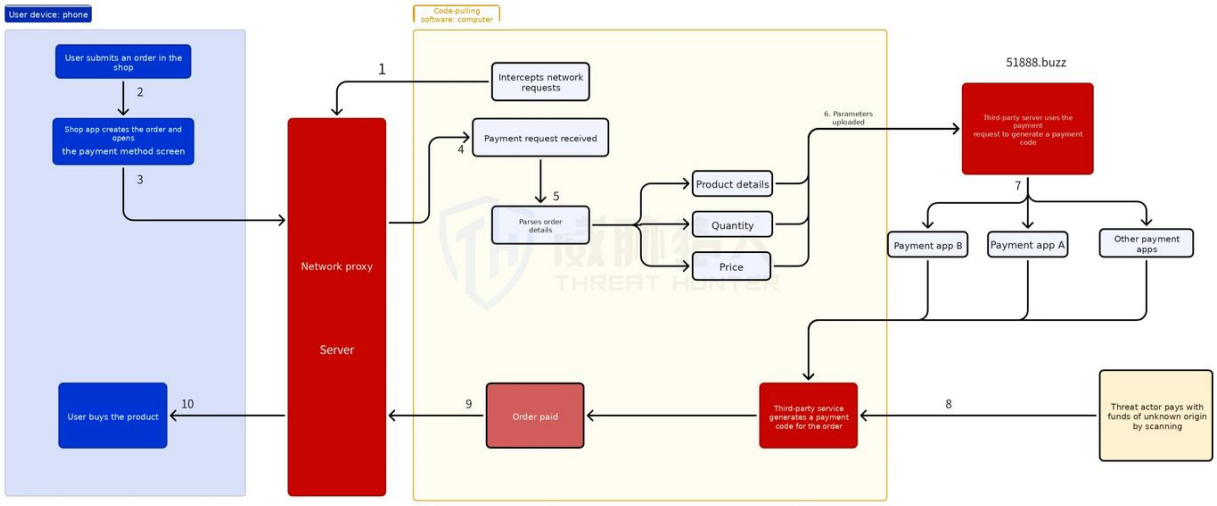
(2) Tool process introduction This type of tool uses packet capture technology to capture payment order links for payment by threat actors in the money laundering process. The specific operation process is as follows:

1. Set up VPN port forwarding on mobile phone

2. Open the software on the computer and monitor the information forwarded by the mobile phone.

3. On the mobile phone, select the product in the software to place an order, and the payment QR code will pop up on the computer.

4. Use other mobile phones to scan the QR code and pay.



How a code-pulling tool turns shop orders into payment codes

Source: Threat Hunter original report, page 40. Original figure with Chinese text replaced by English.

After investigation, this type of tool is often used in scenarios such as payment for threat actors, money laundering, and order fraud. The following is an example of electronic fraud gang A looking for money laundering gang B to launder money. During the money laundering process, the money laundering gang used the code pulling tool to swindle the payment orders of the formal platform into the money laundering process, causing the black money to flow directly to the formal platform, making the money laundering process wider and more difficult to trace.

The services and main processes provided by money laundering gang B are as follows:

1. An electronic fraud gang obtained 20,000 yuan through fraud and looked for a money laundering gang to launder the money;

2. Money laundering gangs create social group chats and continue to operate them, using discounts to purchase goods as a gimmick to attract normal users;

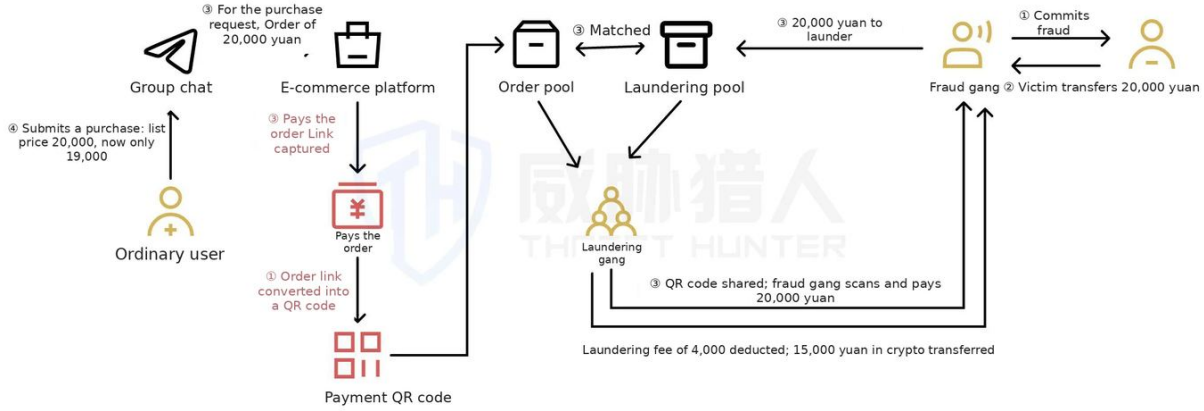
3. Normal user A purchased computer equipment for 20,000 yuan originally; now he purchases it in the group chat for only 19,000 yuan;

4. The money laundering gang matches the money laundering demand of 20,000 yuan with the purchase demand of 20,000 yuan from normal users, allowing the money laundering gang to use fraud to obtain the money.

20,000 yuan to pay a normal user’s purchase order; in this process, the electronic fraud gang relied on the QR code or link generated by the money laundering gang through the code pulling software to complete the payment of the normal user’s 20,000 yuan product order.

5. Normal user A transfers the purchase fee of 19,000 yuan to the money laundering gang. After the money laundering gang deducts the money laundering service fee of 4,000 yuan, the remaining

Transfer 15,000 yuan to the electronic fraud gang in equivalent virtual currency;



How e-commerce orders are used to launder fraud proceeds

Source: Threat Hunter original report, page 40. Original figure with Chinese text replaced by English.

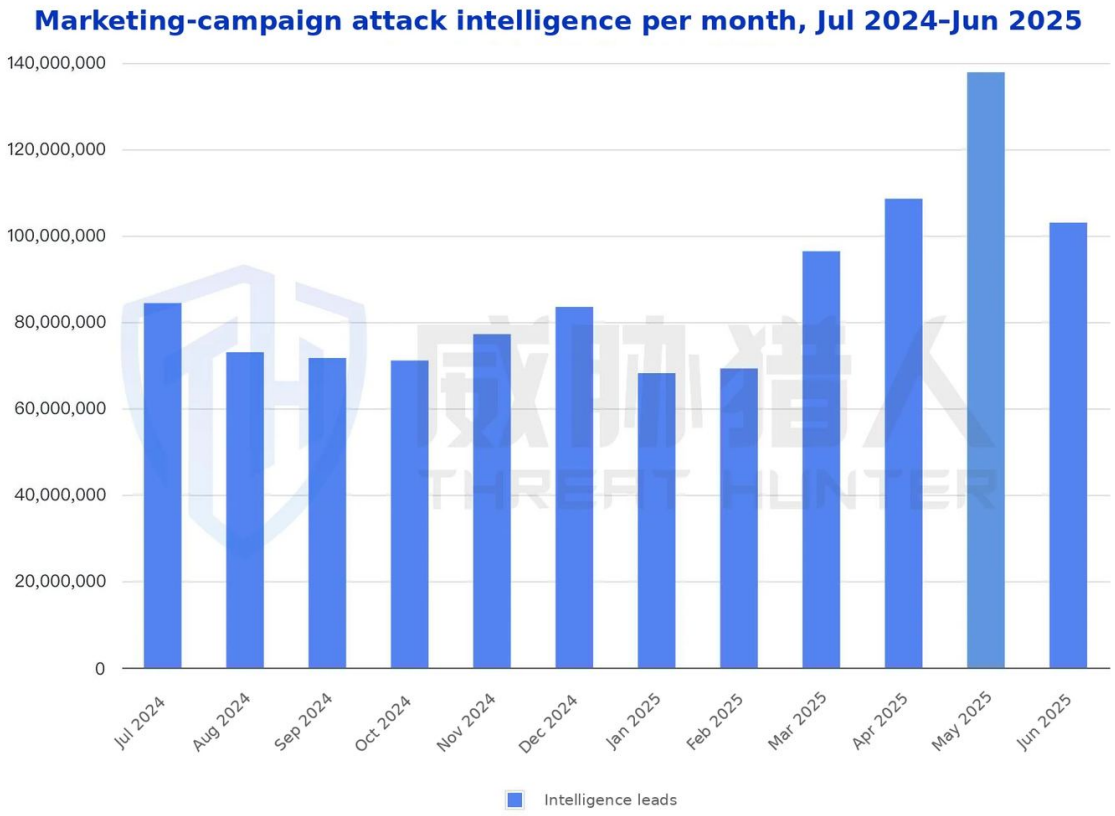
Analysis of threat actors attack scenarios in the first half of 2025

3. Analysis of threat actors attack scenarios in the first half of 2025

3.1 Marketing fraud scenario analysis

In the first half of 2025, the Threat Hunter system captured a total of 580 million pieces of marketing campaign attack intelligence, an increase of more than 26% from the second half of 2024 (460 million pieces), showing a continued high-pressure trend.

The number of attacks has increased significantly since January 2025. From January to March, the number of online reports rose from 68 million to 96 million+. In May, the number of online reports soared to 137 million, which was the peak in half a year. A large number of cybercriminal groups used May Day promotion nodes and the brand 618 warm-up period to focus on marketing fraud content.

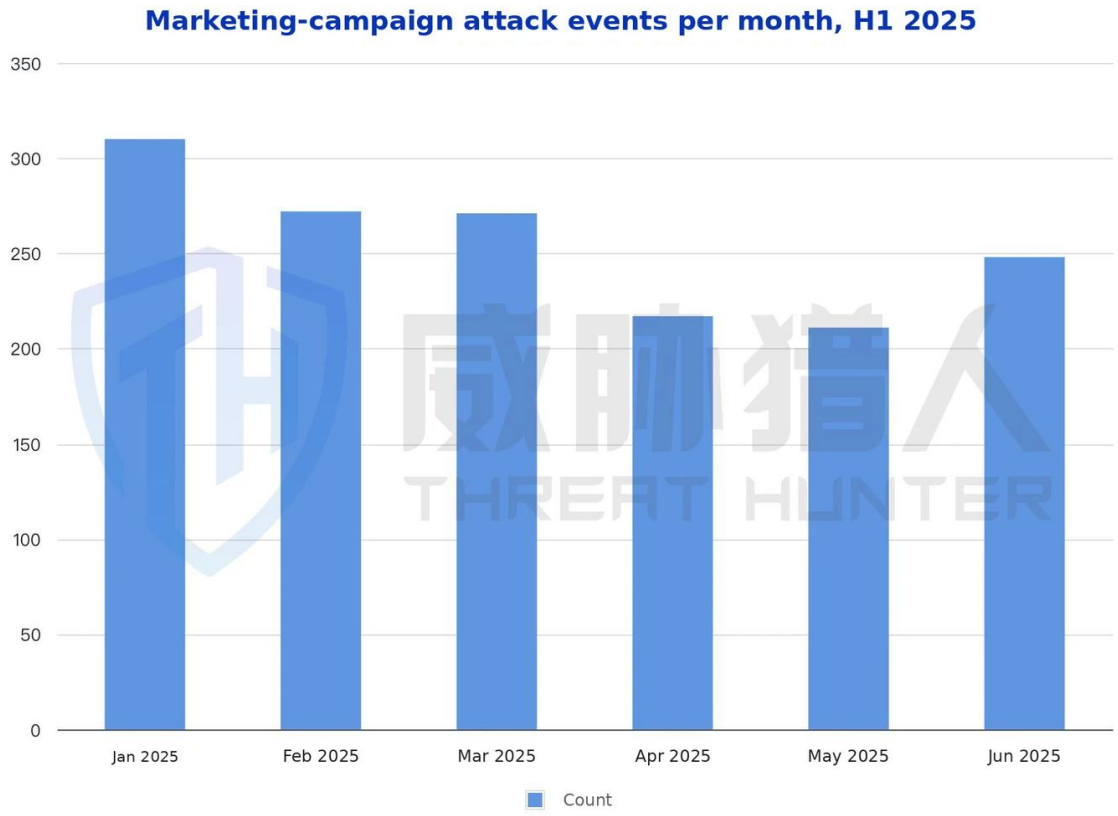


Marketing-campaign attack intelligence per month, Jul 2024–Jun 2025

Source: Threat Hunter original report, page 42. Original figure with Chinese text replaced by English.

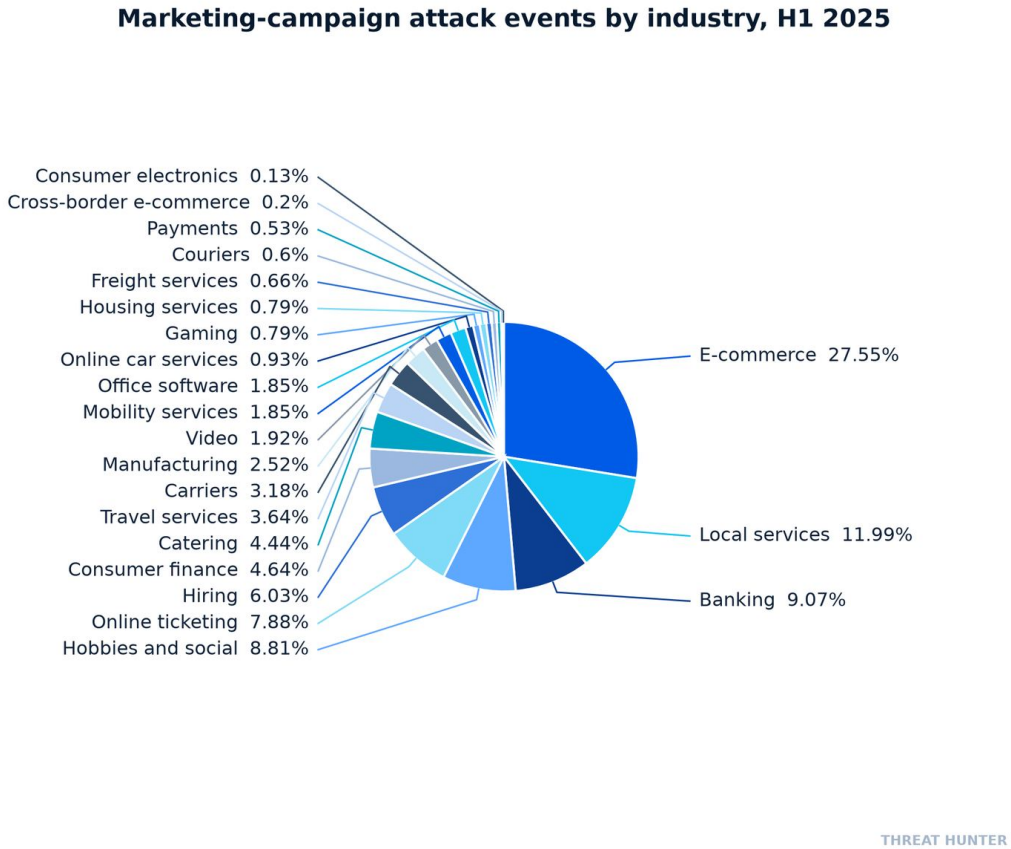
In the first half of 2025, Threat Hunter warned a total of 1,510 synchronous risk events. From the perspective of industry distribution, the e-commerce industry is still the area with the most concentrated risks, accounting for 27.55%, followed by local life (11.99%), banking (9.07%), interest social networking (8.82%), online ticketing (7.88%) and other industries. The overall characteristics are as follows:

- Industries with strong platform attributes have higher risks: industries such as e-commerce, life services, and ticketing have become key targets of threat actors because they rely on user activity, order transactions, and marketing activities;
- Industries with frequent capital interactions are also prone to risk: such as banking, consumer finance, and payment industries. The risk focus is more on conversion path tampering and profiteering behaviors under marketing diversion;



Marketing-campaign attack events per month, H1 2025

Source: Threat Hunter original report, page 43. Original figure with Chinese text replaced by English.



Marketing-campaign attack events by industry, H1 2025

Source: Threat Hunter original report, page 43. Redrawn in English from the original figure.

According to Threat Hunter platform monitoring data, in the first half of 2025, an average of about 375,000 threat actor groups involved in marketing activities were captured every month, with May and June being the highs for half a year. The overall number of groups increased slightly compared to the same period in the second half of 2024.



Threat-actor groups targeting marketing campaigns per month, Jul 2024–Jun 2025

Source: Threat Hunter original report, page 44. Original figure with Chinese text replaced by English.

In the first half of 2025, the Threat Hunter platform captured an average of more than 1.3 million cybercrime operator accounts related to marketing fraud every month, of which the number reached 1.436 million in June, a new high in the past year. The overall increase compared with the average monthly level in the second half of 2024 (approximately 1.17 million) increased by 11%.



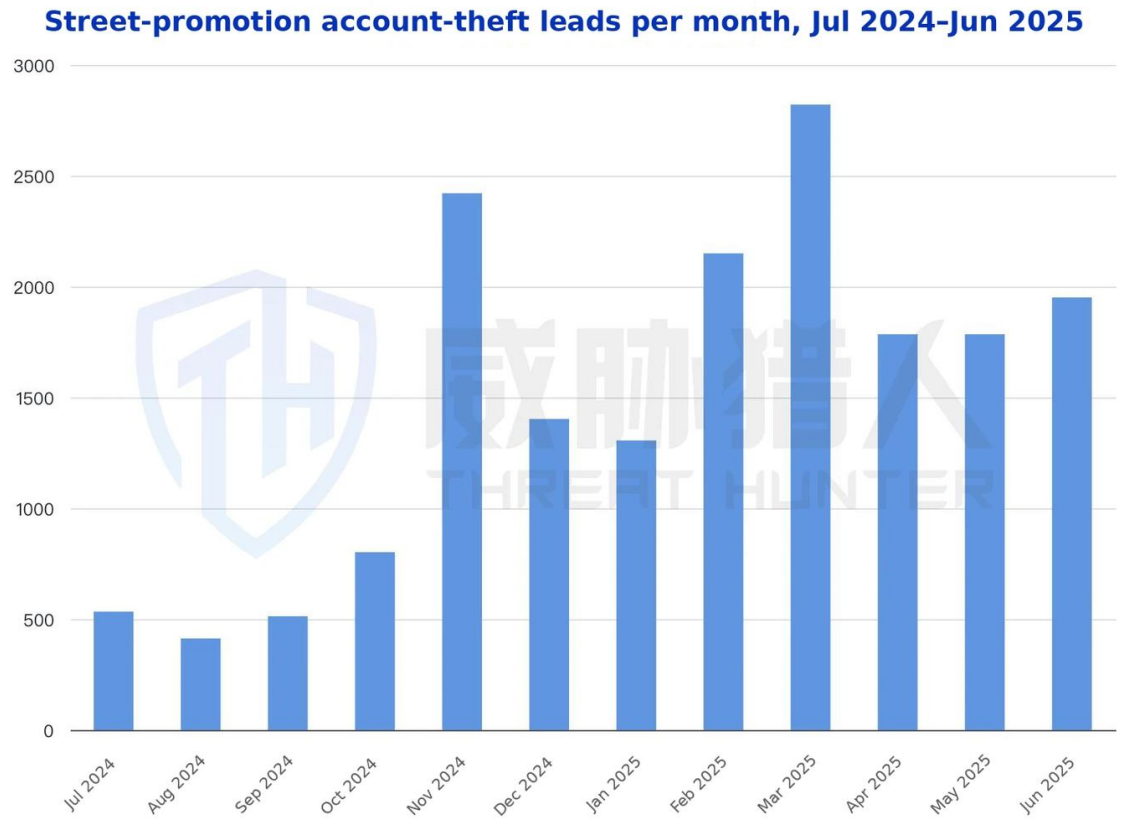
Threat actors targeting marketing campaigns per month, Jul 2024–Jun 2025

Source: Threat Hunter original report, page 44. Original figure with Chinese text replaced by English.

3.1.1 threat actors “graft” traditional underground promotion methods to account theft fraud

Since the first half of this year, the risk of account theft has gradually increased, and cybercriminal groups have continued to innovate their methods, gradually evolving from "technical hijacking" to "social engineering induction", eventually forming a compound attack model of "technical hijacking + social engineering". Such stolen accounts, after being traded by threat actors, will eventually be used for various illegal purposes such as traffic diversion and fraud.

Threat Hunter data shows that in the first half of 2025, a total of 11,798 tips on the risk of account theft were captured, and in the second half of 2024, a total of 6,080 such tips were captured, a month-on-month increase of 94.05%. Among them, there has been a significant increase since February this year, indicating that the Spring Festival is a period of high incidence of local push account theft; the data fell back in the following three months, but the overall number is still at a high level, indicating that the risk has not been eliminated.



Street-promotion account-theft leads per month, Jul 2024–Jun 2025

Source: Threat Hunter original report, page 45. Original figure with Chinese text replaced by English.

(1) The traditional local promotion method has attracted the attention and utilization of threat actors. The so-called "local promotion", which is the abbreviation of "ground promotion", was originally a marketing method for companies to contact users and promote products offline by setting up stalls, sweeping streets, distributing leaflets, and face-to-face explanations. Its core feature is real contact + on-site transformation, which is often found in crowded areas such as subway entrances, business districts, campuses, and exhibitions.

It is through this form that cybercriminal groups "graft" traditional offline promotion techniques into fraud attacks. Through the use of mainstream social platforms, threat actors use words such as "scan QR code to log in", "swipe orders to get rebates" and "win and receive prizes" to induce users to scan QR codes, download apps or hand over their mobile phones, inducing them to actively submit authorization information or perform sensitive operations, thereby gaining control of their accounts.

(2) Two types of high-frequency account-stealing paths. Threat Hunter has identified two types of high-frequency account-stealing paths:

One type is a single-point crime, in which local promoters hold code-receiving cards and use words to induce users to scan codes and change accounts. The process is simple, and the stolen accounts are directly sold for cash, and the organizational structure is loose.

The other type is chain-based crimes, in which the upstream develops Trojan tools, the midstream implements the implantation, and the downstream is responsible for account transfer and

monetization. The division of labor is clear, the scale of the crime is larger, and the concealment is stronger.

1. Traffic diversion + account re-binding: threat actors' efficient account theft route. When threat actors contact victims face-to-face, they often guide victims to scan QR codes or hand over their mobile phones through offline promotion activities, scan code lottery draws, etc., and then use the name of "auxiliary operations" to quickly complete the operations of resetting account passwords and re-binding phone numbers. This type of threat actor stealing accounts is simple and efficient. But the account is easily disconnected. threat actors can obtain the short-term use rights of their accounts (1-2 days), so threat actors often connect with buyers in advance and quickly sell them for profit after obtaining the accounts.

1. threat actors set up stalls on the streets to attract users to participate in other activities (scan QR codes to register to receive gifts, download apps, etc.)

2. threat actors use words to gain the trust of users, and take the opportunity to get the mobile phone and quickly set a login password for the account (such as aa123456).

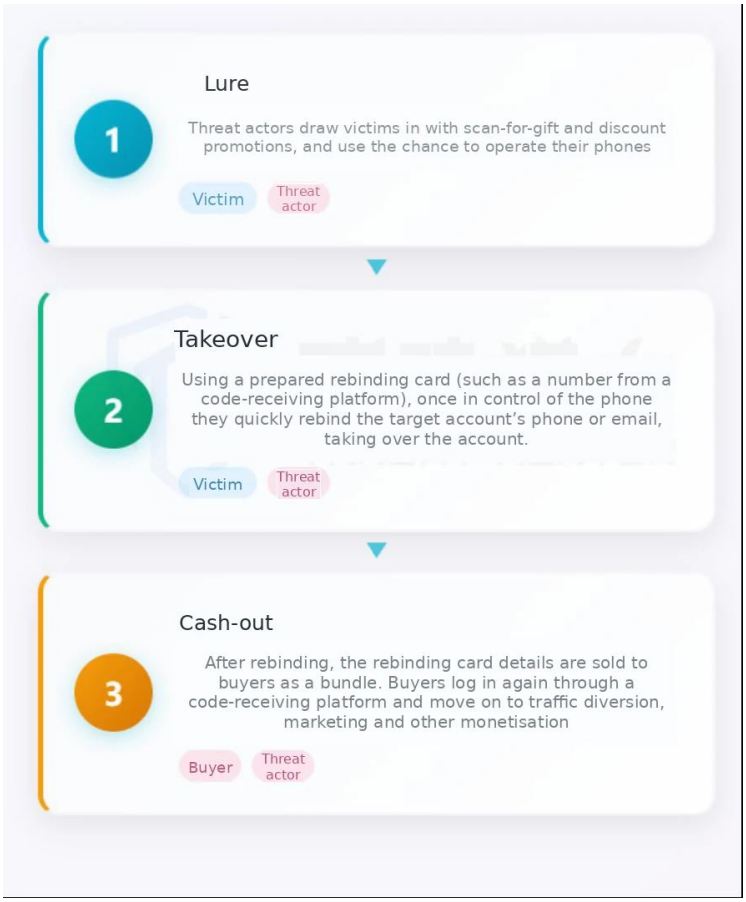
And use the card-binding resources in hand to change the phone number originally bound to the target app account;

3. threat actors use the newly linked phone number to log in to the account. At this time, the system may trigger new device fraud controls:

- If the original mobile phone verification code is required for verification: threat actors induce the victim to provide the SMS verification code
- If it is password verification: use a uniformly set weak password to complete the verification;

4. After confirming that they can log in normally, threat actors quickly sell their accounts and leave the stall location to find the next crowded place to continue.

Continue to cheat



How street-promotion account theft works

Source: Threat Hunter original report, page 47. Original figure with Chinese text replaced by English.

2. Local promotion and traffic + inducement to install Trojan Apps to achieve account theft. threat actors use online or offline promotion to induce victims to install Trojan Apps with words such as "scan the code to receive prizes" and "participate in activities", thereby silently extracting the user's login credentials (such as token, cookie, session_id, etc.) in the target App in the background, and uploading them to the threat actors server in real time. This method is called "parameter extraction" in the industry, which is the abbreviation of "parameter extraction". In essence, it bypasses traditional password verification and directly reuses the user's login session to achieve remote cloning login. After obtaining the credentials, threat actors can use tools such as account adders and simulators to restore the account usage environment and perform batch login, automated operations and monetization. This type of account is usually sold in the form of "data account", which can be logged in directly without verification, and can easily be used by threat actors such as traffic manipulation traffic, diverting traffic, and promoting.

The picture below shows the QR code provided by threat actors upstream to the midstream local promotion team. The local promotion personnel only need to ask users to scan the QR code and their account login credentials will be stolen.



Screenshot of a QR-code login tool

Source: Threat Hunter original report, page 48. Original image retained.

The picture below shows the software interface used by upstream threat actors. Every time a midstream local pusher successfully tricks a user into scanning a code or downloading an app, their login data credentials will be sent back to the backend and displayed in the software. threat actors can export data in batches for sale. Detailed explanation of the threat actors operation link:



Screenshot of an account login tool

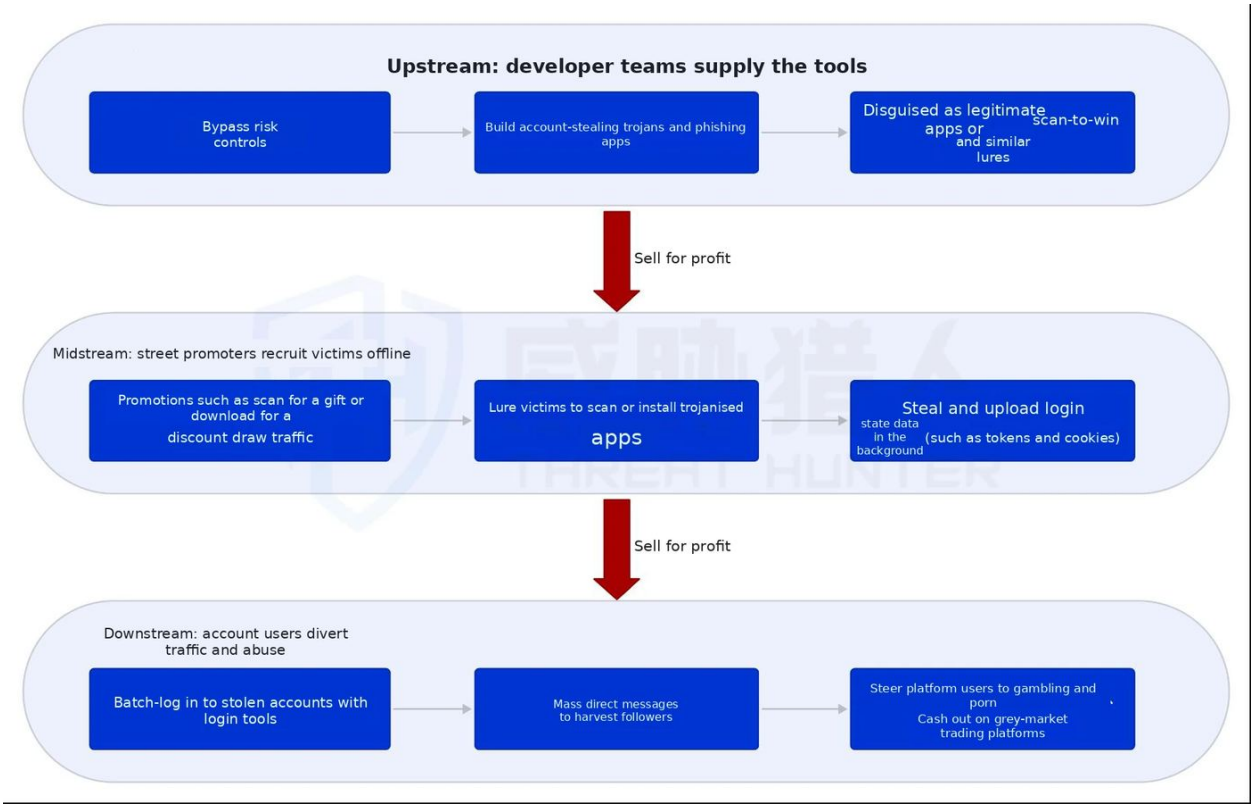
Source: Threat Hunter original report, page 48. Original image retained.

1. threat actors attract passers-by to participate in activities on the streets through methods such as "scanning QR codes to send gifts" and "inviting new people to receive red envelopes".

2. Local promoters guide users to complete one of the following behaviors under "social induction":

- Download a Trojan app with a reference function (usually disguised as an event app or discount tool). After the app is installed, it runs silently in the background and captures the login credential data of the target app;
- Scan the code to log in to the phishing page: local pushers present the QR code to induce users to scan the code to log in with an app, and extract their login credentials through interface monitoring or cache hijacking;
- Inducing verification codes: Lie that identity verification is required and trick users into providing SMS verification codes. threat actors use this to log in to their accounts and simultaneously extract token and other parameters.

3. Once successfully obtained, the login credential data will be uploaded to the threat actors backend server in real time



The street-promotion account-theft supply chain

Source: Threat Hunter original report, page 49. Original figure with Chinese text replaced by English.

3.1.2 Upgrading of the industrial chain of fraud gangs (1) Industrialization evolution path of fraud behavior

According to Threat Hunter's monitoring and analysis, e-commerce order fraud is undergoing a rapid evolution from "fragmentation" to "platformization" and "instrumentation". Early order fraud mainly relied on messaging-app groups, and released tasks in the "acquaintance + fish pond" model. Individual users received commissions and cashbacks by paying in advance to purchase goods. This method highly relies on human coordination, has cumbersome operations, high costs, and low efficiency. In recent years, the order traffic manipulation model has been significantly upgraded. cybercriminal groups develops and sells self-service order traffic manipulation tool systems, moving to a stage where merchants take the lead in the entire order traffic manipulation process.

Stage	Typical features	Organisation	Techniques
1. Scattered fake orders	Manual fake orders in chat groups	Individuals; part-time "fish pond" work	Manual, no technology
2. Transition to machine orders	Emulators and multi-instance tools partly automate fake orders	Script-using threat-actor groups	Emulators plus manual control
3. Fish-pond platforms	Small task-dispatch platforms appear	Small teams	Simple web pages and script tools
4. Systematic coordination	Fake-order platforms handle task scheduling, account screening and device coordination; the process becomes automated and modular	Factory-style operation; semi-automatic platform order taking	Platform tools, risk-control evasion, and account and device tagging

How fake-order operations have evolved

Source: Threat Hunter original report, page 50. Table re-typeset in English from the original.

(2) Upgrading of the order traffic manipulation industry: From the fish pond model to the merchant self-operated closed-loop, merchants can choose their own accounts, configure equipment, and remotely control the order traffic manipulation process through the order traffic manipulation platform developed by threat actors, achieving autonomous control from task initiation, order placing operations to data feedback. Hand traffic manipulation is no longer an important execution role. It only needs to perform the payment action. The whole process no longer relies heavily on manual docking, which greatly reduces the operating threshold and docking costs, and the efficiency and concealment of traffic manipulation orders are also greatly improved.

The current order-sharing ecosystem is no longer the extensive play method of "finding a few groups and completing a few tasks" in the past. Instead, it has completed an industrial-level leap in organizational structure, equipment resources, and execution methods. Threat Hunter summarizes its evolution path and shows three core upgrade trends:

1 Merchants take the lead in traffic manipulation orders, and the degree of realism is raised to the "operational level". Compared with the past, which was left to "hands who manipulate orders" to operate at will, more and more merchants are now beginning to build their own traffic manipulation plans and lead the execution strategy.

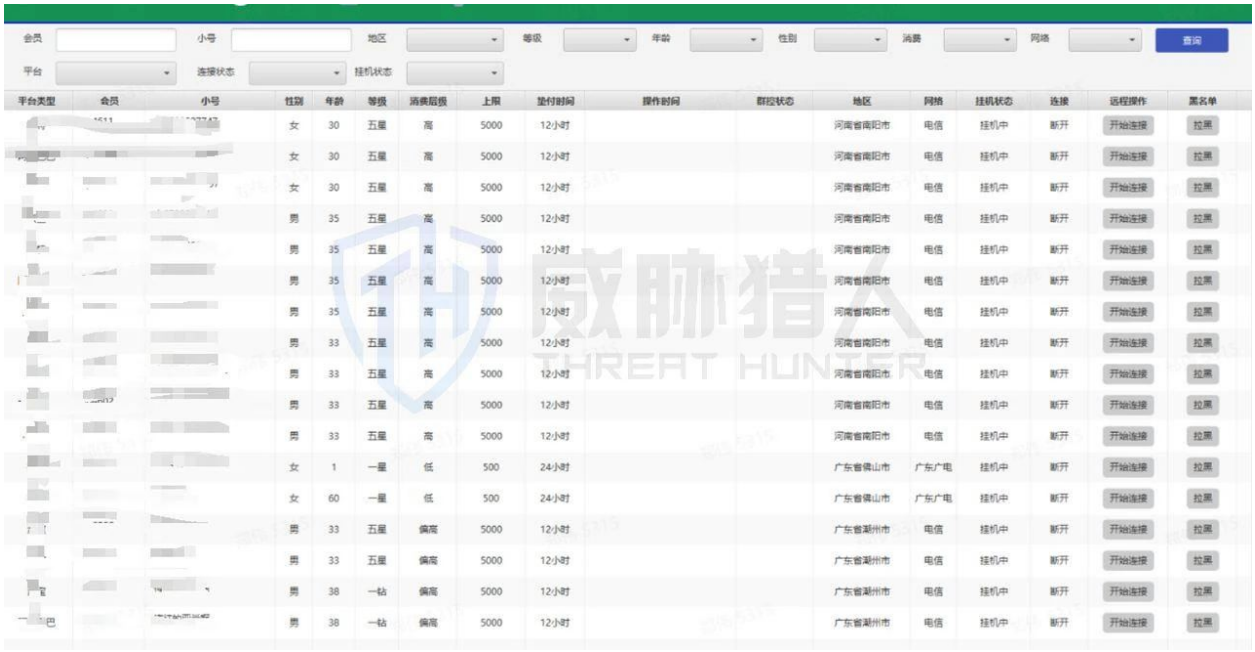
Merchants are well versed in platform traffic logic and know what kind of user behavior can bring real traffic and weight support, so they will:

- Accurately select equipment based on crowd portraits;
- Simulate the entire chain of behaviors such as searching, browsing, collecting, staying, placing orders, and evaluating;

- Combined with the needs of its own products in terms of conversion, additional purchase rate, repurchase and other operational indicators, make highly realistic task parameter configurations.

Result: traffic manipulation orders is no longer "swiping sales", but "swiping all indicators", which is almost real, and the difficulty of fraud-risk detection has increased sharply.

The picture below shows the software page for order traffic manipulation on the merchant side. You can connect the corresponding devices and platforms according to your actual needs. 2 Evolution of the threat actors equipment system: Tens of thousands of real traffic manipulation devices form an order traffic manipulation dispatch network. Behind the platform-based order traffic manipulation system is a real device network carefully constructed by threat actors. The platform has been connected to more than 40,000 real-swipe mobile phones and can be uniformly scheduled and used through remote control or on-hook systems. These devices:

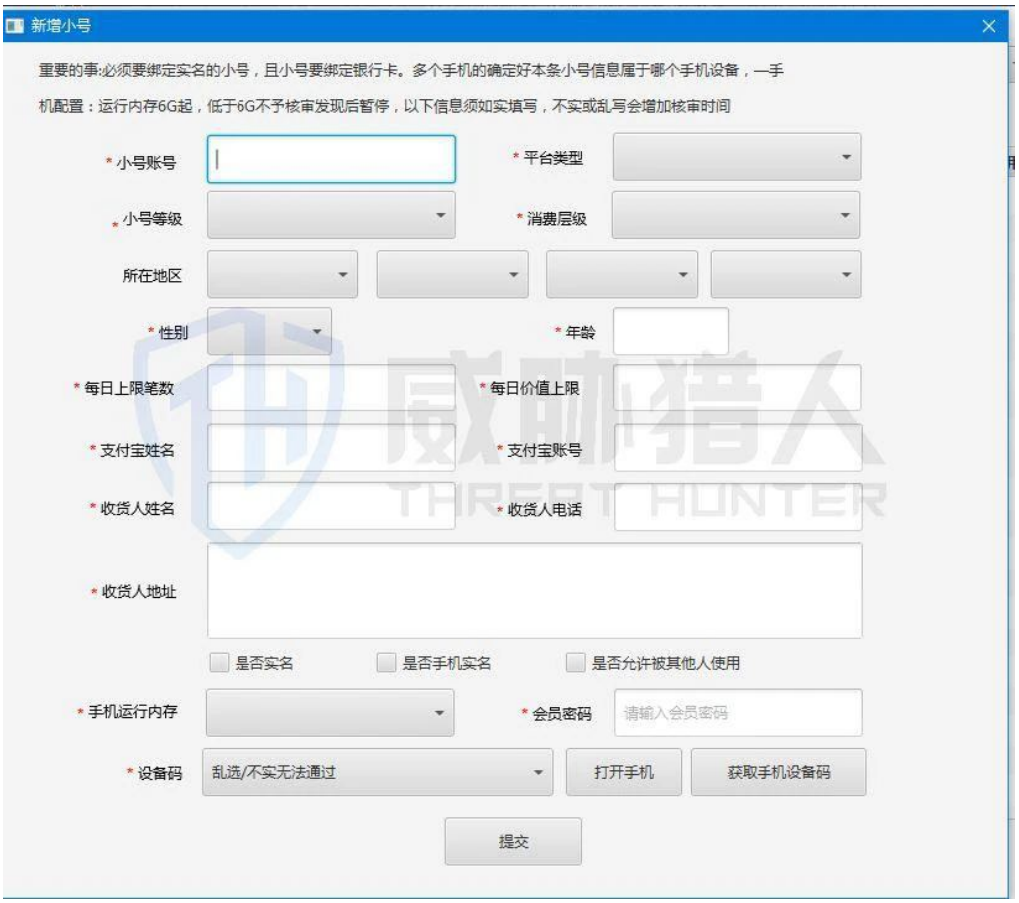


Screenshot of an account-hosting control panel

Source: Threat Hunter original report, page 51. Original image retained.

- It has a long-term use record, high weight and strong credibility;
- Be labeled with behavioral labels (such as region, gender, category preference);
- It is included in the order processing task scheduling system and can be accurately called according to the needs of merchants.
- Essence: Order traffic manipulation has changed from "manpower coordination" to "algorithm + equipment scheduling" and entered the stage of automated production.

The picture below shows the software page for configuring personal information before starting to hang up.



Screenshot of an account registration form

Source: Threat Hunter original report, page 52. Original image retained.

3. Transformation of traffic manipulation participation model: from "full process" to "light participation" In the traditional order traffic manipulation system, traffic manipulation needs to participate in the whole process from receiving tasks, browsing, placing orders, confirming, and evaluating, which is time-consuming and complex. In the current platform model:

- To swipe your hand, you only need to complete the "payment action" when prompted by the system, and there is no need to understand the entire task;
- The platform systematically allocates tasks and automatically operates equipment. You only need to rent your account and equipment to earn profits;
- The threshold for participation is lowered and operating pressure is reduced, attracting a large number of ordinary users to "part-time job traders" and providing massive underlying execution resources for threat actors.
- Trend prediction: As the platform functions become more and more perfect and the reward mechanism is simplified, more and more brushers will join the platform in the future, and the manpower for traffic manipulation orders will gradually become platform-based and pan-professional.

The picture below shows the idle page of the mobile phone:



Screenshot of an order manager tool

Source: Threat Hunter original report, page 53. Original image retained.

3.1.3 The navy industry changes from public opinion interference to commercial competition attack

With the continuous evolution of cybercrime ecosystem organizations, the manipulation behavior of trolls is no longer limited to simple traffic manipulation operations, but has been used in scenarios such as business suppression, content control and review, and hot spot diversion. Tasks are usually released centrally through groups or small crowdsourcing platforms, covering public opinion manipulation operations such as "likes, comments, forwarding, and controlling comments." The navy performs tasks according to preset requirements and submits feedback materials such as screenshots. The entire process is highly concealed and responsive, forming a complete closed loop from task initiation to fund settlement.

(1) The order-taking mode and docking method of navy tasks The distribution method of navy tasks has formed a diversified structure, which is mainly completed through three types of paths: community channels + crowdsourcing platforms + private execution groups.

In order to ensure the execution rate and uniformity of tasks, the navy organization has systematically designed the task docking process. The task issuer no longer communicates directly with all navy forces, but accurately transmits operational requirements to a stable execution group through specific channels. Task docking usually has the following characteristics:

- There are clear requirements for comments or pictures;
- There are execution time windows or interaction rules;
- Have screenshots or account IDs as task feedback credentials;
- There is a unified recycling, review and settlement process (2) Catching commercial brand trolls to smear the case 1 Private domain channels recruit trolls to manipulate negative reviews to guide public opinion attacks



Screenshots of a paid-commenter channel

Source: Threat Hunter original report, page 54. Original image retained.

A set of screenshots of chat records were intercepted, showing that an organizer recruited trolls through social media and carried out targeted comments to attack a well-known domestic car company. The tasks include posting provocative comments and copy-pasting content to create negative reviews. A large number of accounts are used to publish unified negative review content in the comment area of □□specific social platform posts to create product controversy, create negative public opinion about quality, and guide the public to question the brand.

1. Clear mission statement

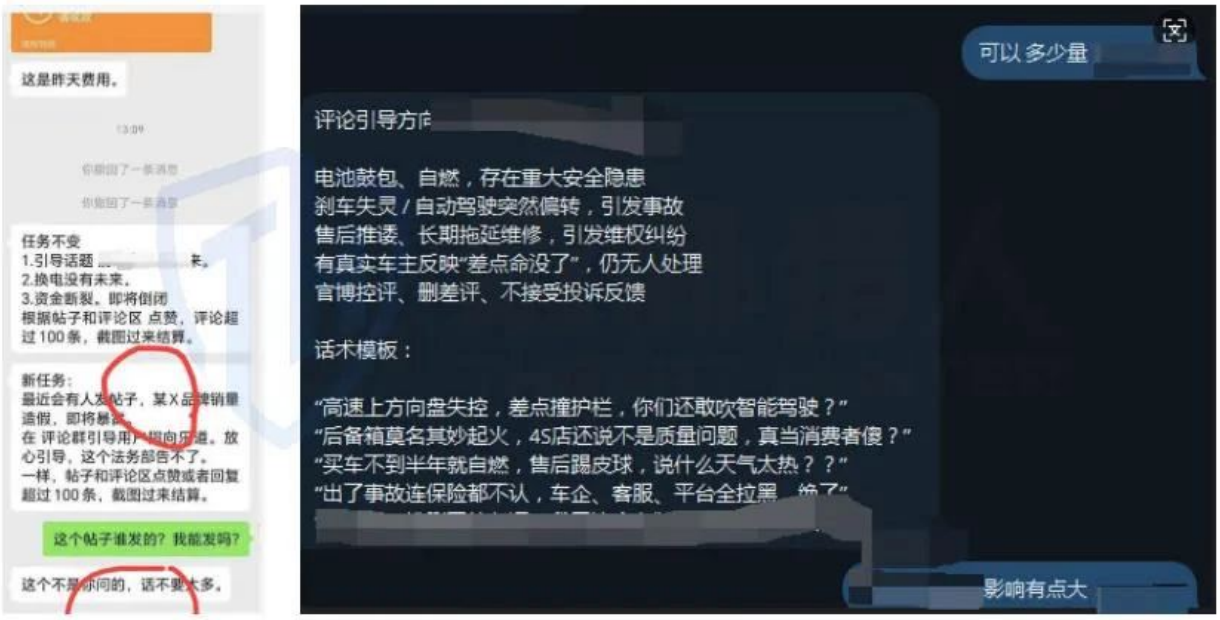
- Keywords such as guidance topics, power exchange disputes, and capital breaks have been preset;
- When the number of comments/likes exceeds 100, settlement will occur, and the execution threshold is low;
- Clarify "screenshot postback" as the verification mechanism.

2. Provide negative review content in batches

- The recruiter provides a unified copywriting and requires the navy to copy and paste directly;
- The price of each comment is 0.5 yuan, billed based on volume;
- Comments contain fabricated facts, exaggerated accusations, and counterfeit technicians' perspectives to enhance "authenticity."

3. Implement intra-group control

- It is prohibited to inquire about the source of the task or the identity of the poster;
- Emphasis on “don’t talk too much” and clearly intends to isolate information;
- A closed loop of “one-way order issuance + screenshot settlement” is formed within the group.



Screenshots of a smear-campaign brief

Source: Threat Hunter original report, page 56. Original image retained.

2 Crowdsourcing channels recruit trolls to write negative reviews and guide public opinion attacks. According to monitoring, threat actors or marketing groups organize trolls to perform targeted comment tasks through crowdsourcing platforms, with the intention of manipulating public opinion on short video platforms and guiding users to have negative perceptions of target brands or products. Such tasks often use "likes + comments" + "negative guidance" as the core operations, hiring a large number of trolls to speak in the comment area, presenting the illusion of "real users complaining", but behind the scenarios are carefully planned emotional manipulation behaviors.

Mission goal: Enter the designated video, post comments with a derogatory tone, and guide public opinion to pay attention to brand issues (such as poor battery life, false product labels, poor after-sales, etc.).

Comment method: first comment + supplementary comment mode, that is, the first troll publishes the main comment, and subsequent accounts will like, interact and spread.

Example phrases:

- “Whoever buys it will regret it, the battery life is ridiculously short”
- “I almost couldn’t stop the last time, the battery is really bad”
- “The quality is really not complimentable”



Screenshots of a comment-posting task

Source: Threat Hunter original report, page 57. Original image retained.

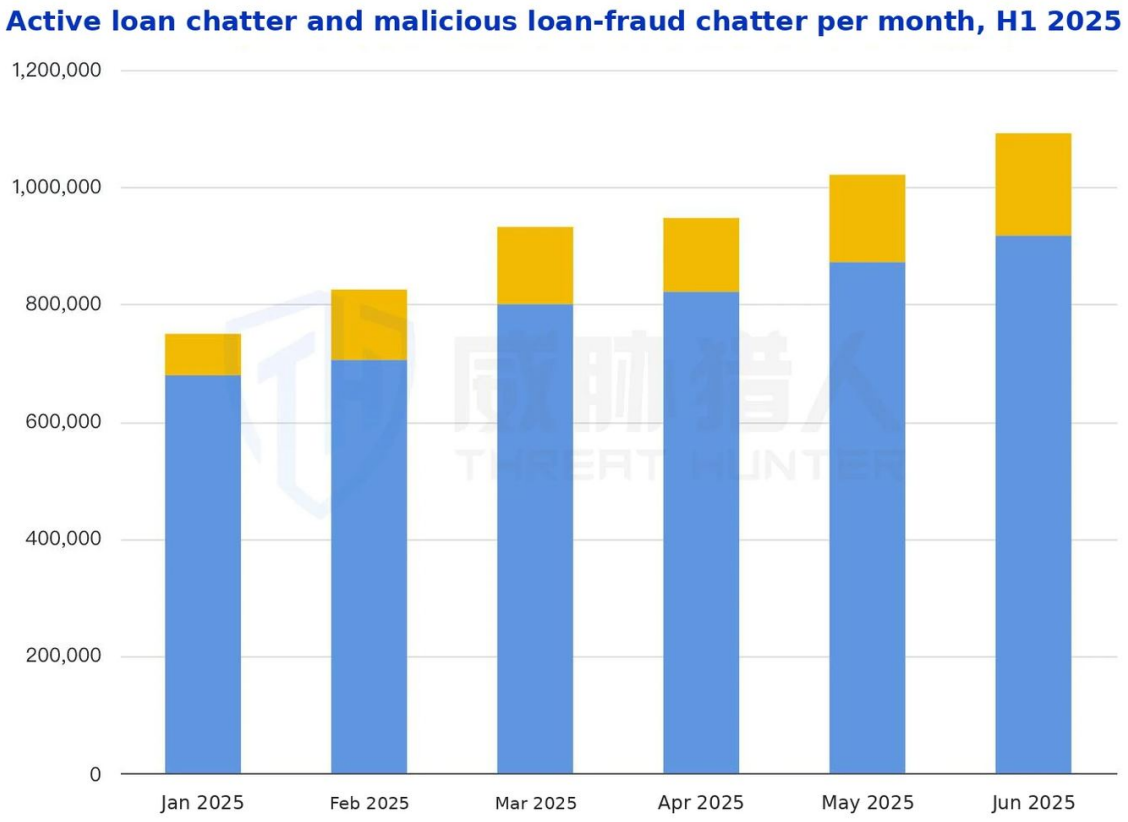
3.2 Analysis of financial fraud scenarios

In the financial fraud scenario, financial loan risk public opinion and credit channel intermediary dynamics have received widespread attention from banks and other financial institutions. The hidden malicious loan risk public opinion is an important source of intelligence for identifying and judging credit fraud, and then adjusting fraud-control strategies.

Malicious loan fraud: refers to various types of illegal loan activities carried out by financial practitioners or groups of threat actors for the purpose of illegal profit-making through false propaganda, forged materials, inducement and deception, etc. Its typical behaviors include: taking on debts, cashing out cars, raising technology quotas, fraud on beauty loans, debt restructuring, AB loans, making fake statements, credit repair, debt optimization and other illegal businesses for personal gain.

3.2.1 In the first half of 2025, malicious fraud attacks on financial loans will continue to increase and remain serious (1) Public opinion on malicious fraud on financial loans and the scale of cybercrime ecosystem continue to expand

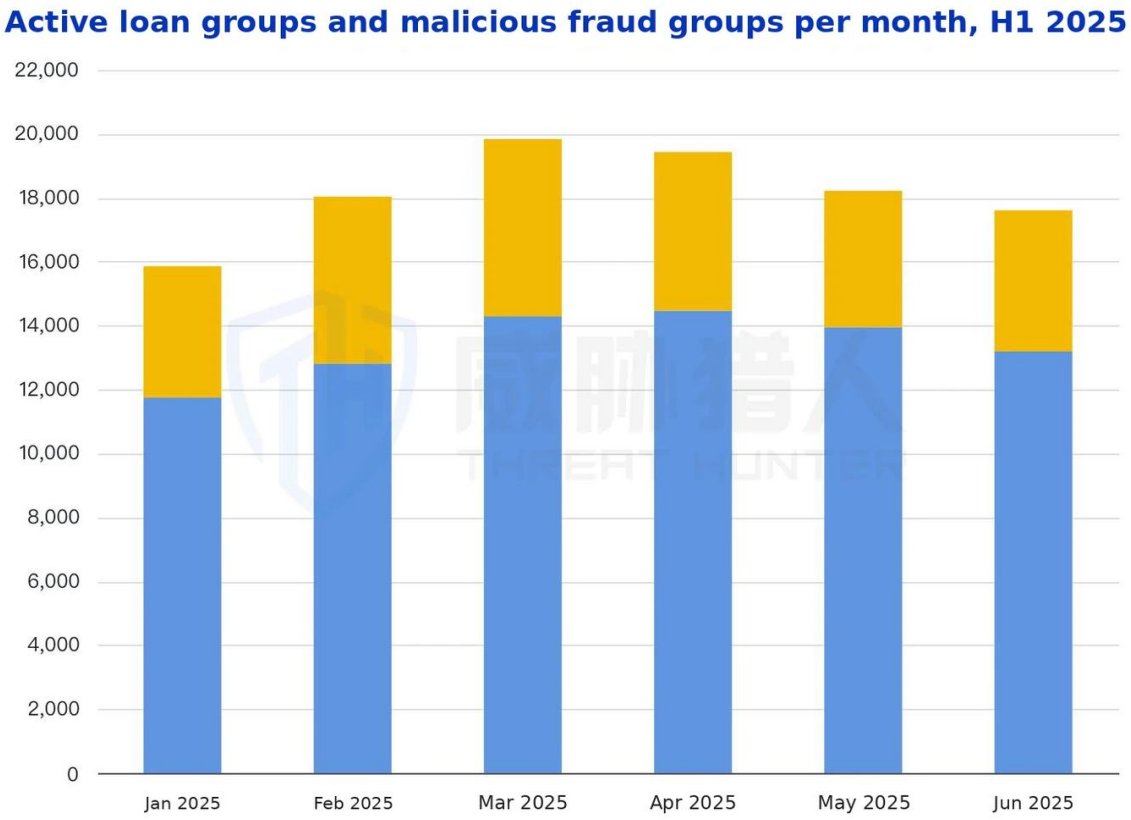
In the first half of 2025, Threat Hunter monitored and captured 4.79 million public opinions on financial loan risks, of which 770,000 were malicious loan fraud public opinions, accounting for 16% of the total. Financial loan risk public opinions decreased by 14% compared with the second half of 2024, and malicious loan fraud public opinions increased by 12% compared with the second half of 2024. The monthly risk public opinion trends show continued growth.



Active loan chatter and malicious loan-fraud chatter per month, H1 2025

Source: Threat Hunter original report, page 58. Original figure with Chinese text replaced by English.

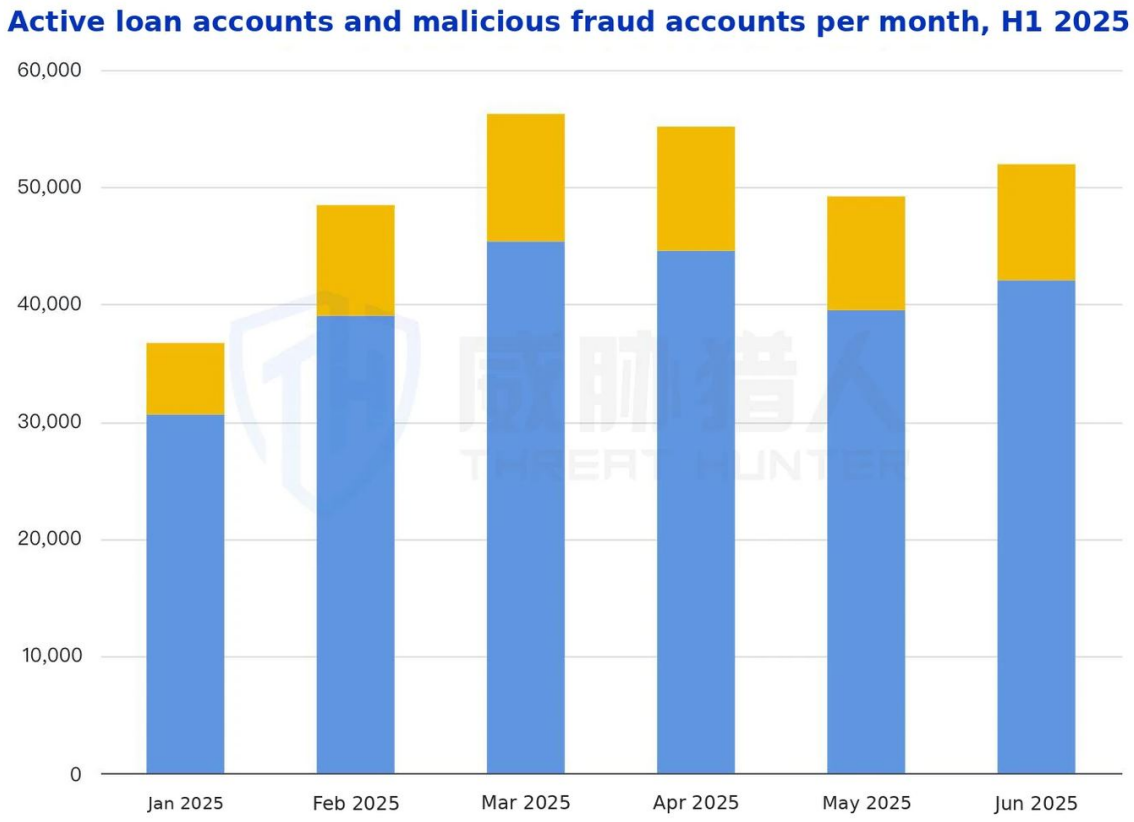
In the first half of 2025, Threat Hunter monitored 33,000 active loan groups, including 13,000 malicious fraud groups, accounting for 39% of the total. Active loan groups decreased by 4% compared with the second half of 2024, and malicious fraud groups increased by 5% compared with the second half of 2024.



Active loan groups and malicious fraud groups per month, H1 2025

Source: Threat Hunter original report, page 58. Original figure with Chinese text replaced by English.

In the first half of 2025, Threat Hunter monitored and captured 118,000 active loan service accounts, of which 35,000 were fraudulent accounts (credit black intermediaries/threat actors) providing malicious loan services, accounting for 29.6% of the total, an average increase of 6% from the second half of 2024.

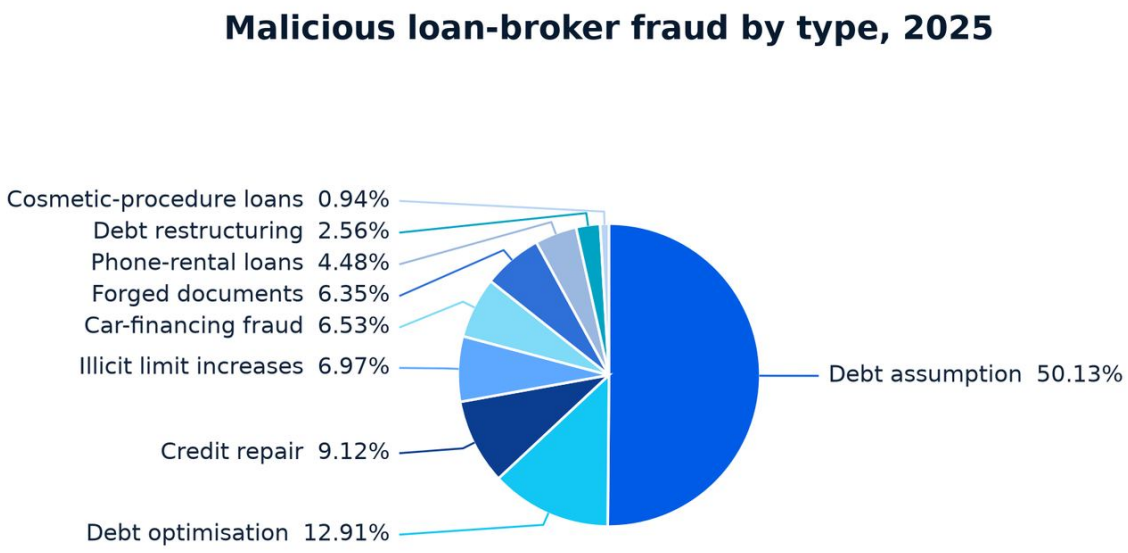


Active loan accounts and malicious fraud accounts per month, H1 2025

Source: Threat Hunter original report, page 59. Original figure with Chinese text replaced by English.

(2) Main fraud types of malicious loans in the first half of 2025 top 3: professional debt, debt optimization, credit repair. Data in the first half of 2025 shows that malicious loans mainly involve more than 9 types of fraud, such as professional debt, debt optimization, credit repair, illegal quotation, car financing fraud, material forgery, etc., of which professional debt accounts for up to 50%, ranking first, becoming underground The core attack methods of actors; debt optimization and credit repair ranked second and third respectively, and the related agency complaint business still maintains a high level of activity.

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

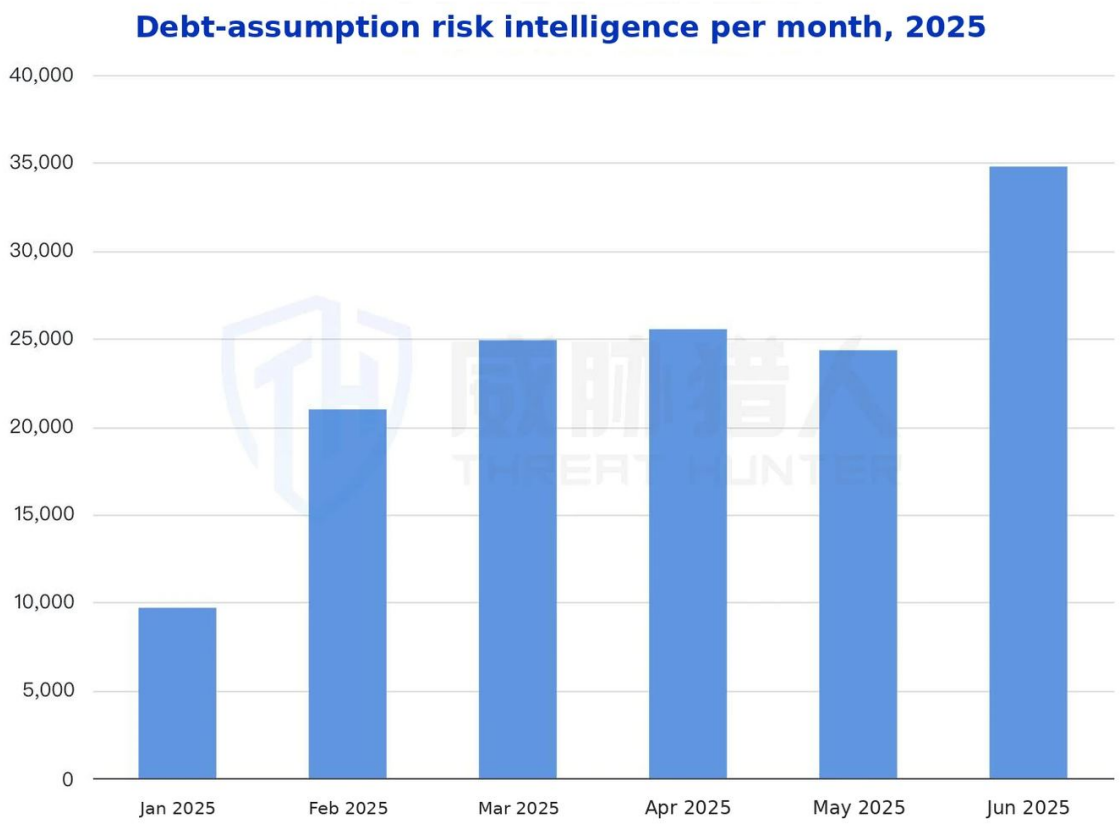


Malicious loan-broker fraud by type, 2025

Source: Threat Hunter original report, page 59. Redrawn in English from the original figure.

3.2.2 The current risk level of professional debt is expanding, and defense pressure continues to rise

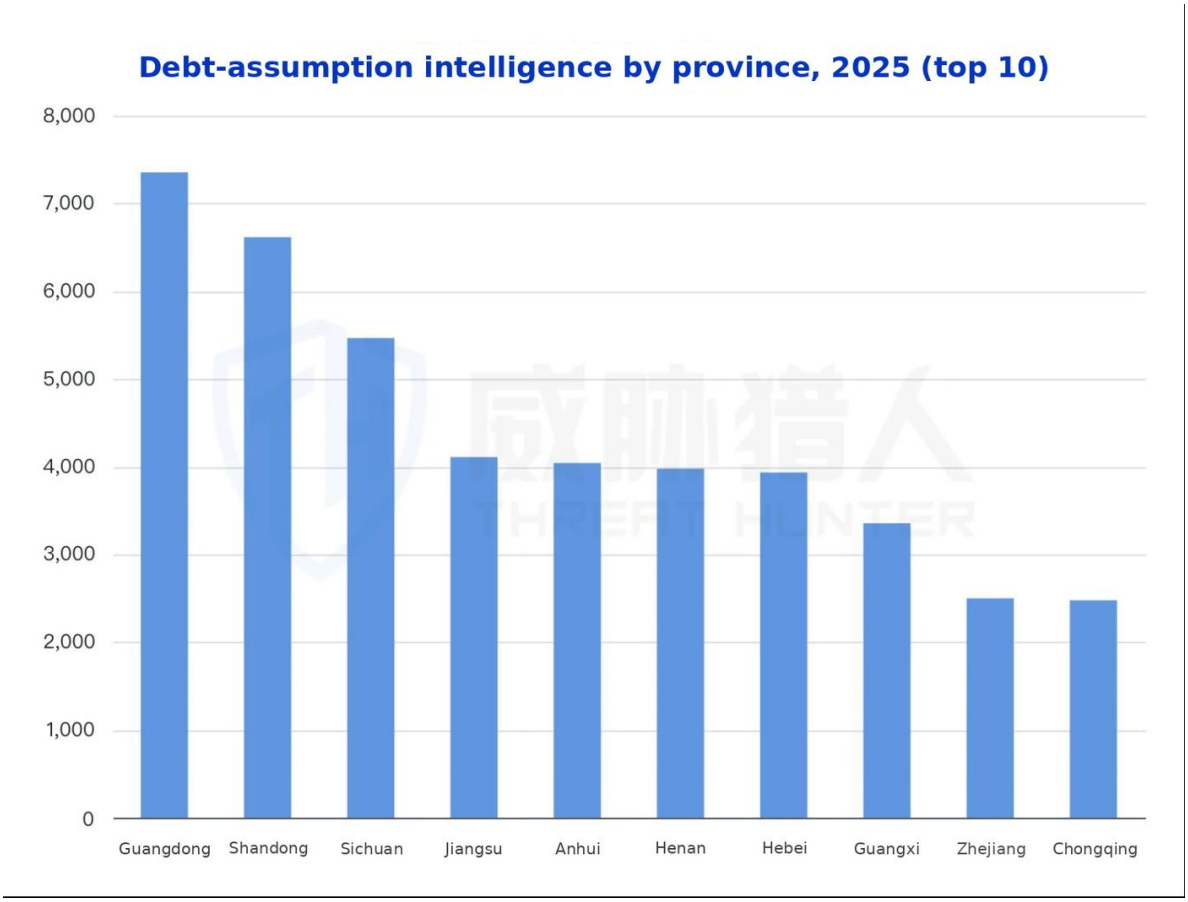
(1) The popularity of professional debt-taking has increased, and it has become the regular main business of cybercrime ecosystem. The capture of "debt-related" attack intelligence is on the rise in the first half of 2025. The popularity of debt-taking has increased, with an increase of 65% in the first half of 2025 compared with the second half of 2024. Professional debt-taking has become the regular main business of cybercrime ecosystem, and its spread is getting wider and wider.



Debt-assumption risk intelligence per month, 2025

Source: Threat Hunter original report, page 60. Original figure with Chinese text replaced by English.

(2) The top three most popular provinces for debt-incurring regions in the first half of 2025: Guangdong, Shandong, and Sichuan. Threat Hunter intelligence data shows that in the first half of 2025, the top three active provinces (including municipalities) for “debt-incurring” related loan fraud are Guangdong, Shandong, and Sichuan.

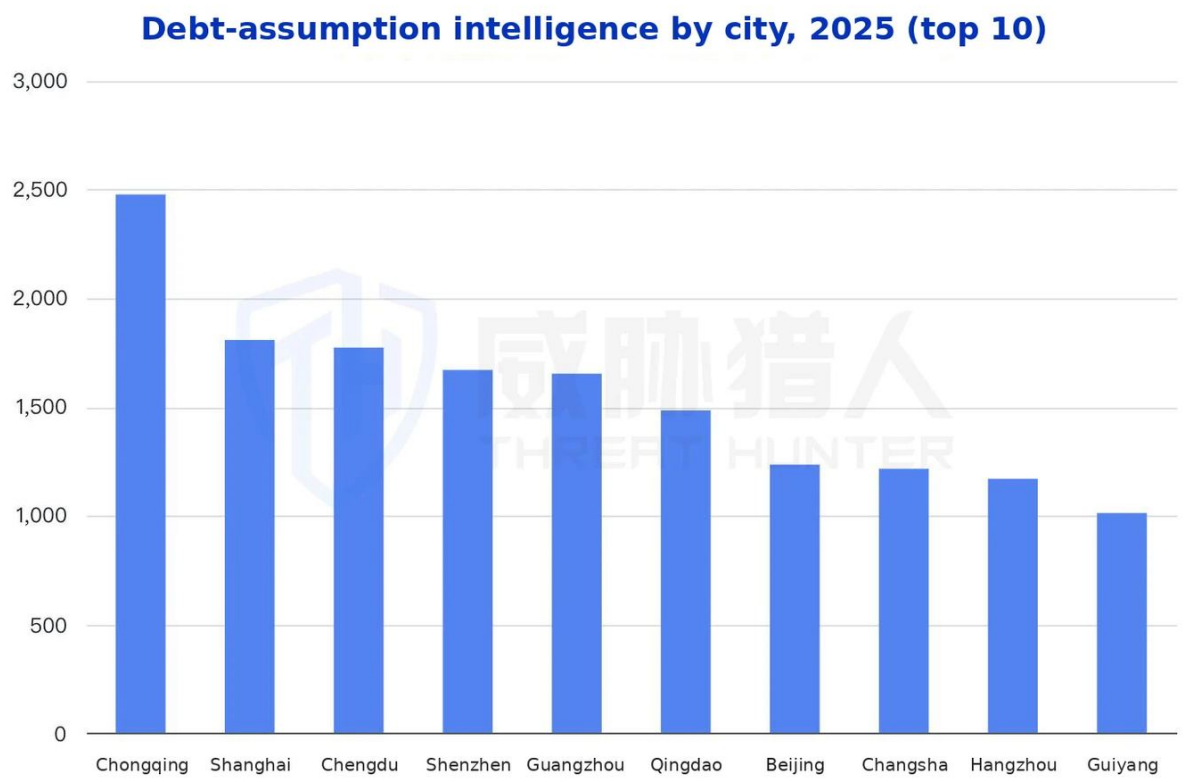


Debt-assumption intelligence by province, 2025

Source: Threat Hunter original report, page 60. Original figure with Chinese text replaced by English.

(3) Top 3 cities with debt in the first half of 2025: Chongqing, Shanghai, Chengdu

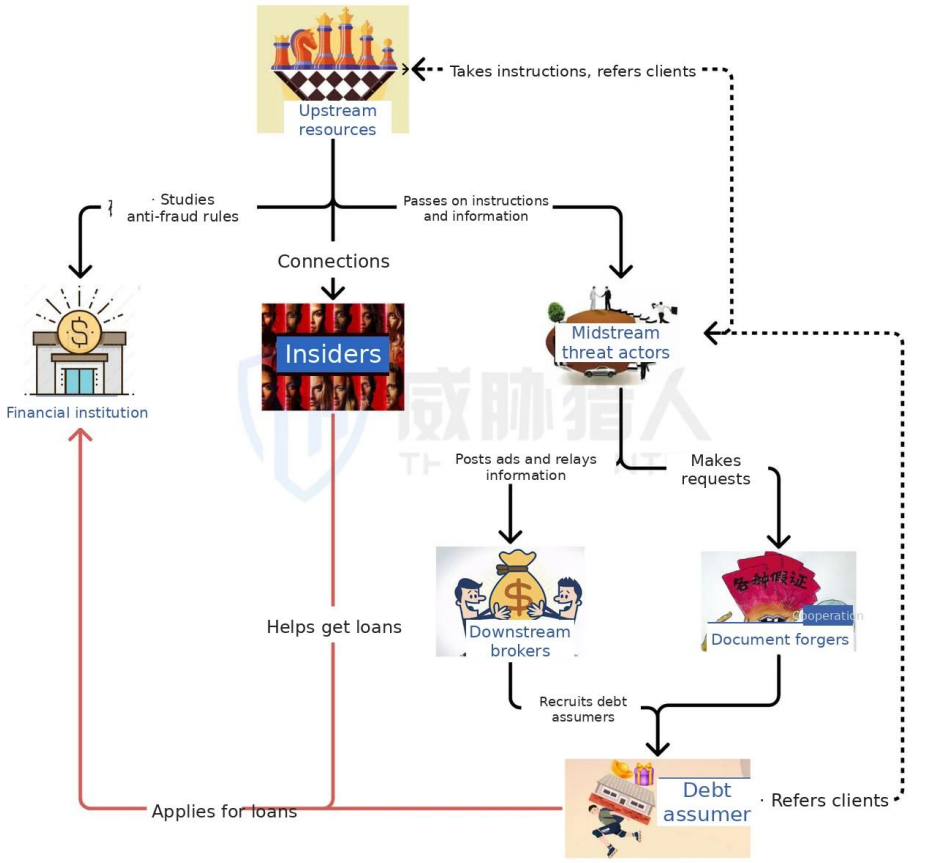
Threat Hunter intelligence data shows that in the first half of 2025, the top three most active cities (including municipalities) for loan fraud related to "debt incurrence" are Chongqing, Shanghai, and Chengdu.



Debt-assumption intelligence by city, 2025

Source: Threat Hunter original report, page 61. Original figure with Chinese text replaced by English.

(4) Analysis of the multi-role industry chain of professional debt-bearing The current chain of underground debt-bearing actors has formed a sophisticated division of labor system, showing highly specialized features from qualification packaging, loan fraud operations to debt transfer. The roles of debt-bearing threat actors are mainly divided into four roles: upstream resource layer, midstream threat actors, downstream intermediaries, and fake material production threat actors. Together with the "insiders" and debtors who collude internally and externally, they form a multi-party illegal benefit chain with clear division of labor and interlocking links.



How the debt-assumption chain works

Source: Threat Hunter original report, page 61. Original figure with Chinese text replaced by English.

(5) Corporate loans become the biggest risk point for incurring debt. Threat Hunter conducted in-depth research on debt risk scenarios and found that housing loans, credit, car loans and corporate loans show differentiated risk characteristics:

Car loans are prone to liquidation of assets and short disposal chains, with rapid risk exposure and obvious fraud characteristics; mortgage loans have strong hidden risks due to the characteristics of collateral credit enhancement and long disposal cycle; corporate loans have obvious lag due to repayment methods such as "interest first, principal later" and "loan renewal without principal", which often accumulate to the stage of concentrated outbreak.

The current debt matching model of threat actors is mainly a combination of combinations, such as the common combination models of real estate credit companies, real estate companies, credit companies, automobile companies, housing credit car companies, etc. Different fraudulent loan matching models depend on the basic situation of the debtor and the channel resources of threat actors.

The following is a special analysis of the core operating links and risk characteristics of professional debt-bearing threat actors in the four types of loan scenarios: housing loans, credit, car loans, and corporate loans. Corporate loans are crucial in the debt-carrying link and have become the biggest risk point for financial institutions in the current professional debt-carrying risk scenario.

The importance of the debt link refers to the function and frequency of utilization of a certain loan scenario in the cybercrime ecosystem debt chain, which comprehensively reflects its impact on the success or failure of the entire chain. The higher the importance, the more critical the link is in the

chain. It may be the main source of funds for threat actors to arbitrage, or it may be a key point in asset credit enhancement.

For financial institutions, highly important loan products usually face higher frequency of fraud attacks and more complex control paths, reflecting more exploitable business vulnerabilities, greater difficulty in prevention and control, and greater fraud-control pressure.

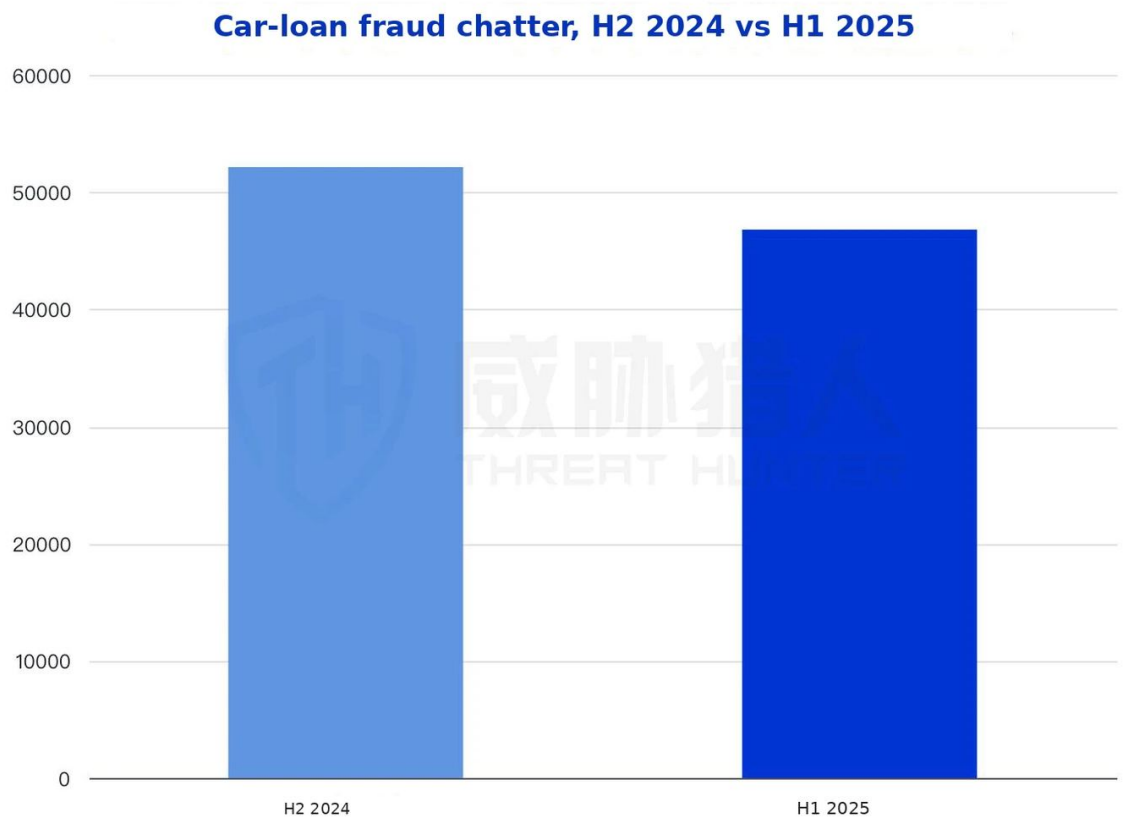
Scenario	Loan types involved	Importance in debt assumption	Role in debt assumption	Risk signs
Business loans	Tax-invoice loans, operating loans	Critical	The core of debt assumption and main source of profit (high limits)	Mostly limited companies and sole traders Genuine operations mixed with inflated data Many loans, many times Usually the last loan taken in debt assumption
Mortgages	Mortgage loans, secured property loans	Very important	Builds up assets and credit for later loans	Second and third charges after a mortgage Developers cash out new homes through nominees One person, many loans Often the first loan in debt assumption
Car loans	Car loans, secured car loans	Important	Low bar, fast cash-out, short cycle	One person or one car, many loans Second and third charges after a car loan, then cash-out Cars disposed of illegally, often blowing up Can be the first loan in debt assumption
Credit loans	Renovation loans, consumer loans	Important	The main source of "upfront costs" for later business loans	Credit or renovation loans one month after the first mortgage repayment Consumer loans can be the first loan in debt assumption
Farmer loans	Farmer loans	Moderately important	Optional, but sometimes used	Rural household status used to borrow against land and fixtures Planting and livestock

The role of each loan scenario in debt assumption

Source: Threat Hunter original report, page 62. Table re-typeset in English from the original.

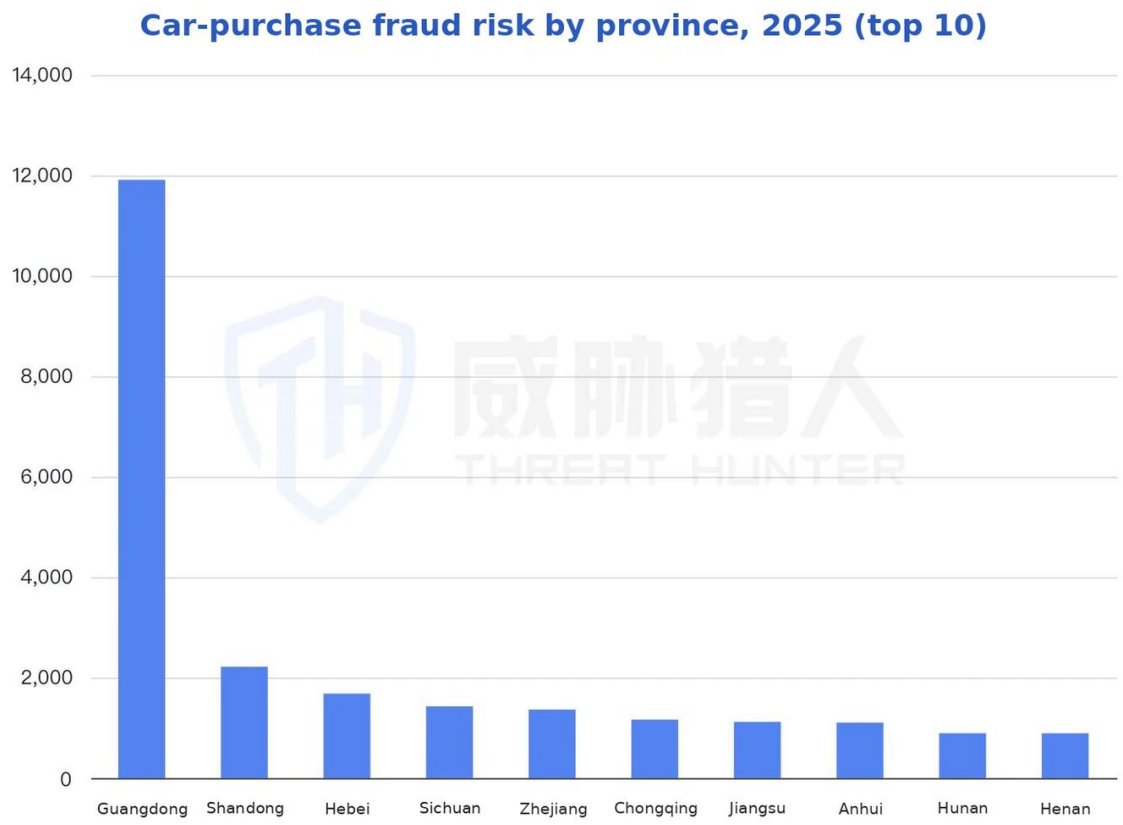
3.2.3 Car loan fraud risk: analysis of threat actors chain and regional situation warning

(1) The risk of car purchase fraud has fluctuated in the first half of 2025, and has dropped by 10% in the first half of 2025 compared with the second half of 2024. (2) Top 3 risk areas for car purchase fraud in the first half of 2025: Guangdong, Shandong, and Hebei. The area with the highest risk of car purchase fraud in the first half of 2025 is Guangdong Province, and it is much higher than other provinces. After in-depth analysis, the high risk of car purchase fraud in Guangdong Province is mainly due to the regional proliferation of new car financing and cash-out models, while this type of model is rarely used in other regions. This model has two salient features: first, it accurately selects users with real car-buying qualifications (good credit, stable income) and financial needs; second, it improves concealment by "emphasizing real qualifications and light packaging for fraud".



Car-loan fraud chatter, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 63. Original figure with Chinese text replaced by English.



Car-purchase fraud risk by province, 2025

Source: Threat Hunter original report, page 63. Original figure with Chinese text replaced by English.

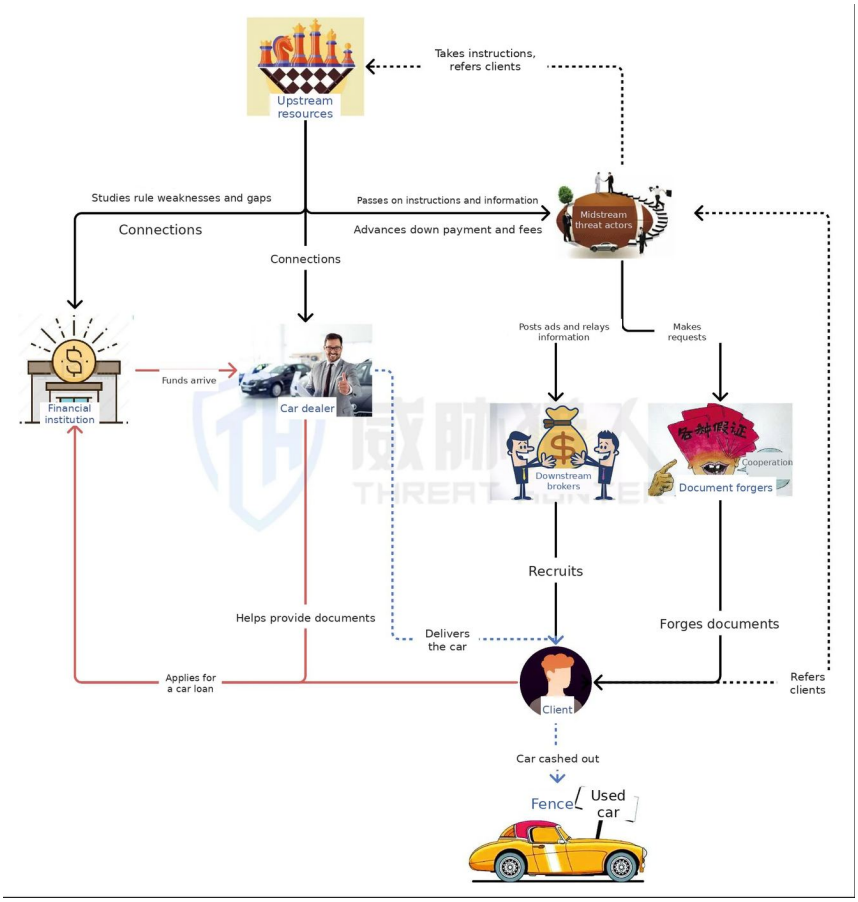
(3) Top 3 cities with car purchase fraud risks in the first half of 2025: Shenzhen, Chongqing, and Guangzhou (4) Car purchase fraud threat actors chain analysis Car purchase fraud has formed a set of threat actors operating models with clear division of labor, clear processes, and interlocking operations. From screening target groups, recruiting customers to purchase cars with loans, and quickly monetizing vehicles, threat actors have built a complete operation chain of threat actors, showing a high degree of organization and maturity.



Car-purchase fraud risk by city, 2025

Source: Threat Hunter original report, page 64. Original figure with Chinese text replaced by English.

(5) The model of car loan threat actors is solidified but risks continue to be high. There are many types of risks in the car loan business, including car financing and cashing out, MLM car purchases, top-notch cars, and car purchase packages. Among them, the risk of car financing and cash-out poses the most prominent threat.



How the car-loan fraud chain works

Source: Threat Hunter original report, page 64. Original figure with Chinese text replaced by English.

The following is the risk performance of each fraud risk model in the car loan scenario:

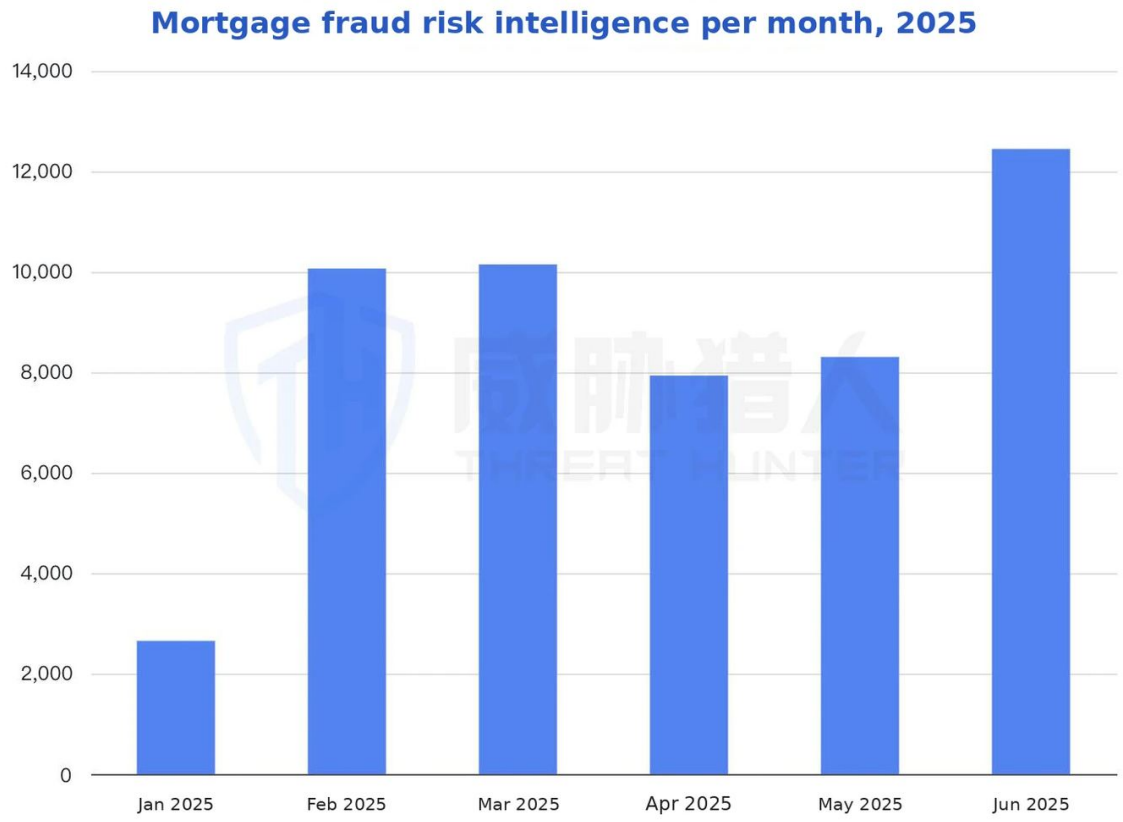
Risk pattern	Risk signs	Purchase intent	Risk level
Car-financing cash-out	One person or one car, many loans Wants money, not the car: the car is sold at once Part of the debt-assumption chain	Cash out for funds	Very high
Pyramid-scheme car purchases	Buyers are members of a pyramid scheme The scheme lures with "consumer points", "zero down payment" and "low monthly payments" Lower-level members buy cars on instalments The "discount" is tied to high spending	Genuine use	High
Nominee cars	One person, many loans Paid to buy a car in their own name for a third party The third party claims "genuine use" but resells the car to cash out	Paid nominee purchase	High
Car-for-job schemes	A job is offered on condition of buying a car, trapping people in instalment purchases; high-paid driver jobs are advertised to get drivers to buy on instalments The promised job does not match reality and the buyer is cheated	Buying a car to get a job	High

Car-loan fraud risk patterns

Source: Threat Hunter original report, page 65. Table re-typeset in English from the original.

3.2.4 Mortgage fraud risks will continue to grow in the first half of 2025

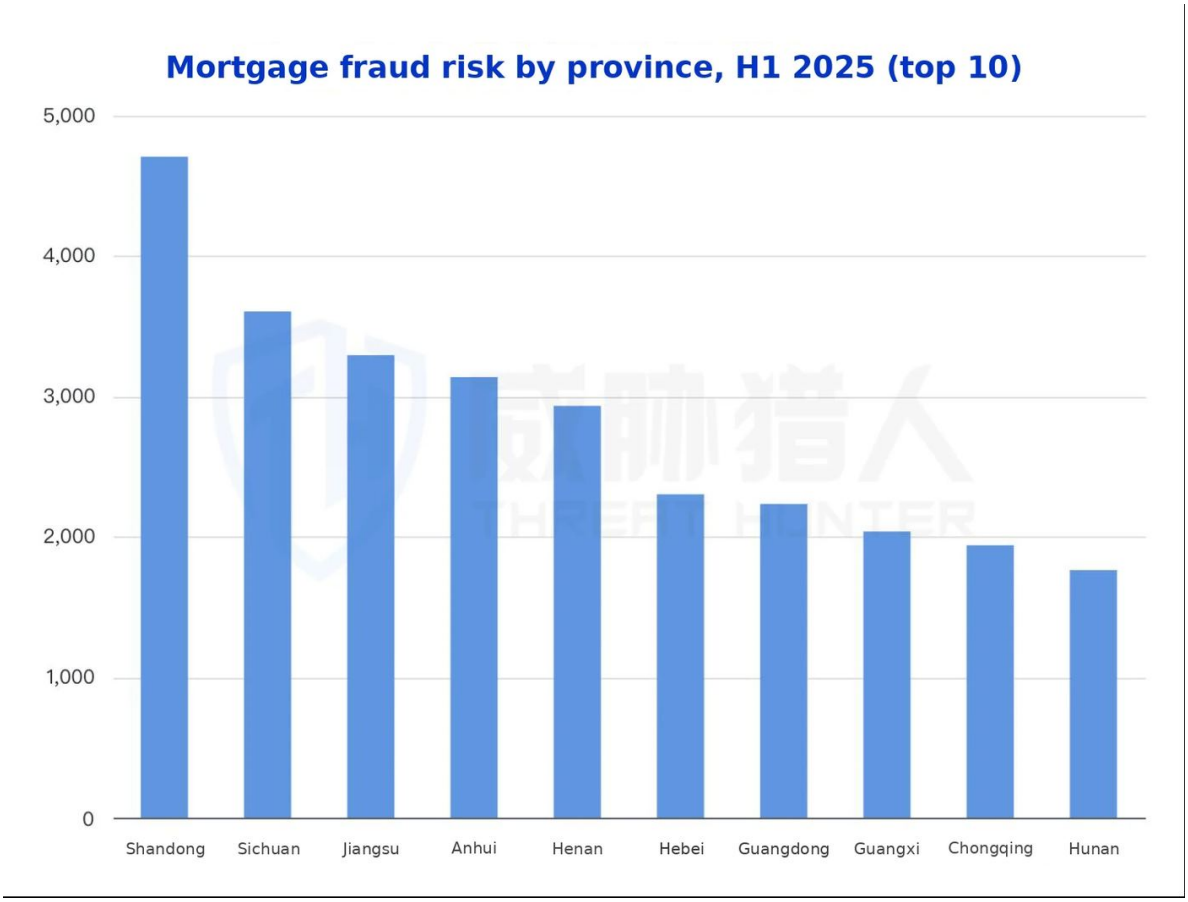
(1) Mortgage fraud risks will continue to grow in the first half of 2025, with an increase of 63% in the first half of 2025 compared with the second half of 2024



Mortgage fraud risk intelligence per month, 2025

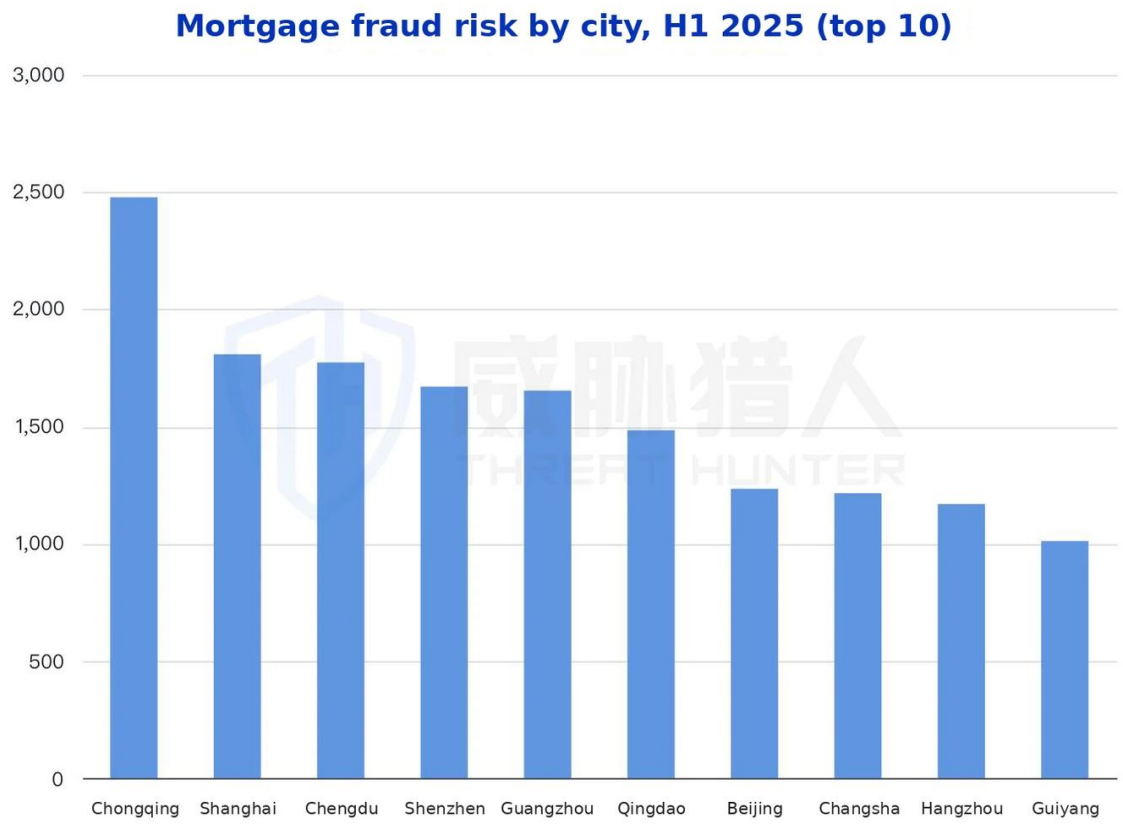
Source: Threat Hunter original report, page 65. Original figure with Chinese text replaced by English.

(2) Top 3 mortgage fraud risk areas in the first half of 2025: Shandong, Sichuan, Jiangsu (3) Top 3 mortgage fraud risk cities in the first half of 2025: Chongqing, Shanghai, Chengdu (4) Mortgage fraud risk types In the home purchase fraud risk scenario, risks are concentrated in two core fraud types. The first is home purchase mortgage loan fraud, where buyers purchase a home for non-real living needs, with the fundamental purpose of financing the home for cash or as an asset to increase debt and credit; the second is real estate mortgage loan fraud, such as common operating mortgage loans, loan-to-loan exchange, debt financing, etc. In these two types of housing loan scenarios, those who actually apply for loans face relatively large financial resources.



Mortgage fraud risk by province, H1 2025

Source: Threat Hunter original report, page 66. Original figure with Chinese text replaced by English.



Mortgage fraud risk by city, H1 2025

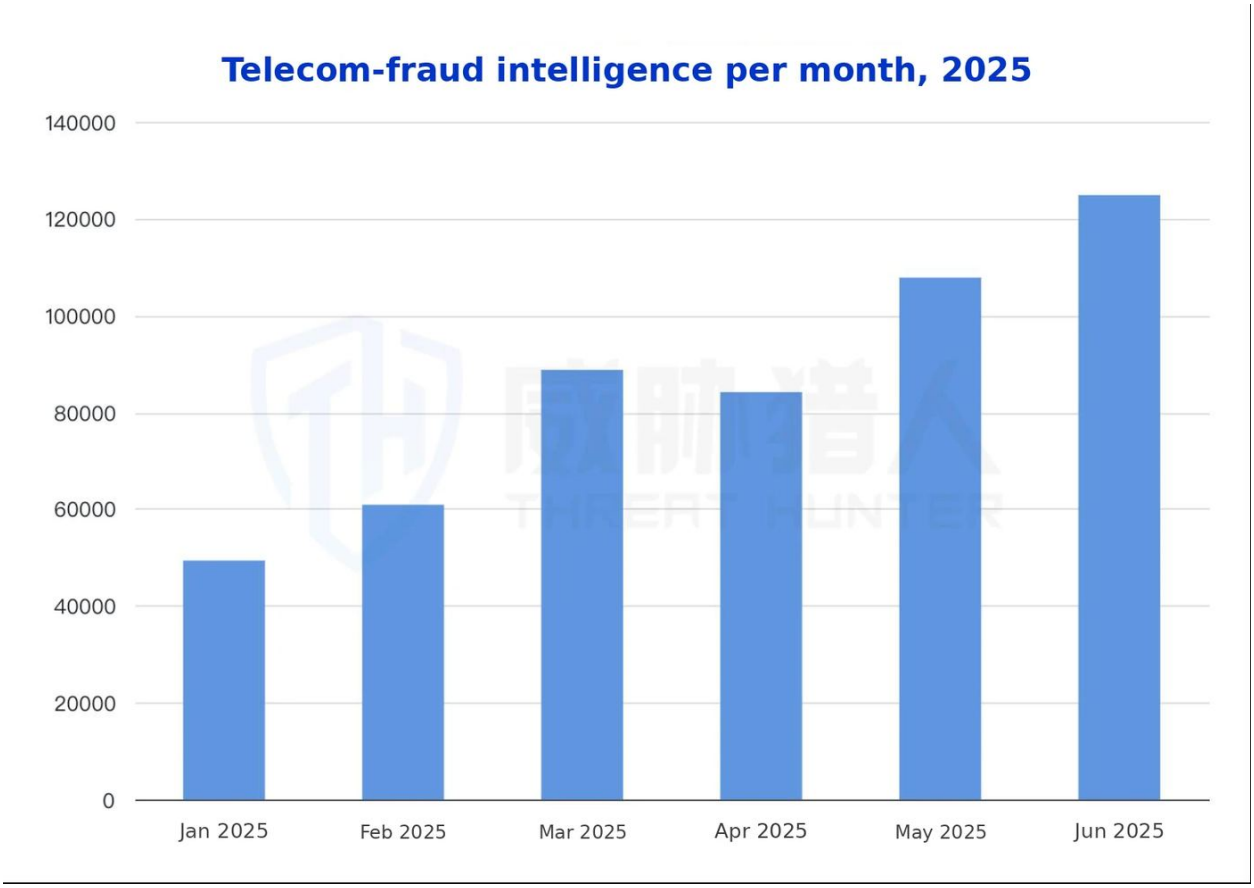
Source: Threat Hunter original report, page 66. Original figure with Chinese text replaced by English.

There is a financial gap, especially when users of housing financing and debt-taking have neither the ability nor the willingness to repay the loans. The risk is directly transferred to the banking institutions, causing the banking institutions to directly face risk impacts.

3.3 Analysis of telecom network fraud scenarios

3.3.1 Telecom fraud data trends in the first half of 2025

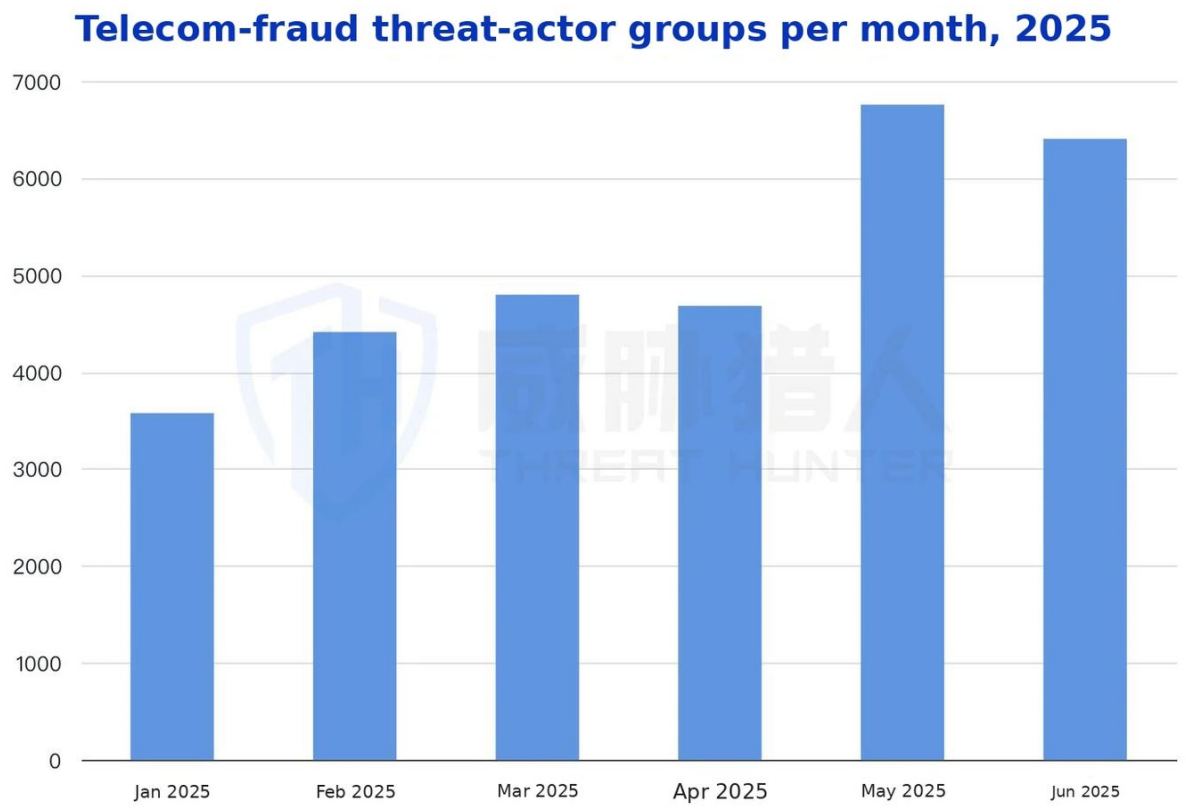
In the first half of 2025, the Threat Hunter risk intelligence platform detected 510,000 pieces of telecom network fraud-related information, a decrease of 27.39% from the second half of 2024. However, this is not the ebb of electronic fraud, but a phased "appearance" caused by the superposition of multiple factors: such as the crackdown on fraud-related tactics on various social networking and short video platforms, the arrest of large gangs such as Haowang Guarantee, and the switching of some communication channels to encrypted platforms. At the same time, the number of active cybercriminal groups and the scale of fraud-related accounts are still rising, indicating that the electronic fraud ecosystem is accelerating its evolution to a more covert and vertical direction.



Telecom-fraud intelligence per month, 2025

Source: Threat Hunter original report, page 67. Original figure with Chinese text replaced by English.

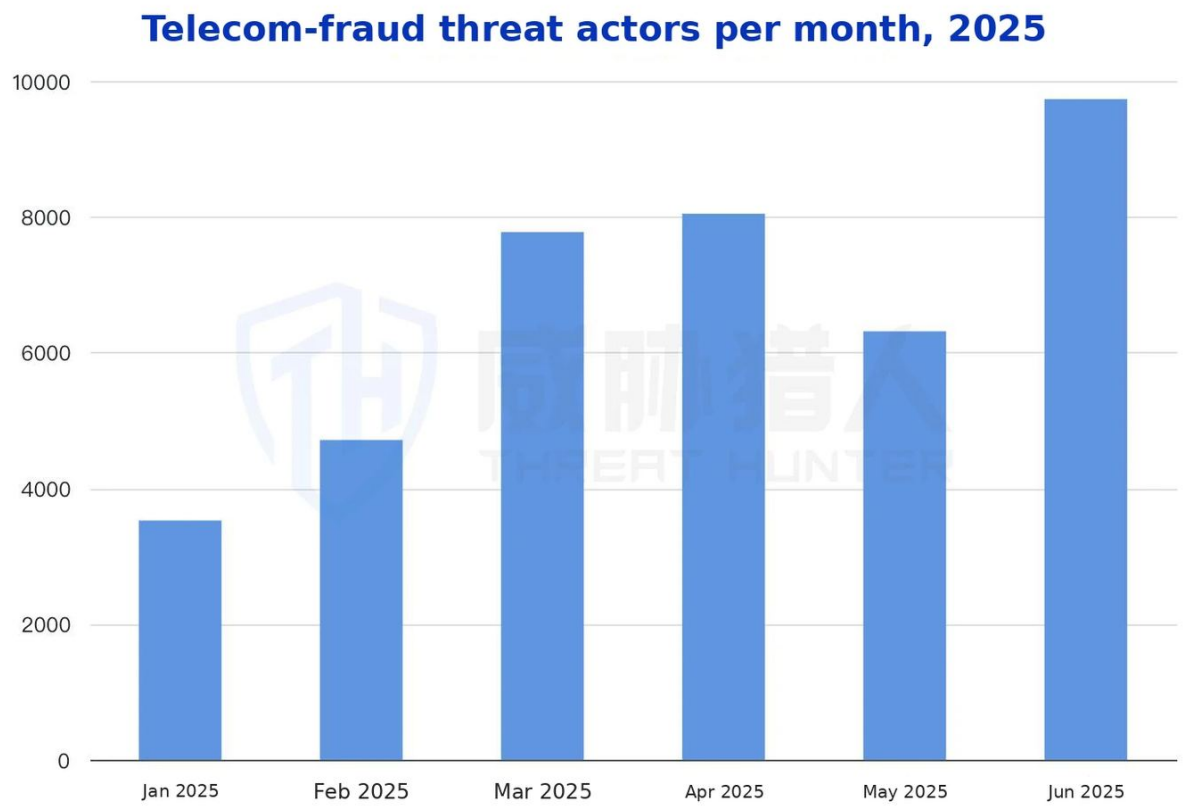
In the first half of 2025, the Threat Hunter risk intelligence platform monitored a total of about 29,000 active malicious activity social groups, an increase of 2.46% from the second half of 2024, and the average monthly number of active groups remained stable at about 5,000. Among the active group chat channels, social media platforms with anonymous group chats and social group chats as the main large-scale user groups, cybercrime ecosystem continues to rely on social platforms to carry out organized crimes, covering illegal activities such as promoting counterfeit links, distributing rhetoric packages, and publishing phishing pages.



Telecom-fraud threat-actor groups per month, 2025

Source: Threat Hunter original report, page 68. Original figure with Chinese text replaced by English.

In the first half of 2025, the Threat Hunter risk intelligence platform detected 40,000 accounts involving malicious activity threat actors, an increase of 7.61% from the second half of 2024. Under continuous crackdowns, cybercriminal groups have improved its survival rate through decentralization, multi-account manipulation and other means, and malicious activity behaviors have become more covert and frequent.



Telecom-fraud threat actors per month, 2025

Source: Threat Hunter original report, page 68. Original figure with Chinese text replaced by English.

3.3.2 The triple trap of “senseless fraud”: technical guidance, verification loopholes and counterfeiting are reshaping the fraud methods

As payment systems and identity verification mechanisms become increasingly intelligent, cybercrime ecosystem fraud techniques are also quietly escalating. Compared with the past "tricking you into clicking links and entering passwords", today's criminals are more inclined to bypass your perception and judgment and use technical processes to guide you to "cooperate to complete" or "passively lose control" to complete payment operations.

In the first half of 2025, the Threat Hunter risk intelligence platform detected that three typical new types of fraud techniques are spreading widely, and they constitute the three major models of current "senseless fraud":

1. Use NFC technology to realize remote card transfer: Essentially, it uses communication technology to break through the physical verification scenario and realize contactless skimming.

The user is unaware that the card information has been "copied".

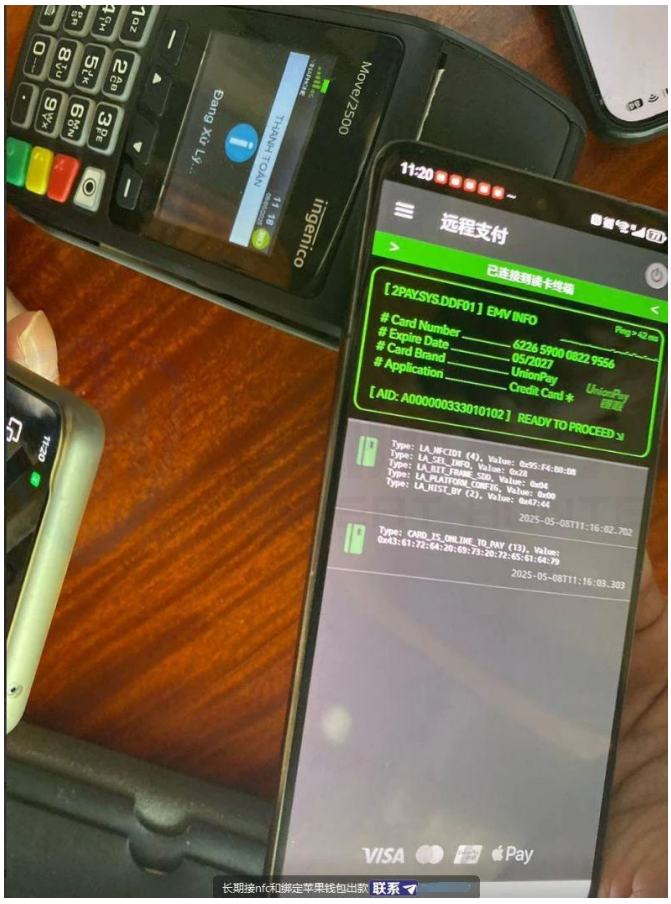
2. Enterprise payment scam: Using verification loopholes to control the payment process: Using logical loopholes in the identity verification process to bypass payment intentions

Confirmation allows users to complete real deductions in the scenario of "paying for others".

3. Counterfeit App fraud: The essence is to use fake official authoritative images to disguise a trustworthy environment and induce users to voluntarily hand over funds or information.

interest.

(1) Abuse of NFC password-free, inducing "active card posting" and off-site fraud. In the first half of 2025, Threat Hunter detected multiple fraud incidents involving NFC fraud. Criminals use "remote card transfer" technology to induce the victim to hold the bank card close to the mobile phone, steal the NFC data and remotely simulate the card to complete the fraud abroad or on other devices. The entire process does not require the user to enter a password. Even if the card is not out of the person's control, it may still be stolen.



Screenshots of an NFC card-relay app

Source: Threat Hunter original report, page 69. Original image retained.

Typical fraud process:

1. Impersonate bank or financial platform customer service

Scammers pretend to be bank fraud-risk personnel through phone calls, text messages, social platforms, etc., claiming that "there are abnormal transactions on the bank card under your name" and requiring immediate security verification.

2. Guide the installation of the disguised App

Victims are asked to download an app called Account Security Assistant or NFC Verification Center. This app imitates a regular bank interface, but actually has an embedded NFC card reading module and data upload interface.

3. Inducing the card to read information

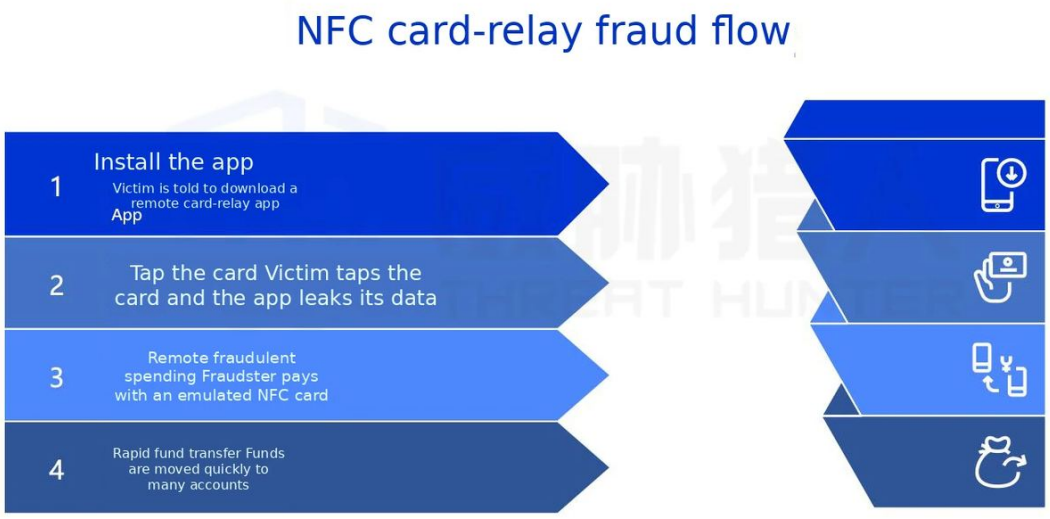
The scammer instructs the user to "hold the bank card to the back of the phone and cooperate to complete the chip verification." In fact, it induces the user to actively upload the card information to the fraud gang through NFC.

4. Remote emulation and theft

The fraud gang uses another mobile phone that supports NFC card simulation to complete fraudulent transactions on the POS machine, which is equivalent to having "your own bank card."

5. Fast fund transfer

After a successful transaction, the funds are quickly transferred to multiple accounts or used for virtual currency transactions. It often takes several hours for the victim to discover that the bank card has been stolen.



NFC card-relay fraud flow

Source: Threat Hunter original report, page 70. Original figure with Chinese text replaced by English.

(2) "Enterprise payment" has been abused by threat actors as a payment diversion entrance, and the platform verification mechanism has created a loophole entrance. "Enterprise payment", "company benefits", "free recharge"... It seems like a good thing, but it is actually a "pay out of pocket" trap set by scammers. In the first half of 2025, Threat Hunter detected that a new type of fraud under the guise of "corporate payment" is accelerating the spread. Scammers disguised themselves as platform customer service and operations staff, and guided users into the payment process under the guise of corporate subsidies and employee benefits. They also took advantage of loopholes in the platform's payment verification mechanism - such as face verification, quick payment, password-free authorization and other links to trigger payment by default rather than confirmation operations. Ultimately, users were able to complete deductions without realizing that they were performing real payment operations. When they discovered abnormal outflows of funds, they realized that the so-called "corporate payment" did not exist at all.



Screenshot of a corporate proxy-payment page

Source: Threat Hunter original report, page 71. Original image retained.

Typical fraud process:

1. Welfare diversion, long-term fishing

Scammers publish advertisements such as "company gift memberships" and "mobile phone recharge subsidies" in messaging-app groups and short-video comment sections to lure users into adding their messaging-app accounts or sending private messages.

2. Pretend to be a corporate payment agent and guide recharge

Scammers pretend to be customer service and operators, claiming that "in order to match the corporate account, you need to cooperate with the test payment process" and induce users to enter the "mobile phone recharge", "coupon collection", "order payment" and other pages of a payment app.

3. Inducing click verification actually triggers payment

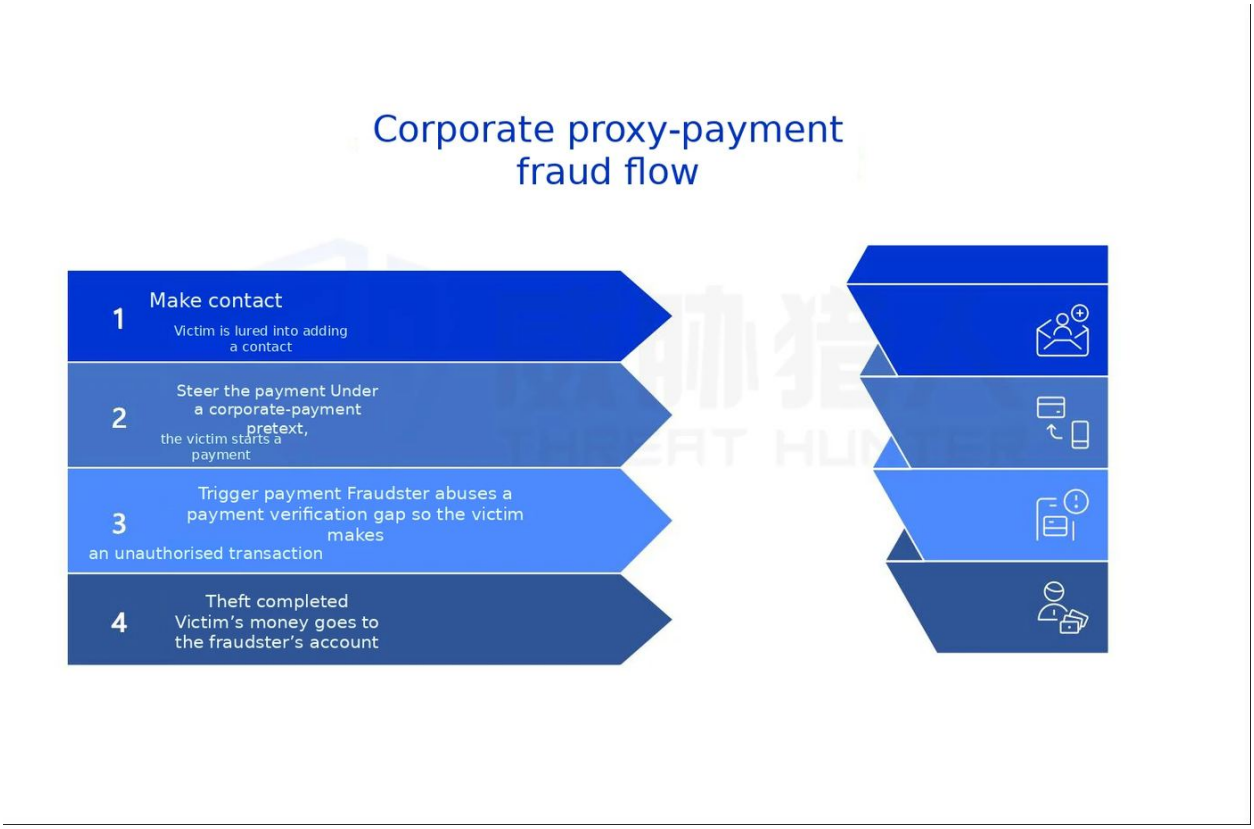
Scammers may use the excuses of "process verification" and "payment test" to guide you to repeatedly enter wrong passwords, scan your face for authentication, or ask you to click "password-free activation", "quick payment simulation" and other buttons in the app. You thought you were just cooperating with the operation, but due to loopholes in the platform's verification process, these actions actually triggered real deductions, causing the funds to be transferred without your knowledge.

4. Complete the transfer without any sense of fraud

In some payment platforms or older clients, as long as the face recognition is successful and the click action is completed, the system will perform the payment operation by default without pop-up confirmation or password links.

5. The fraud is completed and the funds are transferred immediately

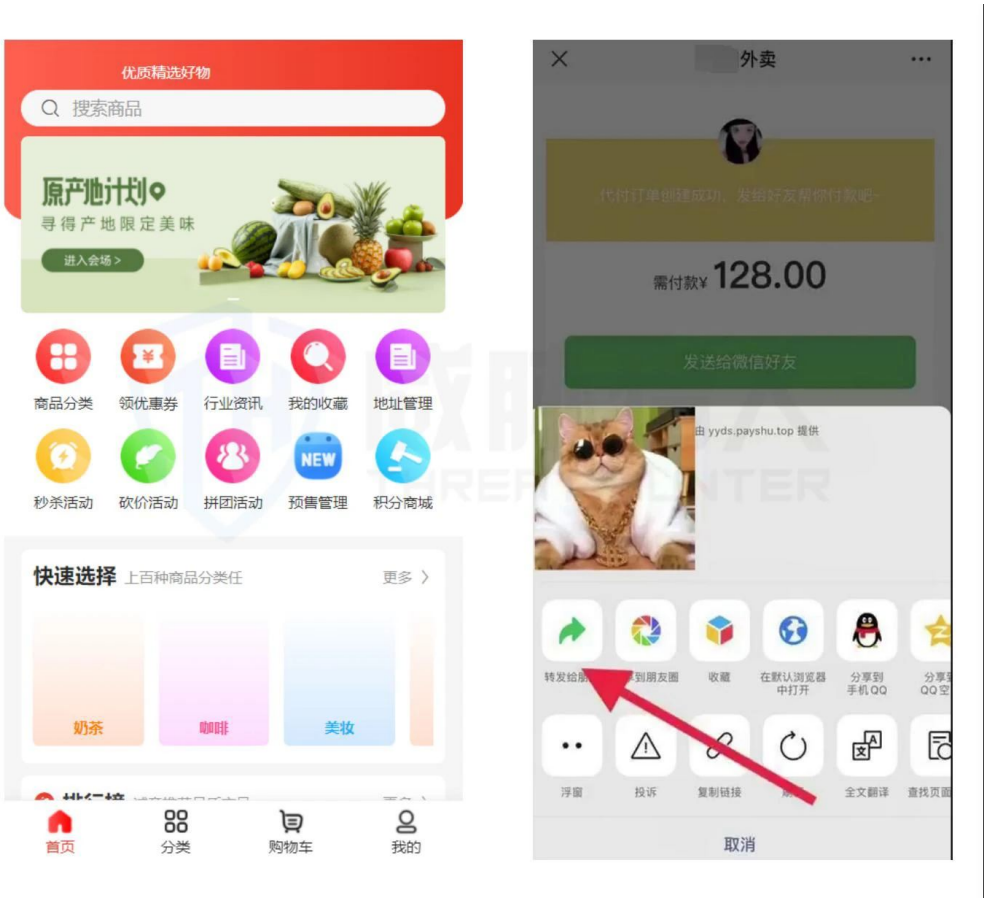
The user completes the payment without realizing it. The payment object is an account controlled by the scammer. Then the funds are quickly transferred out or washed out through the virtual currency platform. The victim often only discovers the abnormality after checking the bill afterwards.



Corporate proxy-payment fraud flow

Source: Threat Hunter original report, page 72. Original figure with Chinese text replaced by English.

(3) Counterfeit apps are packaged as regular platforms and trick you into stepping into a payment trap. As online fraud continues to evolve, "counterfeiting" has become one of the key means of high-frequency use in the cybercrime ecosystem. From counterfeiting banks, express delivery, and government apps to counterfeiting adult malls, social platforms, and internal malls, scammers use highly realistic disguised interfaces and inducement techniques to make users voluntarily hand over their money, permissions, and even privacy without knowing it.



Screenshots of a fake shopping platform

Source: Threat Hunter original report, page 73. Original image retained.

Simulation platform + emotion induction: List of counterfeiting fraud types that will occur most frequently in 2025

Impersonation type	Scenario	Core goal
Sextortion app	Imitates social or private-chat apps and lures users to install it and upload private information	Extortion and control of payment permissions
Emotional-manipulation proxy payment	Fraud gangs build fake e-commerce, food-delivery and adult-product platforms and use online-romance scripts to get victims to pay for goods. The pages look real and the payment flow matches the genuine platform, but the payee is a fraud account, so the money is lost on payment.	Emotional manipulation plus proxy-payment fraud
E-commerce discount phishing page	Imitates discount pages of major e-commerce platforms, spread as "staff purchase" or "hidden subsidy" offers	Steal payment details and steer payments
Fake government or courier app	Imitates official government or logistics apps and sends "overdue payment" or "parcel problem" alerts	Social engineering plus malware

Types of impersonation used in proxy-payment fraud

Source: Threat Hunter original report, page 73. Table re-typeset in English from the original.

Analysis of typical cases: The fraud process of "payment fraud" caused by counterfeit malls is as follows:

1. Cultivation of feelings and guidance of trust

threat actors organize chat agents to register female accounts on dating platforms, and establish an "online love" relationship with the victim through long-term chats. After stabilization, they guide the "man" to fulfill his "couple obligations" and make small demands such as buying milk tea, fruits, meals, and medicines.

2. Place an order in a counterfeit mall and generate a payment link

The chat agent entered the counterfeit e-commerce platform provided by threat actors. The platform page almost completely replicated the homepage of a well-known e-commerce takeaway. It supported the selection of product categories (such as flowers, fruits, milk tea, medicines, etc.), filled in the false delivery address, and generated a "payment link" or payment QR code.

3. The payment process conceals the real payee

What the user sees after scanning the code is an almost completely normal "product payment page". Because the page uses a messaging app's built-in payment function, the payer cannot see the delivery address or payee, only the product name and amount, which can easily be misjudged as a real platform request.

4. fraud controls bypass and multiple forwarding techniques

threat actors operators usually first send the link to their own messaging-app account to test whether there is any risk warning. If there is no abnormality, they will forward it to the victim to ensure that the fraudulent operation will not be intercepted by the messaging app's fraud controls.

5. The fraud is successful when the payment is completed.

Once the payment is successful, the platform displays "paid", but the goods are never actually delivered, and the payee is the account of threat actors. Users often do not doubt the other party because of the small amount and the close attitude of the other party, and even pay for the other party many times.

Step	Stage	What happens
1	Create a fake account	The fraudster registers a fake female profile on a social or dating platform.
2	Build rapport	The fraudster chats with the victim over a long period to build a relationship.
3	Make a small request	The fraudster asks for small items, such as milk tea or fruit.
4	Generate a pay-for-me link	The fraudster creates a proxy-payment link on a fake platform.
5	Hide the payee	The payment page hides the real payee details.
6	Payment made	The victim pays, believing the request is genuine.
7	Fraud succeeds	The fraudster collects the money and the goods never arrive.

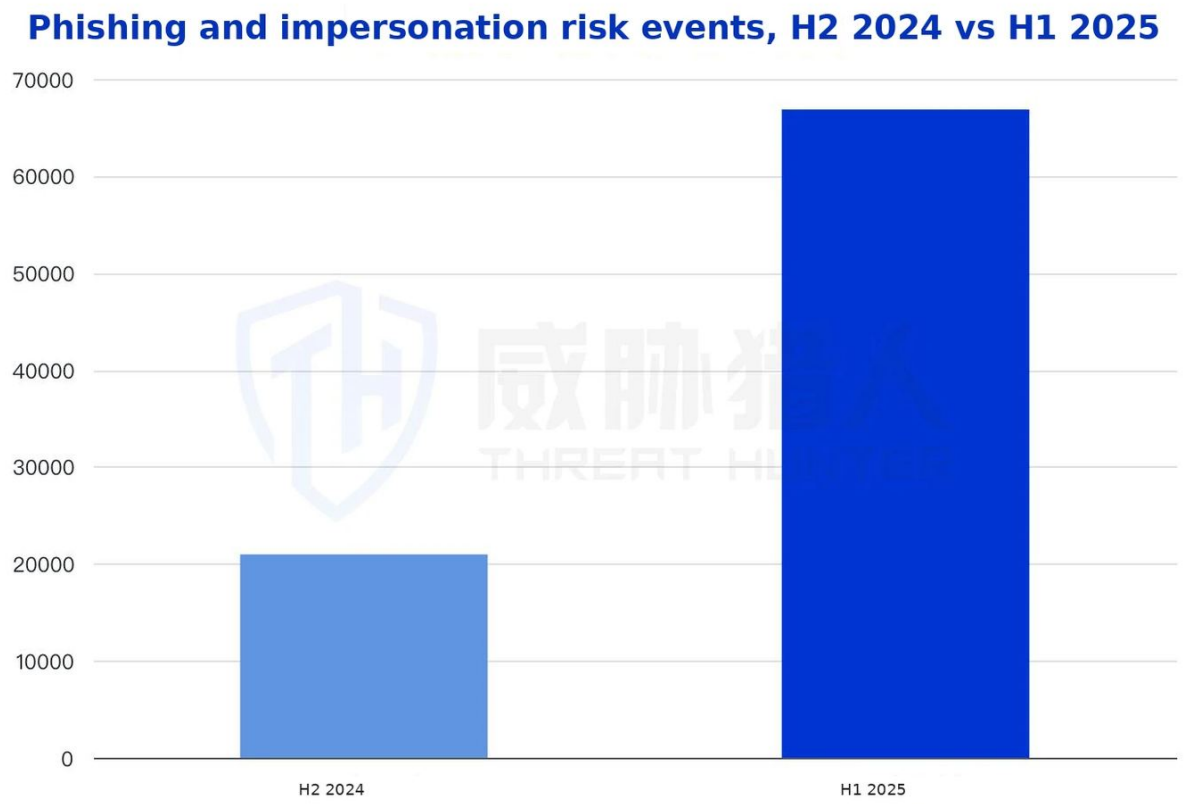
Proxy-payment fraud flow

Source: Threat Hunter original report, page 75. Table re-typeset in English from the original.

3.4 Analysis of Phishing and Counterfeiting Scenarios

3.4.1 The total number of risk events has exceeded 3 times, and social media driven and infringement have become new attack trends

In the first half of 2025, Threat Hunter captured a total of 66,855 cases of phishing counterfeiting risk information, which was a sharp increase compared with 20,968 cases in the second half of 2024, with the total amount exceeding three times. Behind this explosive growth is a systematic upgrade of attack modes: traditional phishing attacks are still the "basic", but new attack chains that use social media as the entrance to traffic and product infringement as a means of monetization are showing strong growth momentum and becoming a core factor in the increase in threat intelligence.



Phishing and impersonation risk events, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 75. Original figure with Chinese text replaced by English.

Product infringement: refers to attackers openly selling products that infringe on corporate intellectual property rights on major e-commerce platforms. In the context of this report, it mainly covers virtual goods such as initial numbers for game private servers, pirated software activation codes, cracked accounts, etc. It is a key link for cybercrime ecosystem to convert traffic into revenue.

Phishing website: Refers to a fake website created by an attacker that is highly similar in appearance and domain name to the official website. Its main purpose is to trick users into

entering sensitive data such as account passwords, personal identity information, bank card or payment information, which is the most direct and common method in phishing attacks.

Counterfeit social media: This refers to attackers registering and operating fake accounts that are highly consistent with the official brand or personal image on social platforms, short video platforms and other channels. These accounts usually attract traffic by publishing fake activities, lottery information, etc., or directly interact with users' private messages to carry out precise fraud. They are currently the main traffic entrance and user access channel for the cybercrime ecosystem.

Counterfeit app: Refers to malicious mobile applications made by attackers that imitate official genuine applications in terms of icons, names, and interface designs.

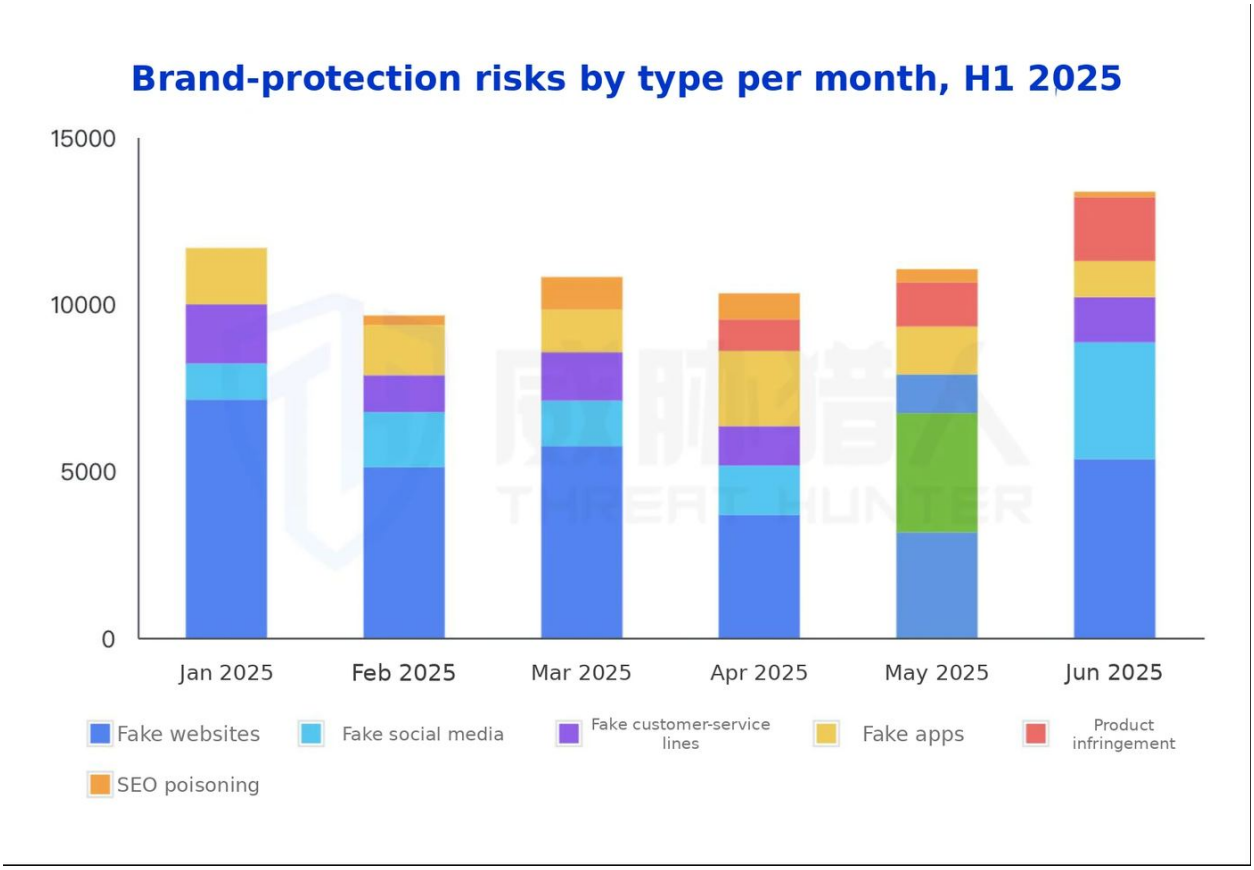
These applications are usually spread through unofficial channels such as third-party download sites, social groups, and SMS links. After installation, they can steal sensitive information from users' devices or implant Trojans, which is a highly harmful form of attack.

Fake customer service hotline: This refers to an attacker using a fake number or using number-changing software to pretend to be an official customer service hotline and proactively contact users. Attackers usually use social engineering to conduct verbal fraud on the grounds of "order anomalies", "account security issues", etc., to induce users to provide verification codes, passwords or directly perform transfer operations, which are often used in the "harvesting" phase of fraud.

SEO pollution: refers to attackers using search engine optimization (SEO) technology to optimize fake pages containing malicious code or pointing to phishing websites to the top of search results. When users search for specific keywords (such as "XX official customer service", "XX software download"), they will mistakenly enter these trap pages. This is a means of achieving precise attacks by hijacking the user's normal search intentions.

(1) Counterfeit websites are the cornerstone of attacks, counterfeit social media, and product infringement have grown strongly. Throughout the first half of the year, a total of 30,155 counterfeit website attacks were captured, accounting for 45.11% of the total risk intelligence. It is almost the single risk type that maintains the highest proportion every month, forming the "chassis" for phishing attacks. This shows that setting up fake sites to directly steal sensitive data such as user accounts, passwords, payment information, etc. is still the most common and core method used by attackers. Its large size determines that it is still the primary defensive position for brand protection work.

It is also worth noting that the proportion of attacks related to product infringement and counterfeit social media has increased significantly since March and April respectively, showing strong growth momentum.

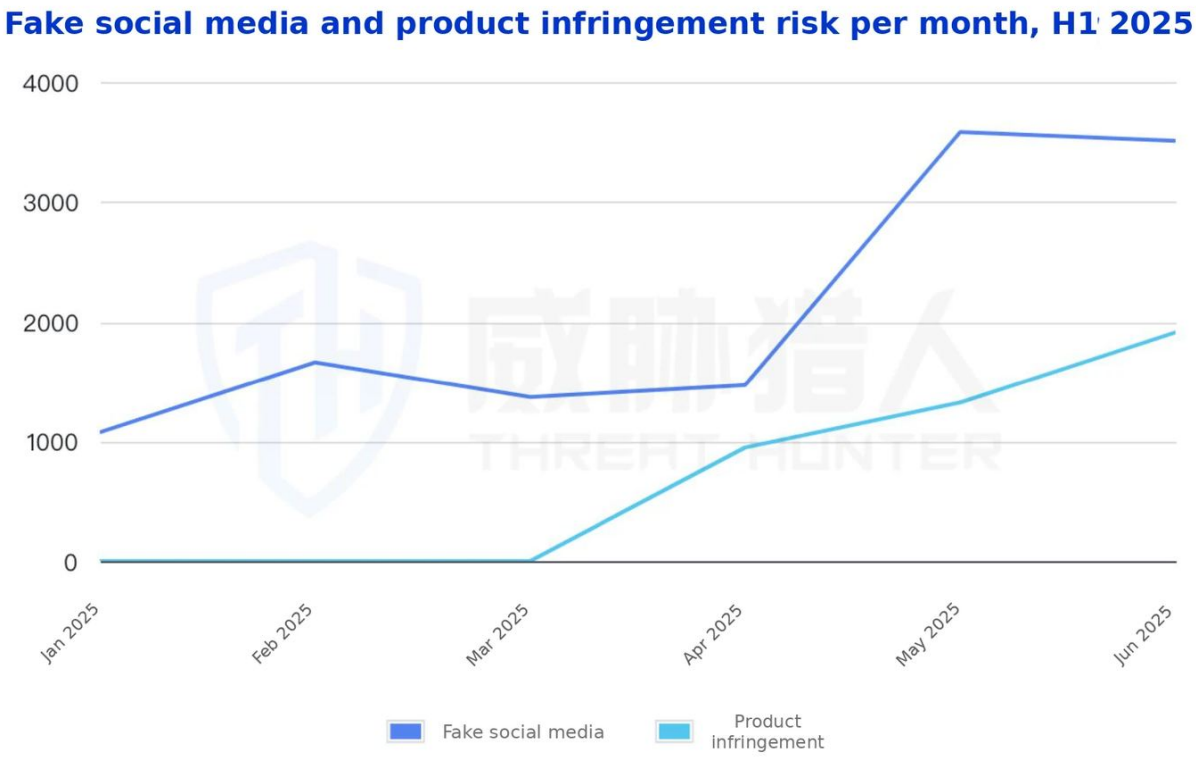


Brand-protection risks by type per month, H1 2025

Source: Threat Hunter original report, page 77. Original figure with Chinese text replaced by English.

(2) Counterfeit social media and product infringement show "collaborative growth", driving changes in attack patterns. Threat Hunter's continuous monitoring of the gaming industry found that a large number of official social media accounts were counterfeited. The ultimate goal was not to directly fish, but to systematically divert users to e-commerce platforms to purchase infringing products such as private servers and plug-ins. In order to fully reveal this attack link of "front-end traffic diversion and back-end monetization", Threat Hunter will officially include "commodity infringement" in monitoring starting from April. Subsequent data clearly verified our judgment: the risk of counterfeiting social media as a traffic entrance surged to 3,581 cases in May, while the risk of product infringement as a monetization channel also rose from 948 newly monitored cases in April to 1,911 cases in June.

The high synchronization of these two risk curves marks the emergence of a complete industrial chain attack model that starts with the gaming industry, diverts traffic through counterfeit social media, and then monetizes infringing products.

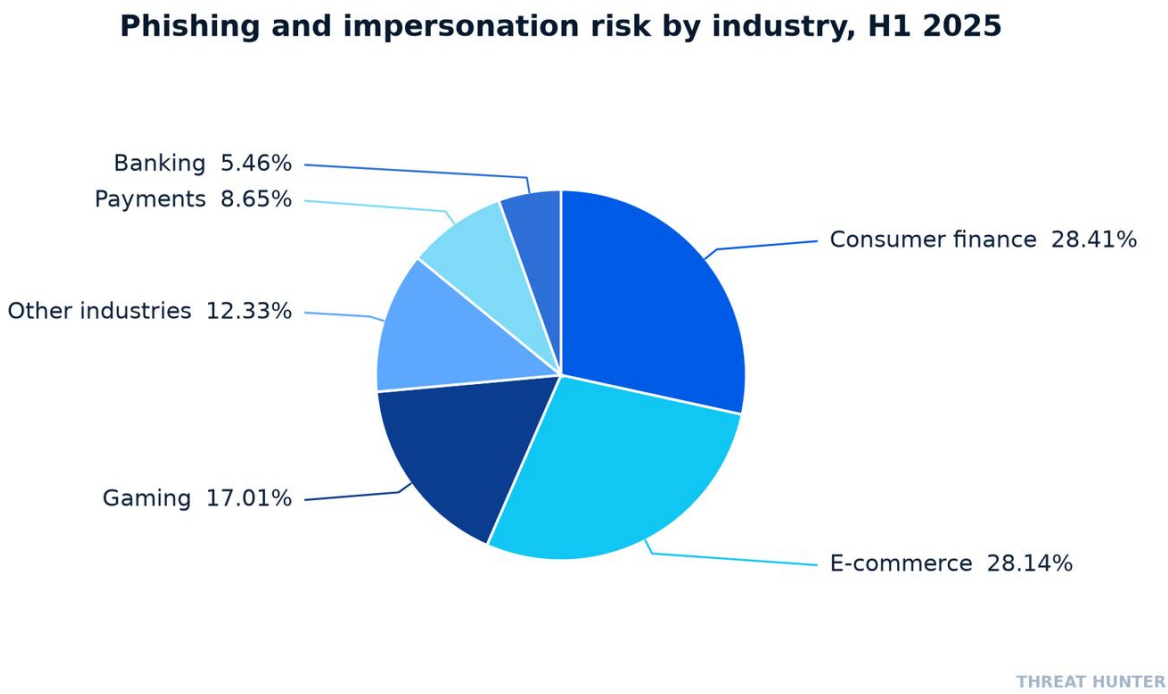


Fake social media and product infringement risk per month, H1 2025

Source: Threat Hunter original report, page 78. Original figure with Chinese text replaced by English.

3.4.2 The pan-financial field and game IP have become two independent battlefields

Data from the first half of 2025 show that the risk of phishing counterfeiting is highly concentrated. Among them, the pan-financial field is the hardest hit area with the most concentrated attacks. This field aims to directly steal funds, including consumer finance (28.41%), e-commerce (28.14%), payment (8.65%), and banks (5.46%). The total proportion is as high as 70.66%, while the gaming industry, which is centered on the systematic collapse of business models, accounts for 17.01%. Taken together, the two major fields of pan-finance and gaming account for nearly 90%, constituting the main battlefield for current phishing and counterfeiting attacks.



Phishing and impersonation risk by industry, H1 2025

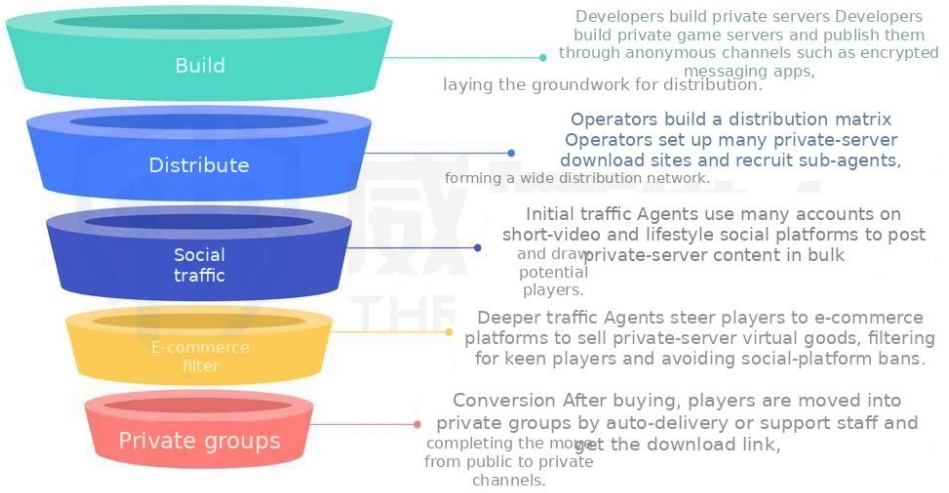
Source: Threat Hunter original report, page 78. Redrawn in English from the original figure.

(1) Pan-financial field: The direct plunder ecological pan-financial field with funds as the core (consumer finance, e-commerce, banking, and payment industries account for up to 80.6% in total) has become a "natural hunting ground" for phishing and fraud because it directly handles massive capital flows, payment information, and user personal data. By spoofing websites, payment pages, customer service telephone numbers, etc., attackers aim to steal key information such as users' bank card numbers, passwords, and verification codes, thereby directly stealing funds.

(2) Game industry: The risk of systematically disrupting the business foundation of the game industry by removing wages from the bottom of the cauldron stems from a completely different logic. Its core is intellectual property infringement attacks such as private servers and plug-ins. Attackers directly copy official games by building private servers, which not only erodes brand value, but more importantly, diverts core paying users and directly eats into official commercial revenue. The essence of this attack is to systematically destroy the business model of the target enterprise. By building a parasitic gray industry chain, it hollows out the revenue base of genuine games and shortens their life cycle.

3.4.3 Revealing the "Drainage Matrix" of game private servers: a new paradigm of threat actors who systematically steal brand core assets

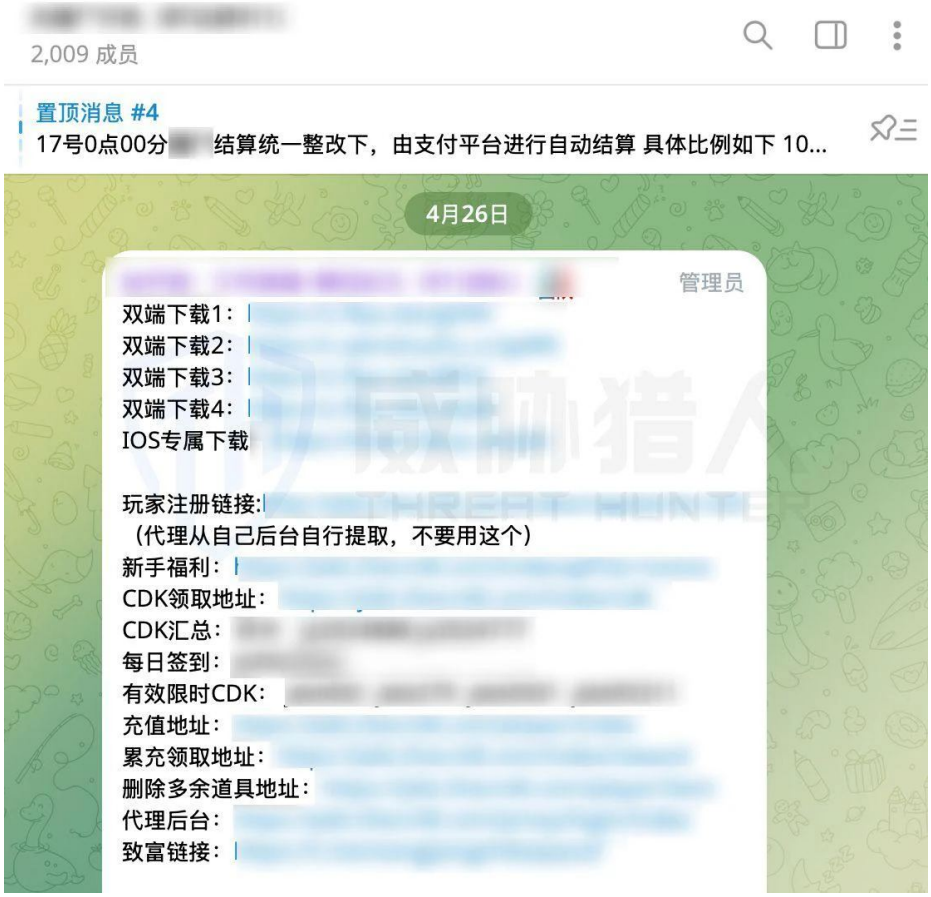
(1) Industrial chain structure: From the source of technology to the rampant matrix distribution of private game servers, it has evolved from a "small workshop" in the past to a cybercrime ecosystem empire with clear division of labor, multi-platform linkage, and automated operation. Its core is no longer a single promotion link, but a carefully designed and progressive "drainage matrix":



How private game servers are distributed

Source: Threat Hunter original report, page 80. Original figure with Chinese text replaced by English.

Upstream - technical source: An anonymous technical team is responsible for cracking the official source code, building private servers, and releasing them through encrypted channels such as encrypted messaging apps. This is the "arsenal" of the entire threat actors, and it is the difficulty of traditional attack methods.



Screenshot of a private-server agent channel

Source: Threat Hunter original report, page 80. Original image retained.

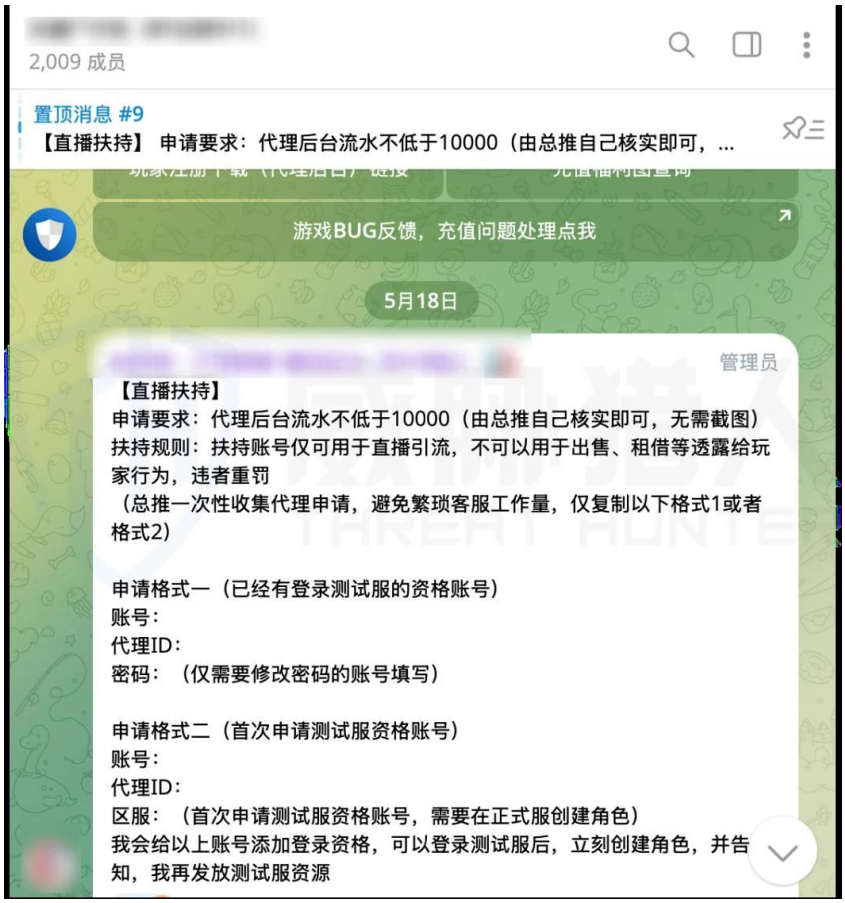
Midstream - channel distribution: A professional operation team establishes a large number of private server download websites and develops a pyramid-like offline agent network to build a highly resilient matrix distribution channel covering the entire network. Blocking a single node cannot shake its foundation.

Downstream-traffic conversion: executed by a large number of agents, responsible for accurately converting public domain traffic into private domain users, it is the most active and large link in the entire system.

(2) Core operation: the precise funnel of “drainage-screening-conversion”. Drainage and conversion in the downstream of the funnel follow a set of standardized three steps, and each step is carefully designed:

Initial traffic diversion (social media exposure):

Agents register a large number of accounts and publish attractive content such as "internal benefits" and "high explosive rates" related to private servers to conduct widespread exposure and attract the attention of potential players. There are generally two ways to attract traffic. One is to attract traffic by posting on social media platforms with graphics and text, and the other is to attract traffic through live streaming on video platforms.



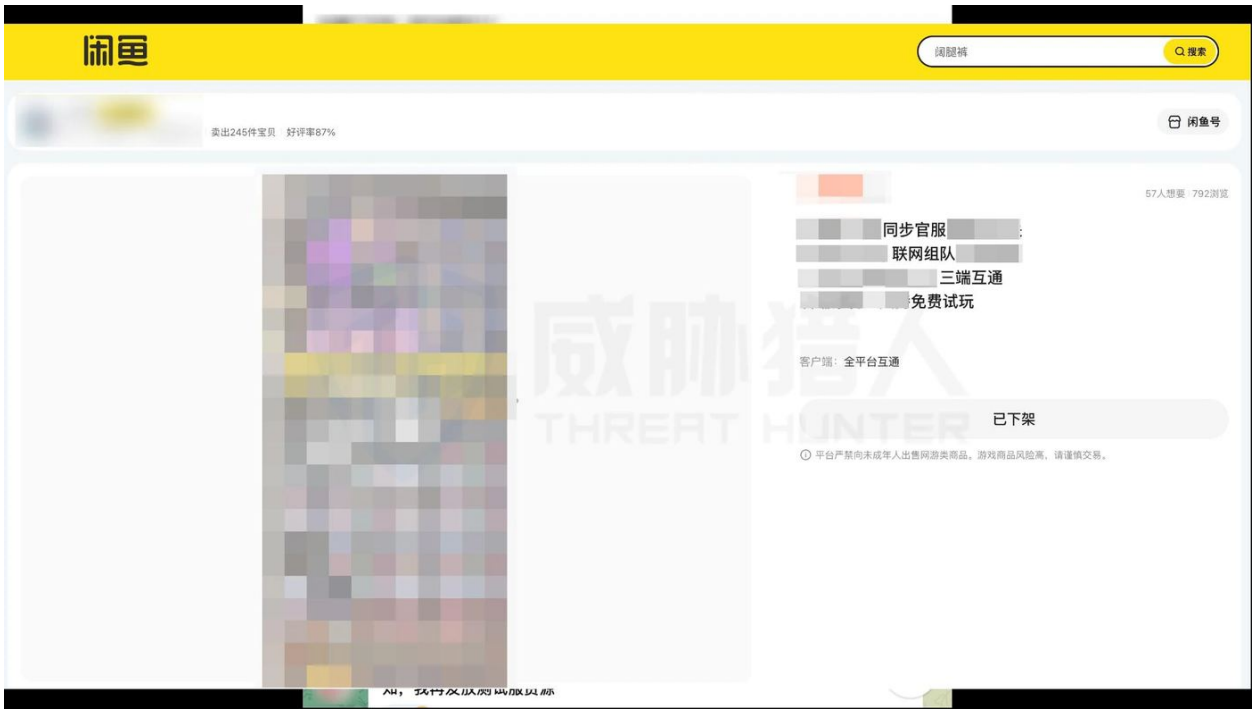
Screenshot of a private-server agent announcement

Source: Threat Hunter original report, page 81. Original image retained.

Deep drainage (e-commerce screening):

This is the most critical hub in the entire attack chain. The attacker will not provide download links directly on social media, but will guide users to the e-commerce platform to purchase an "initial account" or "resource package" that costs only a few yuan. This kills two birds with one stone:

- Screen high-value targets: The payment behavior itself is an efficient "intent screening", which can accurately identify "potential funders" who may make large recharges in the future from a large number of users.
- Avoid platform bans: Compared with directly publishing a private server website or private server app on social media, this "e-commerce traffic diversion" model is more hidden. This is because the traffic-draining content (such as game guides, welfare receipts, etc.) published by the attacker itself does not contain direct violation information, but "both vague and clear" guides users to the e-commerce platform to complete a seemingly normal transaction. This makes it difficult for game officials to effectively complain and ban based on social media content alone, thus greatly extending the survival time of the entire attack link.



Screenshots of private-server listings on a second-hand marketplace

Source: Threat Hunter original report, page 82. Original image retained.

- Final conversion (private domain precipitation): After the user purchases, he is drawn into private community groups such as messaging-app groups through customer service guidance or automatic delivery. At this point, threat actors have completed the transition from public domain traffic to private domain assets. In this closed environment, subsequent large-amount recharges and instigation of core paying players will be completely out of supervision. Brands will not only lose revenue, but also permanently lose core users.

(3) Business closed loop: Viral expansion driven by high shares and anonymous settlement. This system can expand virally, and its core driving force lies in its business model. Exclusive information from Threat Hunter shows that a private server agent can obtain up to 46% of player recharge rebates, and settles through cryptocurrencies such as USDT stablecoins. This "high commission + anonymous settlement" model has greatly encouraged the expansion of downstream agents, and at the same time has also brought huge challenges to traceability and crackdowns.



Screenshot of a chat about private-server agent earnings

Source: Threat Hunter original report, page 83. Original image retained.

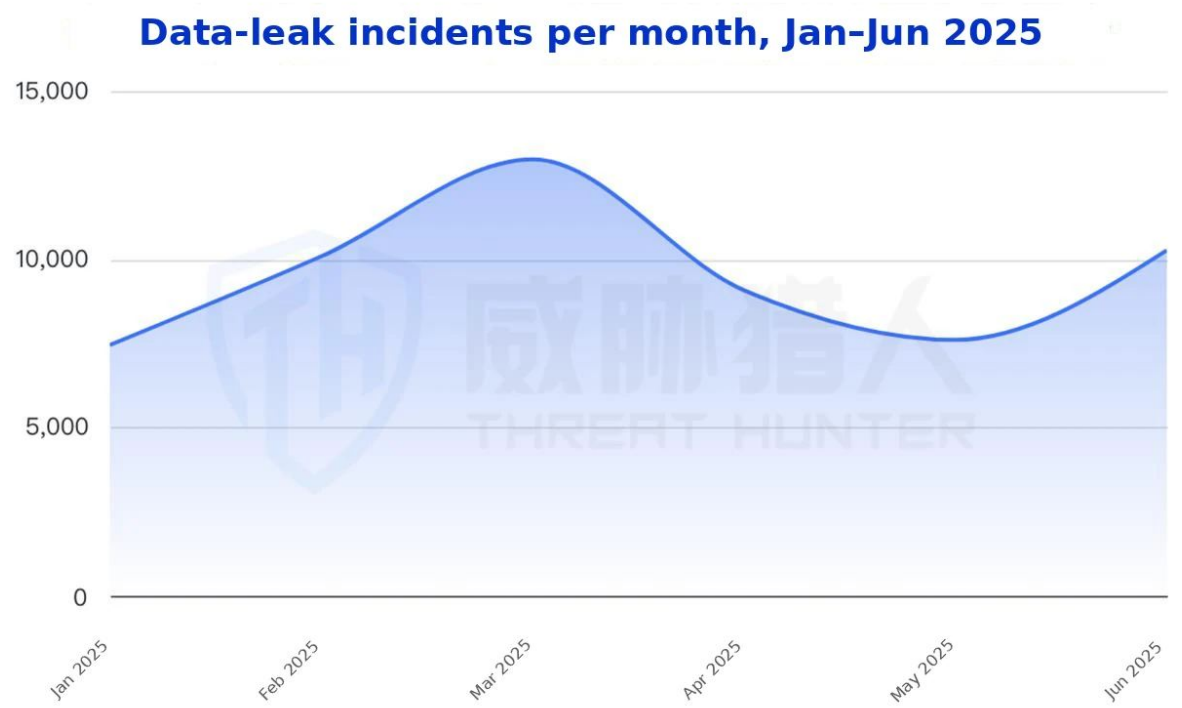
3.5 Data leakage scenario analysis

3.5.1 There were 57,092 data breaches in the first half of 2025, an increase from the second half of 2024

Reported share: 1.54%

According to data from the Threat Hunter data leakage risk monitoring platform, between January and June 2025, a total of 180 million intelligence clues were monitored across the entire network. After manual analysis by the authenticity verification engine and DRRC, a total of 57,092 data breaches were confirmed to be valid, an increase of 1.54% from the second half of 2024.

Judging from the changing trend of the number of data leakage incidents in the first half of the year, it shows obvious abnormal fluctuations. It showed an upward trend from January to March. The number of attack incidents continued to decline from April to May, and there was a significant rebound in June.



Data-leak incidents per month, Jan–Jun 2025

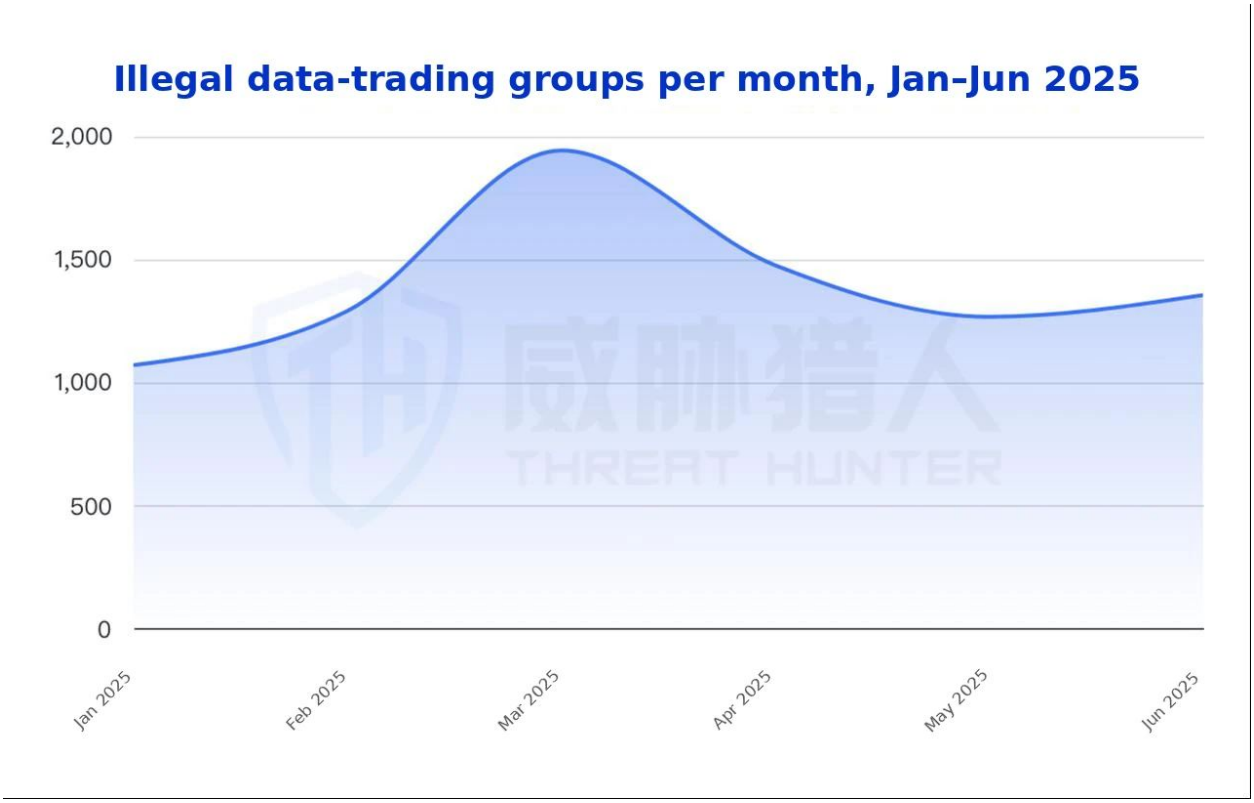
Source: Threat Hunter original report, page 84. Original figure with Chinese text replaced by English.

Threat Hunter found that this fluctuation may be strongly related to a major encrypted messaging app launching a "group closure operation" against illegal gangs in April 2025. This action resulted in the banning of a large number of illegal data trading groups, blocked the trading channels of threat actors, or directly led to a decrease in the number of data leakage incidents.

Analysis of data captured from Threat Hunter found that the number of active illegal data trading groups decreased from 1,943 in March to 1,477 in April, a decrease of 23.98%; further analysis found that 33.71% of active groups in March were suspected of being banned in April.

Correspondingly, the number of data breaches we monitored in April 2025 was 9,085, a month-on-month decrease of 29.93%.

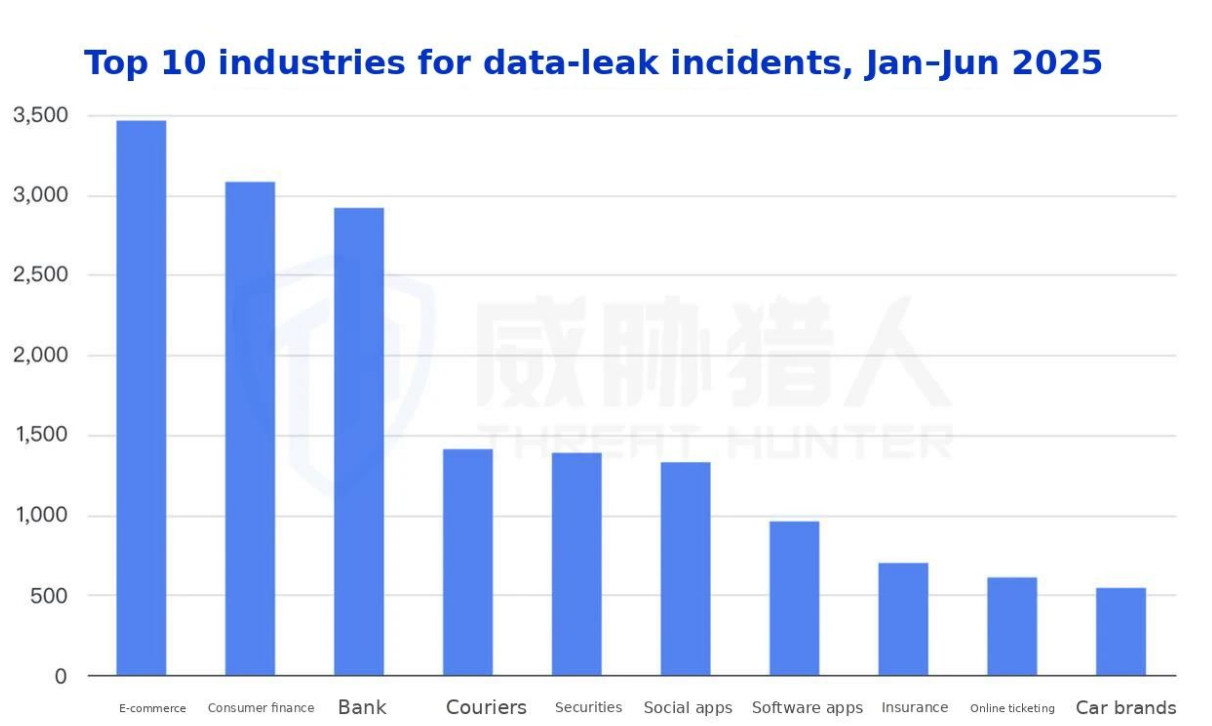
However, due to the difficulty of completely policing the encrypted messaging app and the extremely strong "regeneration ability" of illegal gangs, a large number of new or alternative groups became active again in a short period of time, driving the number of data breaches to rebound again in June 2025.



Illegal data-trading groups per month, Jan–Jun 2025

Source: Threat Hunter original report, page 84. Original figure with Chinese text replaced by English.

From the perspective of industry distribution, network-wide data breaches in the first half of 2025 involved a total of 76 industries, and the top 3 industries were e-commerce, consumer finance, and banking. Among them, highly sensitive and high-realizability industries, represented by e-commerce and finance, are still the hardest hit areas for data leakage.



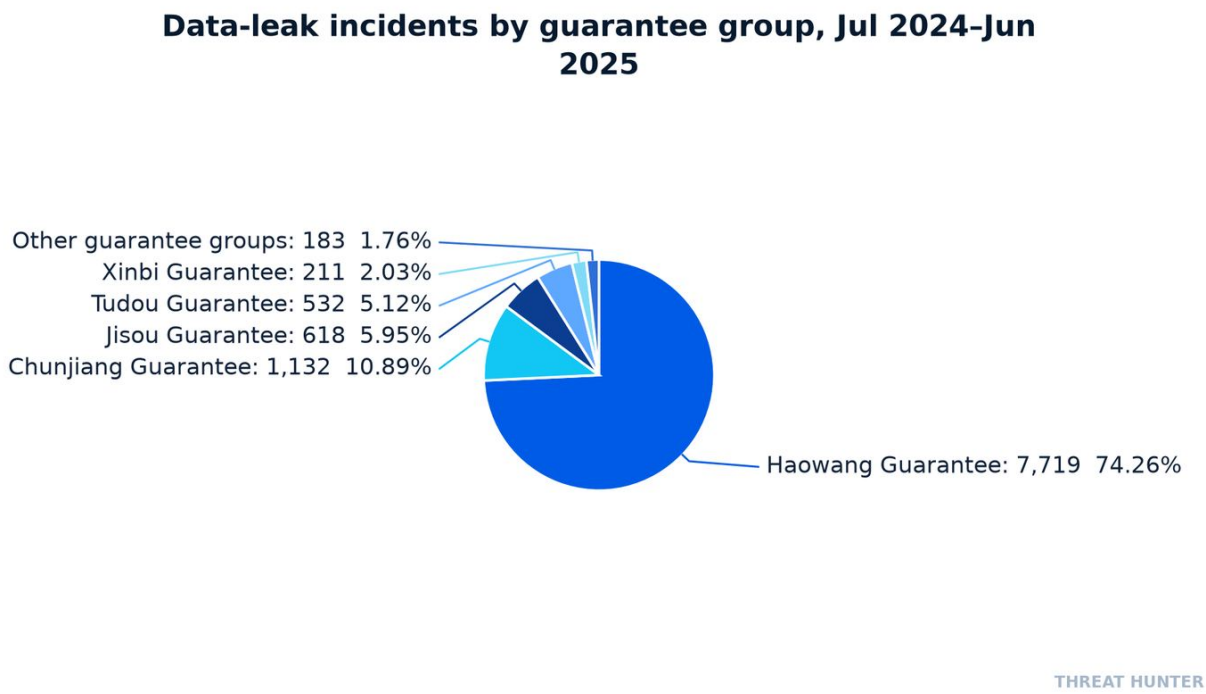
Top 10 industries for data-leak incidents, Jan–Jun 2025

Source: Threat Hunter original report, page 85. Original figure with Chinese text replaced by English.

3.5.2 The leading guarantee gang was attacked, and new guarantees were quickly filled (1) Haowang Guarantee suffered heavy losses and was shut down, temporarily affecting the data leakage transactions of threat actors

In the illegal data trading market, both the data supply side and the demand side are highly active, forming a strong supply and demand relationship and giving rise to a complete transaction chain of threat actors. However, due to the high risks and uncertainties in the transaction itself, it is difficult for buyers and sellers to establish a direct trust relationship, so the guarantee group emerged as a neutral "third-party guarantor" mechanism.

Among them, "Haowang Guarantee" (formerly known as "Huiwang Guarantee") has been active on anonymous encrypted messaging apps for a long time. With its third-party credit intermediary services, it has become the core guarantee platform for threat actors such as data transactions, fraud, and money laundering. It will dominate the market in the first half of 2025 and before. Judging from event data in the past year, the number of data leakage transactions guaranteed by it accounts for as high as 74.26%.



Data-leak incidents by guarantee group, Jul 2024–Jun 2025

Source: Threat Hunter original report, page 86. Redrawn in English from the original figure.

However, in May 2025, Haowang Guarantee suffered a heavy blow.

- On May 1, the US Financial Crimes Enforcement Network (FinCEN) listed its parent company Huione Group (Huiwang) as an institution of "primary money laundering concern" and cut off its international financial channels. Subsequently, the encrypted messaging app banned its trading groups and accounts in early May.
- On May 9, Haowang officially announced that "a large number of trader accounts have been canceled." At this point, its operating system completely collapsed, and the public group business interruption rate reached 100%.

Date	Event	Details
May 1, 2025	US sanctions hit Haowang Guarantee	FinCEN named Cambodia’s Huione Group a primary money-laundering concern and proposed a rule to counter online fraud and theft.
May 2, 2025	Backup groups ready to move	Threat actors set up Haowang backup groups on Tudou Guarantee, ready to move there.
May 9, 2025	Channels to restore groups opened	Haowang first announced that, because of the messaging app’s risk controls, many trader accounts had been closed and were being restored, and opened a way to restore public and dedicated groups.
May 13, 2025	Pledges moved to Tudou	Because of the messaging app’s risk controls and policy changes, Haowang’s public groups stopped business and moved pledges to Tudou Guarantee; dedicated groups carried on. Users could ask traders for refunds and were told all deposits were safe.
May 13, 2025	No hope of recovery; operations stop	Haowang’s public groups announced that all its NFTs, channels and groups had been blocked by the messaging app on May 13, 2025, and that it would stop operating from that day.
May 13, 2025	Tudou backs Haowang users with free rent	Tudou’s public groups announced three months’ free group rent for Haowang customers whose groups were blocked, to cut their losses and keep them running.

Timeline of Haowang Guarantee’s collapse, May 2025

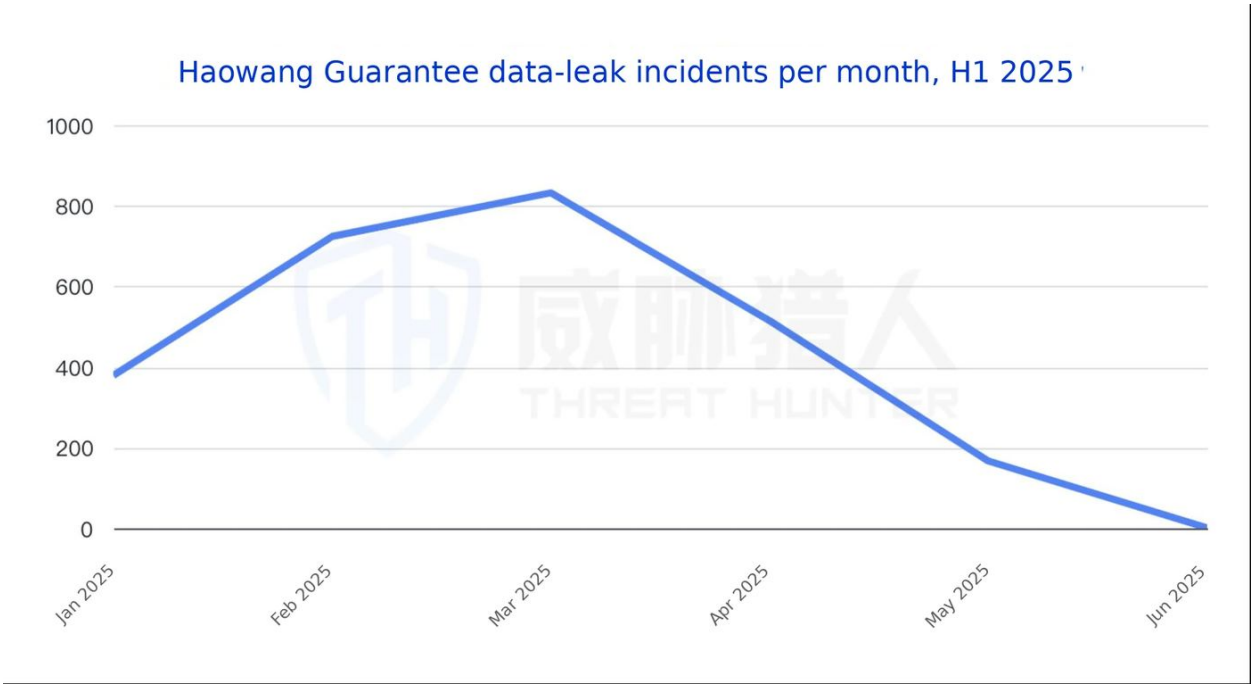
Source: Threat Hunter original report, page 86. Table re-typeset in English from the original.



Screenshots of Haowang Guarantee announcements

Source: Threat Hunter original report, page 87. Original image retained.

Threat Hunter monitoring found that since the outage of "Haowang Guarantee", the number of related data leakage incidents plummeted from 832 in March to basically zero in June.

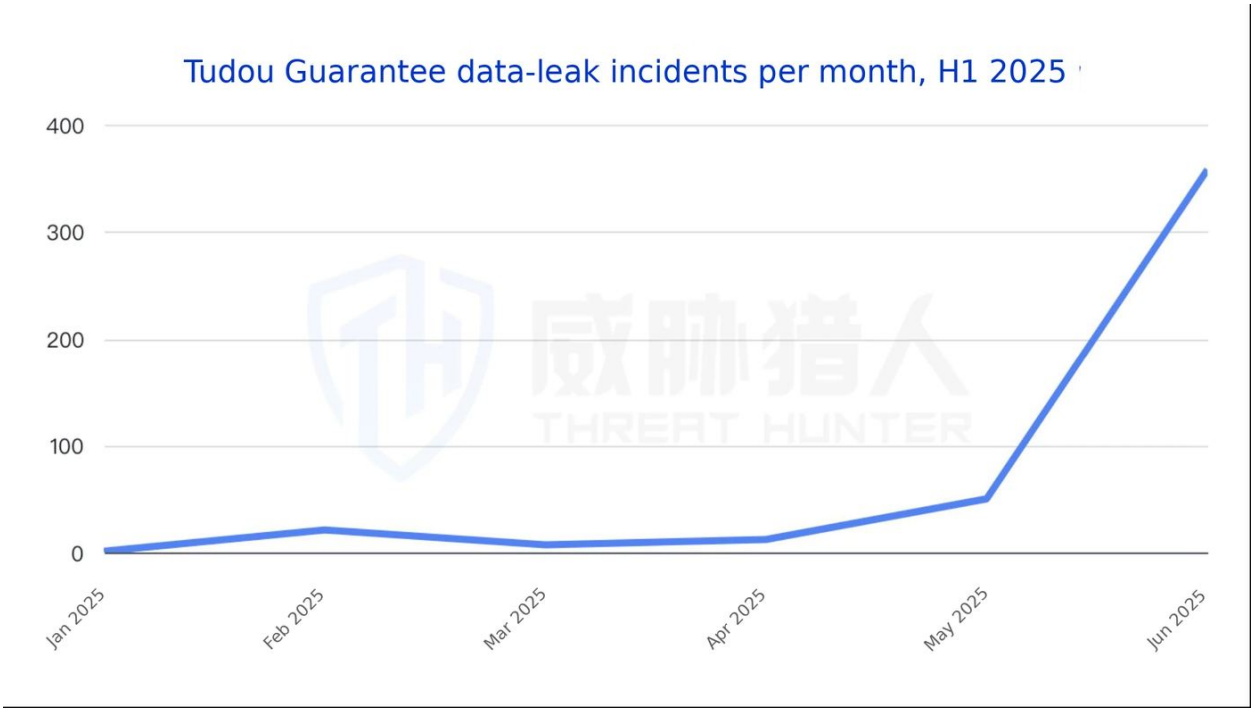


Haowang Guarantee data-leak incidents per month, H1 2025

Source: Threat Hunter original report, page 87. Original figure with Chinese text replaced by English.

(2) New guarantees were quickly filled and transactions quickly resumed, but the demand from the underground market did not disappear. After the collapse of "Haowang Guarantee", new platforms such as "Tudou Guarantee" quickly emerged.

Data shows that data breaches related to Tudou Guarantee surged from 12 in April to 358 in June, an increase of nearly 30 times.

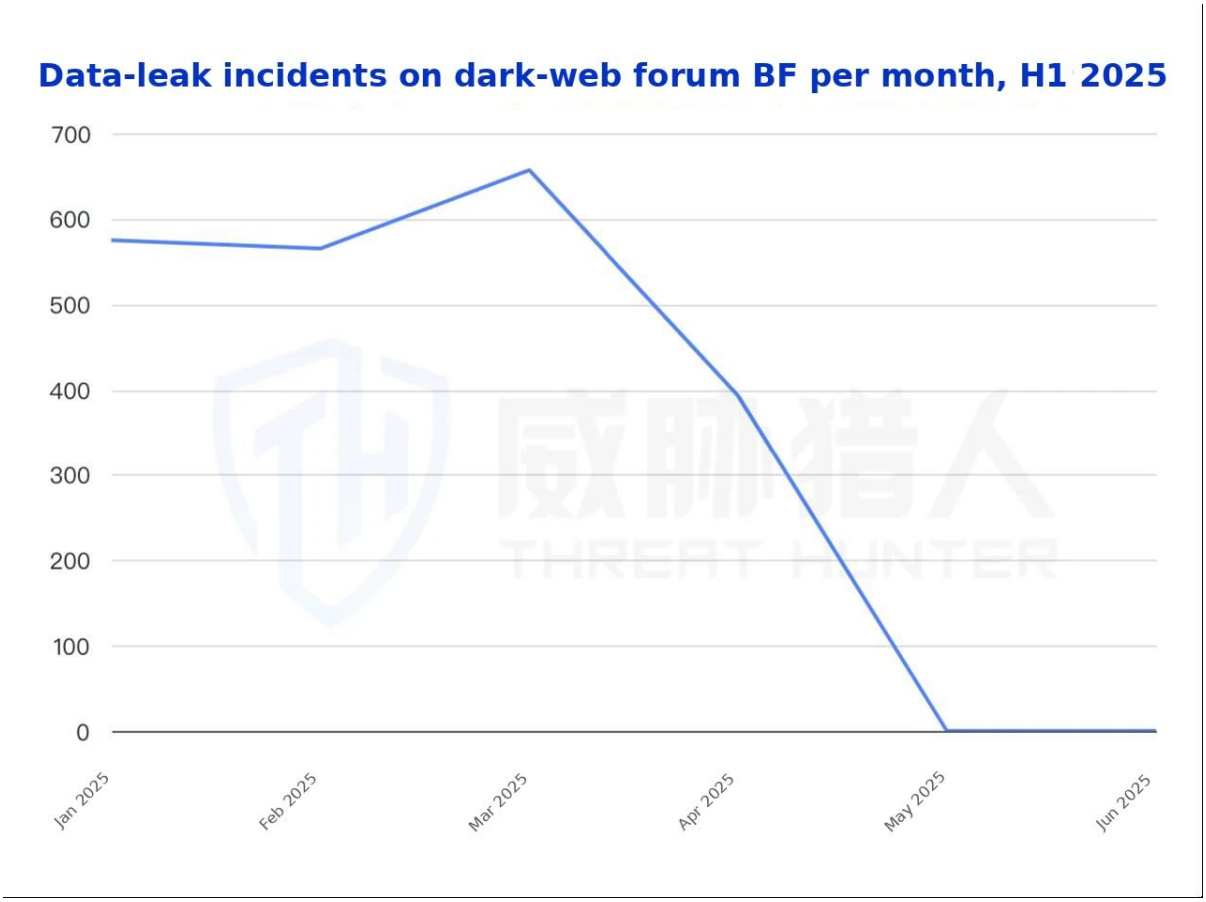


Tudou Guarantee data-leak incidents per month, H1 2025

Source: Threat Hunter original report, page 88. Original figure with Chinese text replaced by English.

The intermediary role of "guaranteed platform" has gradually emerged in the ecosystem of threat actors. The existence of intermediaries not only brokers transactions, but also undertakes the functions of hosting funds and arbitrating disputes. It is an important fulcrum for the sustainable operation of the entire threat actors transaction. Because of this, even if a certain platform is cracked down, new intermediaries will quickly fill their positions and reappear with different vests. As long as transactions exist, the market demand for such "threat actors service providers" will not disappear, making it difficult for them to be completely eradicated.

This industrial chain law also works on important communication channels for threat actors. Taking the leading darknet forum BF as an example, it was also hit in April 2025 and contributed nearly 15% of the data events to darknet channels before it was shut down. Although the threat-actor platform faces continued high-pressure attacks, the market demand for data transactions has never weakened. Take the leading darknet forum BF as an example. In the first half of 2025, the platform was still one of the most important data leakage supply nodes in the world.



Data-leak incidents on dark-web forum BF per month, H1 2025

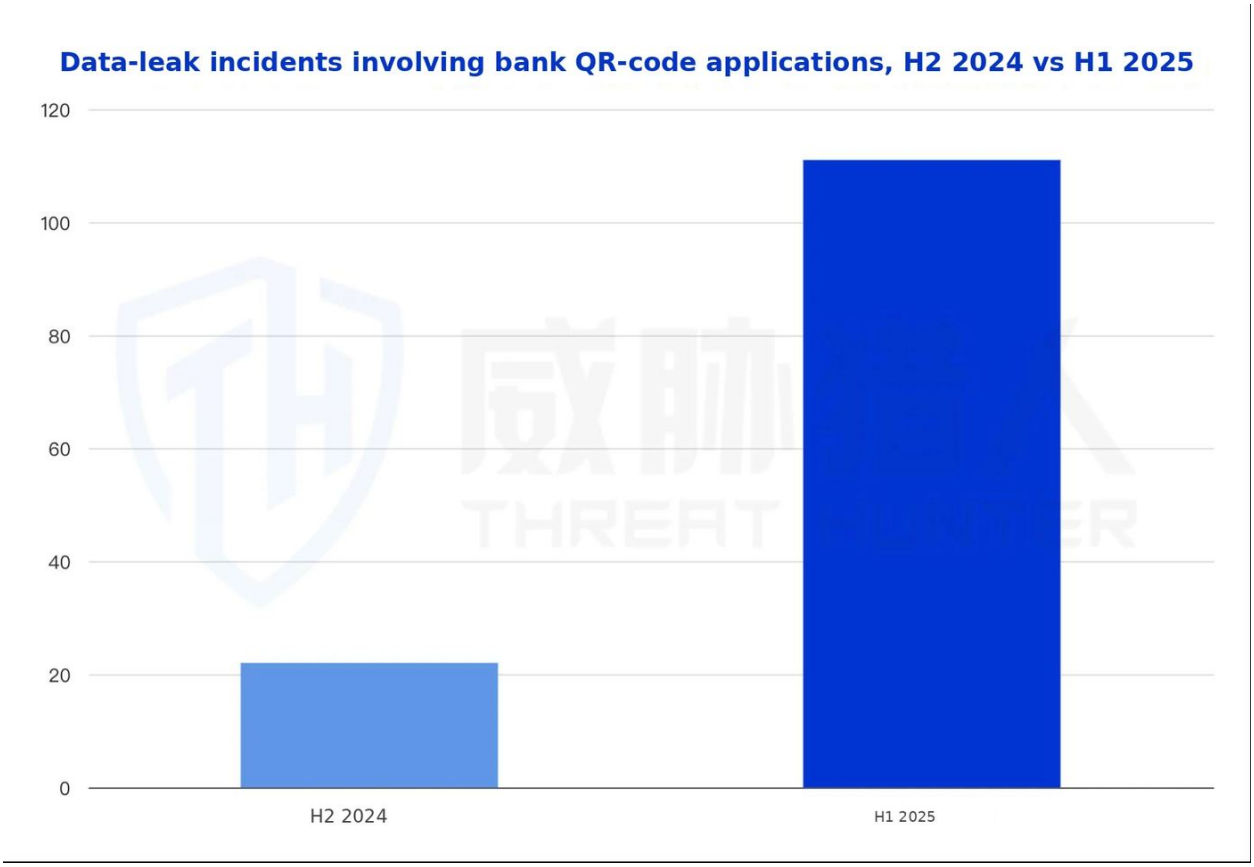
Source: Threat Hunter original report, page 88. Original figure with Chinese text replaced by English.

BF’s case confirms the core law of the cybercrime ecosystem market: when the main trading platform is cracked down, users and demand will quickly migrate to existing or emerging alternatives. The data trading market has strong adaptability. Even if the head platform is destroyed, threat actors can still rely on other channels to maintain business operations.

3.5.3 Bank “scan QR code application” loan information leakage incidents increased significantly compared with the second half of 2024, with an increase of more than 4 times (1) Bank “scan QR code application” loan information leakage incidents increased sharply in the first half of the year

Threat Hunter's continuous monitoring found that among the leaked data captured in the first half of 2025, there was another type of loan information leakage incident called "bank code scanning application materials", with a total of 111 cases, compared with 89 new cases in the second half of 2024, an increase of 404.55%.

Bank code scanning application: refers to information data for users to apply for loan business by scanning the loan activity QR code provided by the bank account manager.

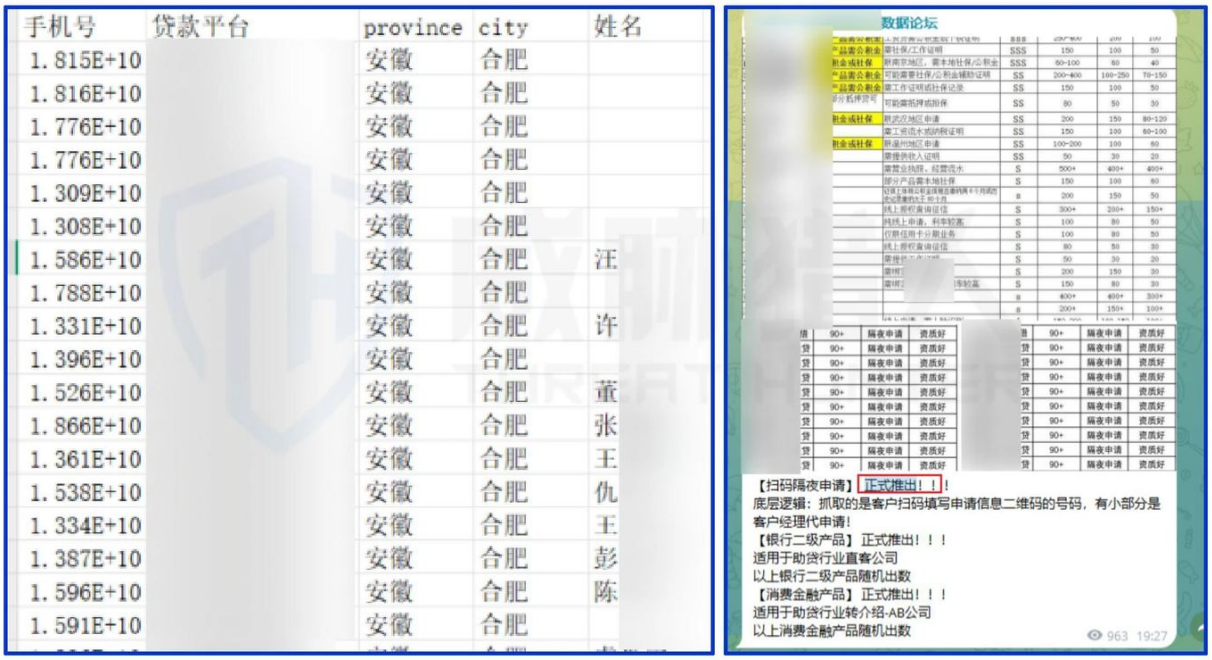


Data-leak incidents involving bank QR-code applications, H2 2024 vs H1 2025

Source: Threat Hunter original report, page 89. Original figure with Chinese text replaced by English.

Through in-depth analysis, Threat Hunter learned about the so-called "scan code application overnight" data among threat actors, which mainly focuses on bank "loan" business. It mainly includes information such as the phone number of the loan user, city area, and loan application approval results; at the same time, according to threat actors

Judging from the screening of the bank loan platform provided, there are more than 80 bank loan businesses, basically local banks or commercial banks.

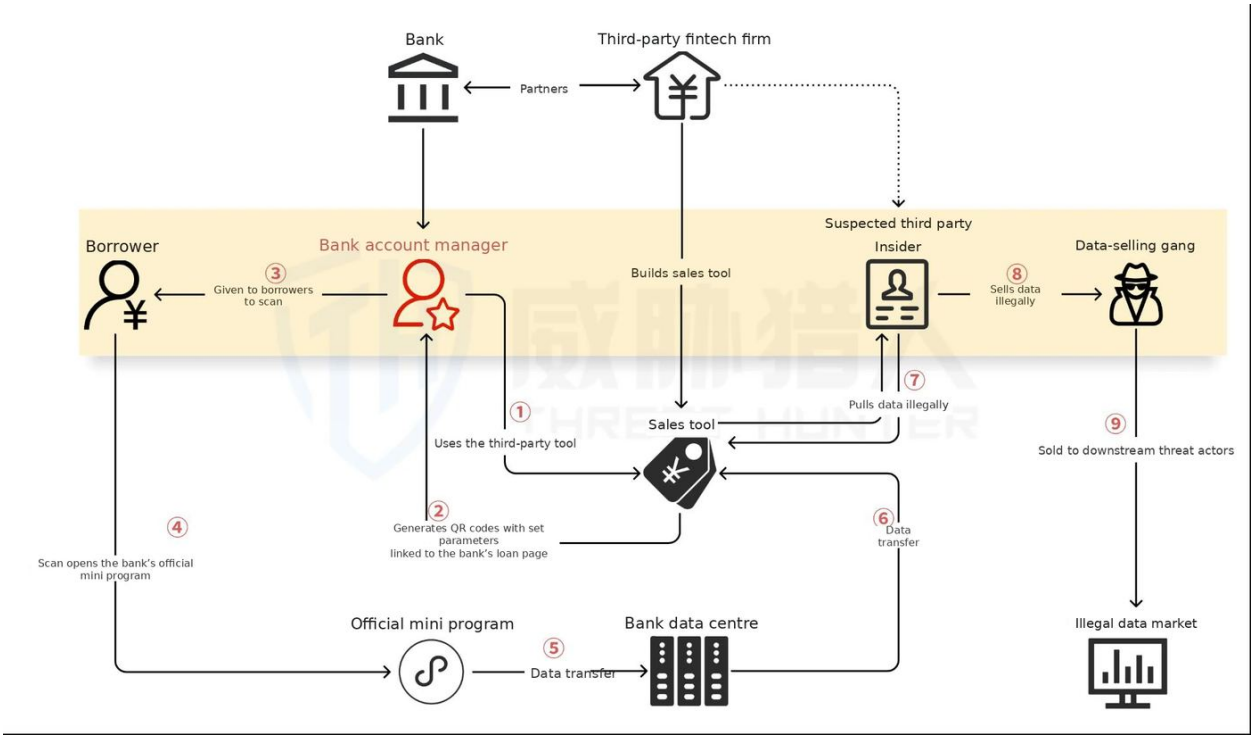


手机号	贷款平台	province	city	姓名
1.815E+10		安徽	合肥	
1.816E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.776E+10		安徽	合肥	
1.309E+10		安徽	合肥	
1.308E+10		安徽	合肥	
1.586E+10		安徽	合肥	汪
1.788E+10		安徽	合肥	
1.331E+10		安徽	合肥	许
1.396E+10		安徽	合肥	
1.526E+10		安徽	合肥	董
1.866E+10		安徽	合肥	张
1.361E+10		安徽	合肥	王
1.538E+10		安徽	合肥	仇
1.334E+10		安徽	合肥	王
1.387E+10		安徽	合肥	彭
1.596E+10		安徽	合肥	陈
1.591E+10		安徽	合肥	

Screenshots of overnight loan-application data offers

Source: Threat Hunter original report, page 90. Original image retained.

(2) Leakage of bank “scan code application” loan information: Marketing tools of third-party financial technology companies have become a core risk point. Threat Hunter analyzed and traced the source of the bank QR codes involved in the leaked data and found that they all pointed to the “xx Marketing Assistant” platform developed by the same well-known financial technology service provider. Based on the list of bank loan platforms released by threat actors, it can be confirmed that more than 80 banking institutions are affected.



How bank loan-application data leaks

Source: Threat Hunter original report, page 90. Original figure with Chinese text replaced by English.

Based on the fact that this type of related incident involves multiple banks, Threat Hunter conducted an in-depth restoration of the specific details and found:

1. In the process of applying for a loan, the user scans the QR code of the loan business activity provided by the bank account manager;

2. The QR code information of this type of bank loan business carries the account manager information and jumps to the bank’s official mini program;

3. Then the user operates and submits a loan application on the specific loan business of the bank's official mini program.



隔夜申请平台推荐				每日出量（三网）不固定		预计出量
平台名称	是否需要公积金	其他材料/备注	推荐级别	一线及高配二线	二线	三线及以下
	部分产品需公积金	本地户籍优先	SSS	200左右-300	100-200	40-100
	否	需银行流水或工资证明	SSS	200左右-300	100-200	40-100
	部分产品需公积金	需公积金或个税证明	sss	250-400	200	100
	部分产品需公积金	需社保/工作证明	SSS	150	100	50
	需公积金或社保	限南京地区，需本地社保/公积金	SSS	60-100	60	40
	部分产品需公积金	可能需要社保/公积金辅助证明	SS	200-400	100-250	70-150
	部分产品需公积金	需工作证明或社保记录	SS	150	100	50
	否（部分抵押贷可能需）	可能需抵押或担保	SS	80	50	30
	需公积金或社保	限武汉地区申请	SS	200	150	80-120
	否	需工资流水或纳税证明	SS	150	100	60-100
	需公积金或社保	限温州地区申请	SS	100-200	100	60
	否	需提供收入证明	SS	50	30	20
	否	需营业执照、经营流水	S	500+	400+	400+
	否	部分产品需本地社保	S	150	100	60
	需要	征信上体现公积金信息且缴纳满 6 个月或历史记录缴纳大于 60 个月	s	200	150	50
	否	线上授权查询征信	S	300+	200+	150+
	否	纯线上申请，利率较高	S	100	80	50
	否	仅限信用卡分期业务	S	100	80	50
	否	线上授权查询征信	S	80	50	30
	否	需提供工作证明	S	50	30	20
	否	需绑定 银行卡	S	200	150	30
	否	需绑定 账户，利率较高	S	150	80	30
	否		s	400+	400+	300+
	否		s	200+	150+	100+
	否	线上申请，需人脸识别	A	150-200	100-150	100+
	否	需提供银行流水	A	150-200	100	80
	否	需授权查询征信	A	100	80	30
	否（抵押贷可能需）	可能需房产/车辆抵押	A	80	50	20
	否	线上申请，需人脸识别	A	100	70	30

Screenshot of an overnight-application platform list

Source: Threat Hunter original report, page 91. Original image retained.

Threat Hunter learned that the loan QR code information provided by the account manager was actually produced through a sales tool developed by a third-party financial technology company (because the tool page is relatively sensitive, it will not be shown in detail here).

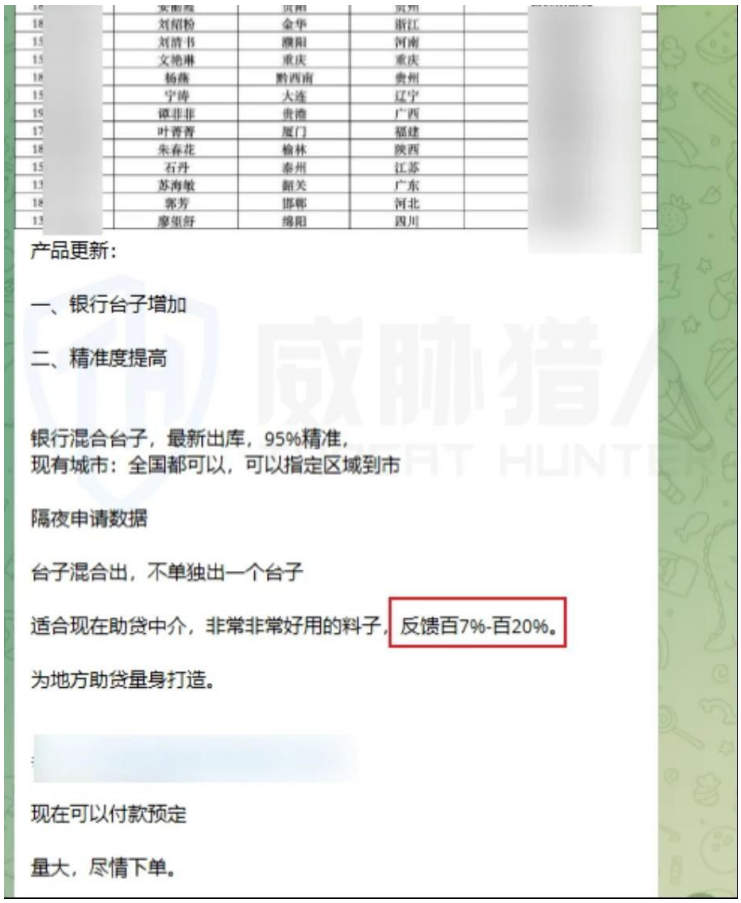
Threat Hunter analyzed this third-party financial technology company and found that the company not only provides application system software development for banks, but also provides intelligent fraud-control strategies. Different fraud-control strategies are provided for loan users with different qualifications to cooperate with bank account managers for follow-up. It mainly provides banks with business digitization and promotes the development of bank loan business. After a user submits a loan application in the bank's official mini program, the bank will synchronize the user's relevant information to the sales tool to facilitate performance statistics and follow-up by the bank's account manager. At the same time, it also brings the risk of data leakage.



Screenshots of chats selling bank-application data

Source: Threat Hunter original report, page 92. Original image retained.

According to Threat Hunter's follow-up and analysis of the information released by threat actors, it was found that when this type of incident began to be publicized, threat actors claimed that the data came from "insiders", that is, internal employees leaked it. Considering that more than 80 banking institutions are involved in the above, the probability of leakage by internal employees of 80 banking institutions is extremely low, and it is initially inferred that they are internal employees of third-party financial technology companies.



Screenshots of overnight-application data samples

Source: Threat Hunter original report, page 92. Original image retained.

According to research by Threat Hunter, after such information and data are leaked to the illegal data trading market, they are mainly used to assist loan companies in targeted marketing. At the same time, according to the feedback from threat actors after marketing, the effect is very good, with a success rate of up to 20%, which also proves the authenticity of such data.

Risks and Hazards:

Customer churn and revenue loss: High-intention customers are contacted by competitors (loan assistance companies) on the day after application, offering alternative products with lower interest rates or faster approvals, which directly leads to the loss of potential customers of the bank and the loss of predictable interest income and intermediate business income.

Brand reputation damage: Data leakage has seriously damaged users' trust in the bank's data security capabilities, especially in the core business of lending, and will have a long-term negative impact on the bank's brand. "Regulatory compliance risk: Such incidents have constituted a serious leak of personal financial information and violated the "Personal Information Protection Law" and other relevant regulations. Banks, as data processors, will face the risk of high fines and regulatory accountability.

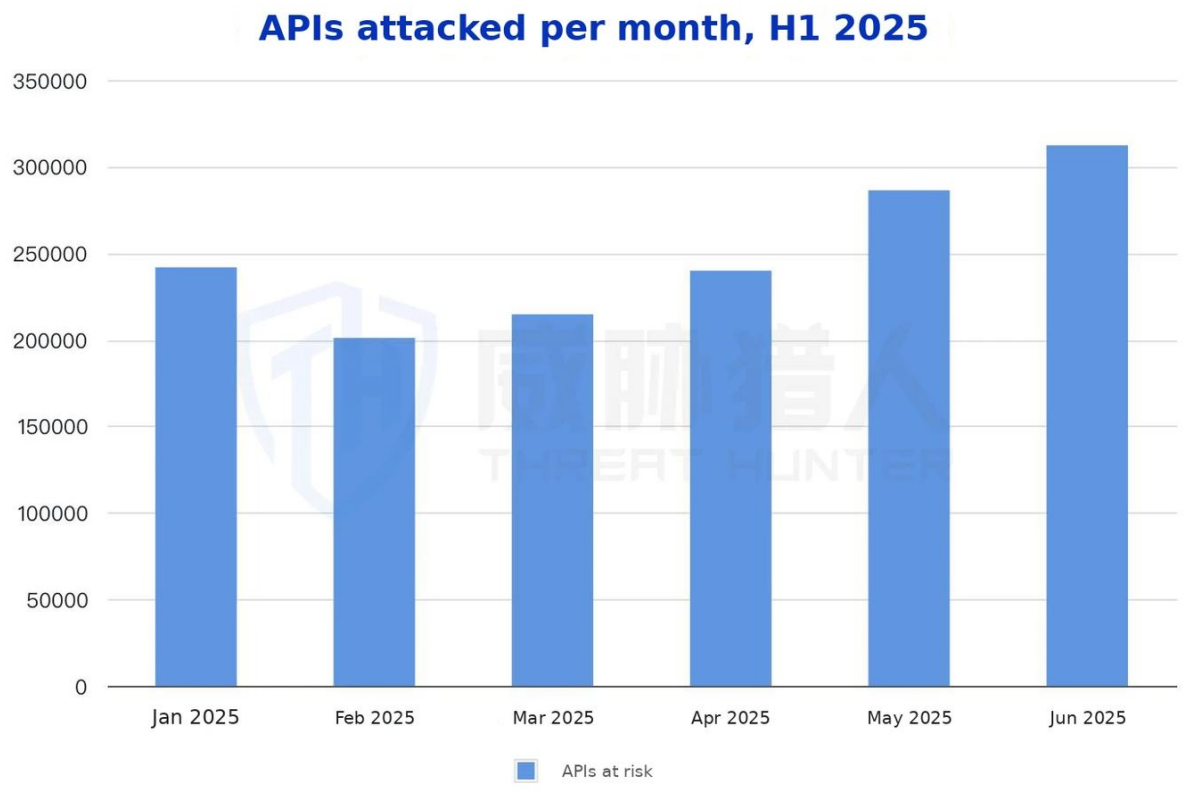
3.6 API security scenario analysis

Under the trend of digitalization and onlineization, API interfaces, as an important channel for application connection and data transmission, have experienced massive growth in recent years. The imbalance between the growth rate of API applications and their security development has made them the preferred target for malicious attacks, and the battle between attack and defense surrounding API security has intensified.

Threat Hunter intelligence data shows that the number of APIs attacked in the first half of 2025 exceeded 1.49 million, involving multiple industries such as consumer finance, banking, e-commerce, online education, and securities.

3.6.1 The average number of APIs attacked each month in the first half of 2025 exceeded 249,000

Threat Hunter monitoring shows that the number of captured API attacks per month in the first half of 2025 is on the rise. The average number of APIs under attack per month reached 249,000, a significant increase from 194,000 in the second half of 2024. The average monthly increase reached 55,000, an increase of 28.35%. The obvious growth trend is mainly due to the increase in cybercriminal attacks in the financial industry, which has led to an increase in the overall trend.



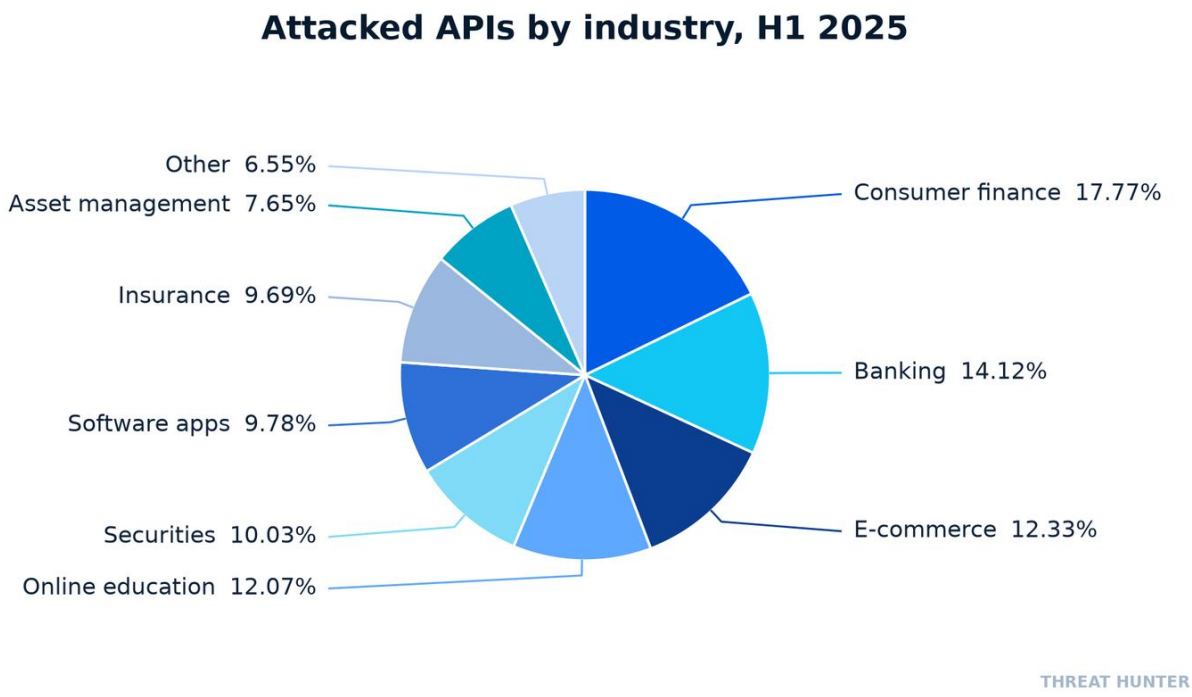
APIs attacked per month, H1 2025

Source: Threat Hunter original report, page 94. Original figure with Chinese text replaced by English.

3.6.2 The financial industry has become the primary target, and consumer finance risks have reached the peak

In the first half of 2025, the Threat Hunter honeypot platform monitored nearly 1.5 million API attacks, affecting 1,176 companies.

From an industry perspective, attacks are highly concentrated in the five major industries of consumer finance, banking, e-commerce, online education, and securities. Among them, the financial industry consisting of consumer finance, banking, and securities is the hardest hit area, accounting for 41.92% of attacks. The consumer finance industry is the primary target of attackers.



Attacked APIs by industry, H1 2025

Source: Threat Hunter original report, page 94. Redrawn in English from the original figure.

Judging from the magnitude of the attack subjects, 209 consumer finance companies were targeted in 2025, accounting for a high proportion of the API attack industry.

17.77%. Attacks are mainly concentrated on licensed consumer finance companies, Internet platform financial services, transformation loan assistance platforms and small loan companies.

Division. After analysis, there are three main reasons why consumer finance companies are highly concerned by threat actors:

1. The complexity of data collection and circulation has increased dramatically: consumer finance platform businesses are deeply embedded in complex scenarios such as e-commerce and social networking, resulting in

User data comes from a wide range of sources and types, and the data transfer chain between the platform and its partners is long and fragile. Attackers often take advantage of interface weaknesses in any link in the chain to launch attacks such as information theft and credential stuffing.

2. Explosive growth of API interfaces in the open ecosystem: In order to support complex embedded financial scenarios (such as scenario installment, credit payment

payment, joint fraud controls), the platform needs to open a large number of API interfaces with different functions to a large number of internal and external partners (merchants, technical service providers, data sources). The increase in the number of interfaces and the complexity of calling relationships have significantly expanded the attack exposure surface. If security management is not synchronized and refined, it will be easily exploited by attackers to carry out interface detection, unauthorized access and even large-scale credential stuffing attacks.

3. Driven by benefits brought by the high value of highly sensitive data: consumer finance platforms centrally store massive amounts of sensitive user information (identity, credit information,

Finance, etc.), the price of a single piece of this sensitive information can reach 100 yuan in the black market, which is far higher than other industry data, creating a huge temptation for attackers.

3.6.3 Typical API attack events worthy of attention in the first half of 2025

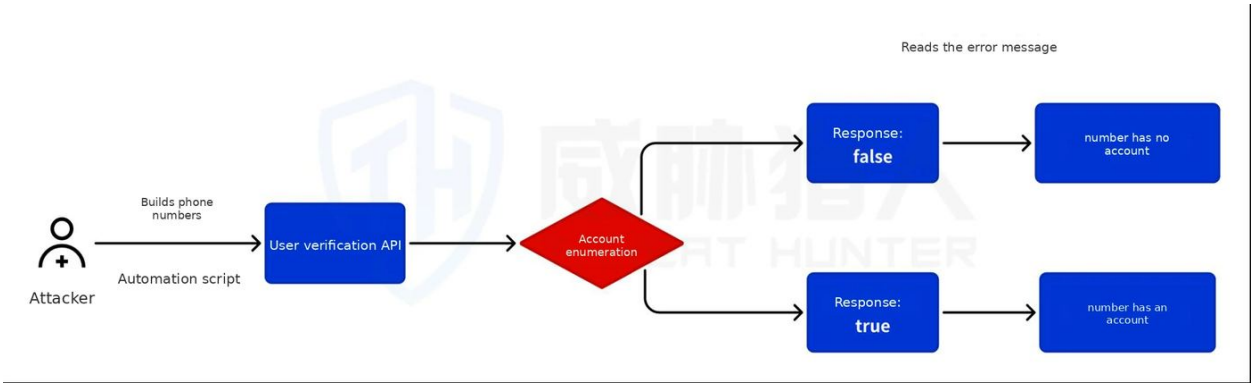
Threat Hunter monitored threat actors' API attacks involving multiple downstream malicious scenarios, covering fleecing, malicious order traffic manipulation, data crawling, marketing business fraud, and inventory reservations. Monitoring data in the first half of 2025 shows that the core API attack methods supporting these malicious activities focus on account scanning attacks, credential stuffing attacks, and credential occupation attacks.

(1) Account scanning attack: The online business of an Internet platform suffered a cybercrime ecosystem account scanning attack, and a large amount of user information was leaked.

In March 2025, Threat Hunter detected that an attacker launched an account scanning attack on a domestic Internet platform. From February to March, the attacker used proxy IP to launch more than 100,000 attacks on the platform interface, resulting in the exposure of 50,000 valid accounts.

After traffic analysis and recurrence, it was found that in the platform's user verification interface, there were obvious differences in the response data returned by the verification of registered users and unregistered users. Therefore, threat actors used this interface to verify in large quantities whether phone numbers were registered users of the platform, resulting in the exposure of valid accounts and the leakage of user privacy.

The specific attack process is shown in the figure below. The threat actors construct the request body and use different phone numbers, while other authentication parameter information characteristics remain unchanged. The threat actors can determine whether the phone number is a valid account through the echo. If the phone number is an invalid account, the echo is "false". If the phone number is a valid account, the platform echoes "true".



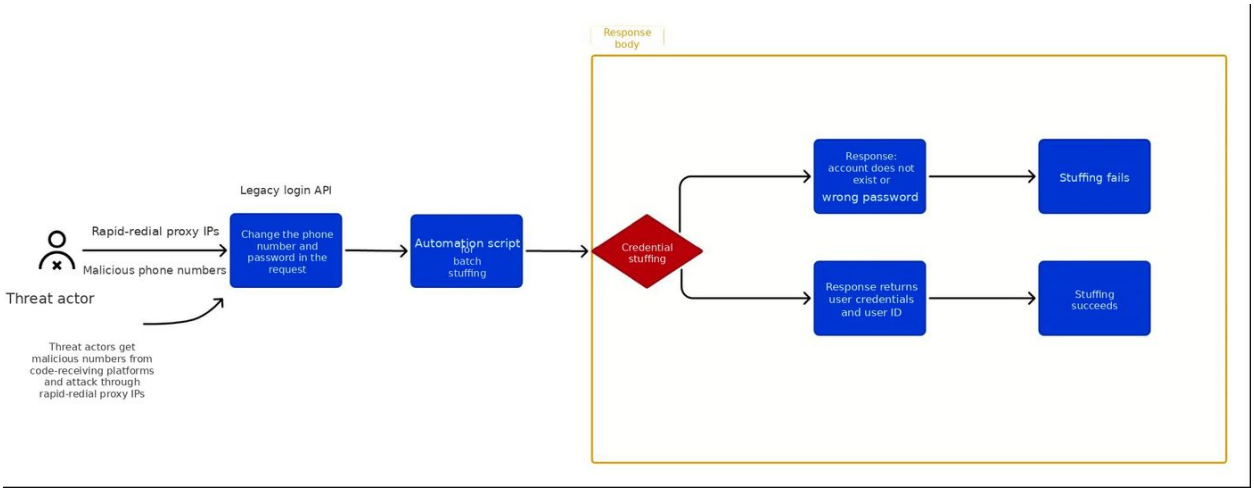
Account-enumeration attack flow

Source: Threat Hunter original report, page 96. Original figure with Chinese text replaced by English.

(2) Credential Stuffing Attack: The old login interface was not retired and became a breach of credential stuffing. A certain platform was hit by batch credential stuffing attacks. The traffic captured from the Threat Hunter honeypot found that in May 2025, the attacker used the proxy IP to launch attacks on the old version of the platform's login interface more than 300,000 times, successfully credential stuffing nearly 3,000 accounts.

In-depth analysis shows that the attacker's attack interface is an old version of the platform's login interface. This interface has flaws in plaintext password transmission and lacks dynamic signatures and human-computer verification. This allows threat actors to bypass security protection at very low cost and pose a threat to the account system. After the credential stuffing attack was successful, the attacker maliciously initiated high-frequency payment operations through stolen account credentials, causing substantial economic losses to the original account holder.

The attack process is shown in the figure below. threat actors use the old version of the login interface to launch a credential stuffing attack. Due to the lack of frequency limits and plaintext password transmission defects in the old version of the interface, the attacker uses automated script attacks to target the Mobile field and password field in the request body. Based on the different data content returned in the response body, it is judged whether the credential stuffing is successful. If the credential stuffing fails, the response body information returns "the account does not exist or the password is wrong". If the credential stuffing is successful, the response body returns user credentials, user ID and other sensitive information.



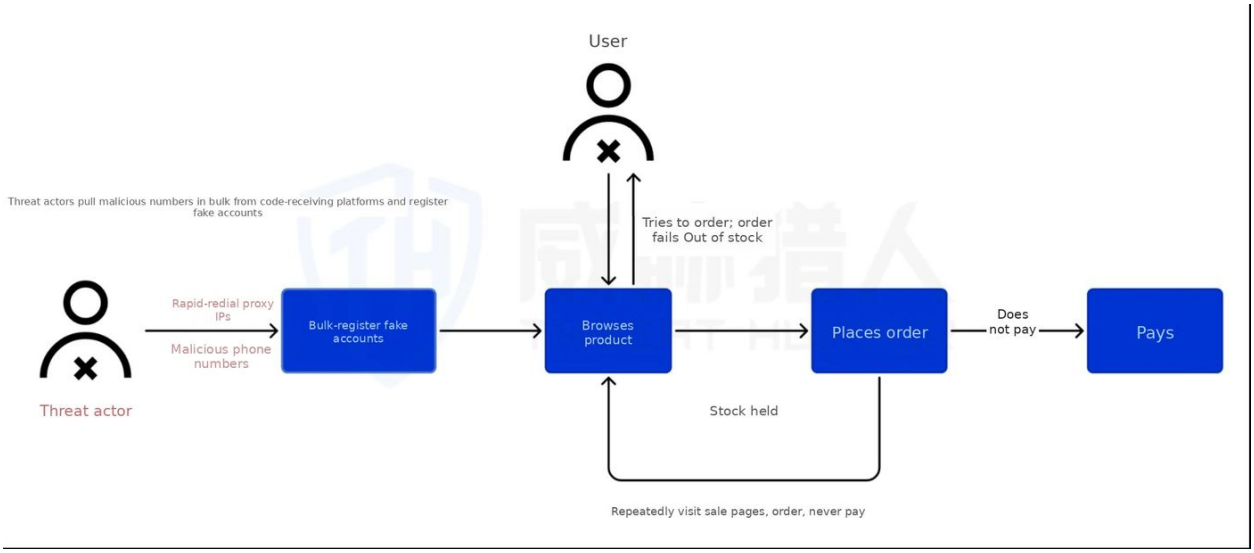
Credential-stuffing attack on a legacy login API

Source: Threat Hunter original report, page 97. Original figure with Chinese text replaced by English.

(3) Database occupation attack: A certain platform interface vulnerability was exploited to perform database occupation attacks to make profits. In June 2025, the Threat Hunter honeypot captured the batch attack traffic initiated by the attacker using the proxy dial IP and the phone number of the receiving platform. Specifically, it launched 100,000 attacks on the interface of an e-commerce store, and occupied 10,000 special-priced products in batches for self-purchase arbitrage.

In-depth analysis revealed that the target interface contained a high-risk vulnerability: the abnormal account could purchase special items an unlimited number of times and generate pending payment orders until the inventory was exhausted. Subsequently, the account will place orders for goods in batches, and the third-party platform will sell them to achieve arbitrage.

The attack process is shown in the figure below. threat actors obtain a large number of fake numbers through the SMS verification-code receiving service, superimpose the proxy instant dial IP pool technology, register puppet accounts on the platform in batches, and maliciously squeeze out the inventory of special products. It uses false account self-purchase orders to complete arbitrage and laundering goods. It also prevents normal users from completing transactions and destroys the fair trading ecosystem of the platform.



Inventory-hoarding attack flow

Source: Threat Hunter original report, page 98. Original figure with Chinese text replaced by English.

Write at the end:

For enterprises, they must fully realize that the offensive and defensive game with threat actors is a long-term, dynamic and continuously evolving process. Only by relying on cybercrime ecosystem intelligence data covering the entire network and across platforms can potential threats be identified in advance before the attack occurs, and accurate source tracing and pre-emptive interception can be achieved in stages such as attack resource preparation, tool scheduling, and path construction. By knowing clearly what resources threat actors will use, which path they will take, and how they will carry out the attack, we can truly achieve "control before the enemy arrives."

This is exactly the value of intelligence, and it is also the direction Threat Hunter continues to invest in: through systematic cybercriminal groups attack and defense research and intelligence monitoring capabilities, it helps 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.

Company official website: www.threathunter.cn Cooperation email: Marketing@threathunter.cn